U.S. Department
of Transportation
**Federal Highway
Administration**

INTELLIGENT TRANSPORTATION SYSTEMS (ITS)

Information Security Analysis

November 1997

Intelligent Transportation Systems
Joint Program Office

Technical Report Documentation Page

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.
FHWA-JPO-98-009		

4. Title and Subtitle	5. Report Date
Intelligent Transportation Systems (ITS) Information Security Analysis	November, 1997
	6. Performing Organization Code
7. Author(s)	8. Performing Organization Report No.
Keith Biesecker, Elizabeth Foreman, Kevin Jones, Barbara Staples	
9. Performing Organization Name and Address	10. Work Unit No. (TRAIS)
Mitretek Systems 7525 Colshire Drive McLean, VA	11. Contract or Grant No. DTFH61- -95-C-00040
	13. Type of Report and Period Covered
12. Sponsoring Agency Name and Address	
Department of Transportation FHWA Intelligent Transportation Systems Joint Program Office 400 Seventh Street, S.W. - Room 3422 Washington, DC. 20590	14. Sponsoring Agency Code HVH-1

15. Supplementary Notes

William S. Jones

16. Abstract

The Intelligent Transportation Systems (ITS) program is the application of information technologies (computing, sensing, and communications) to surface transportation. Because of a reliance on these technologies, ITS will become increasingly dependent on information security. By understanding how to achieve and maintain secure systems, the ITS community can develop comprehensive information security practices and appropriate security policies for ITS programs. Subsequently, they can put these into practice.

This document presents the results from an information security analysis that was based on the National ITS Architecture. The ITS information security analysis comprised three assessments to identify and characterize the various threats to (1) the ITS subsystems, (2) their exchange of information, and (3) their supporting communications infrastructure. The assessments also provide recommended solutions (i.e., security services) that can be used to reduce or eliminate identified threats and to better protect ITS. While focusing on the threats and their impacts to ITS security, this report also provides necessary background information and a general understanding of information security. It addresses common information and a general security issues as well as those that pertain specifically ITS.

The conclusions and recommendations form this report address increasing information security awareness within the ITS community, the development of secure ITS operations, and the issue of future security activities within the ITS domain.

17. Key Words	18. Distribution Statement
Information security, Intelligent Transportation Systems (ITS)	No restrictions. This document is available to the public from: The National Technical Information Service Springfield, Virginia 22161

19. Security Classif. (of this report)	20. Security Classif. (of this page)	21. No. of Pages	22. Price
Unclassified	Unclassified	206	

Form DOT F 1700.7 (8-72) Reproduction of completed page authorized

ABSTRACT

The Intelligent Transportation Systems (ITS) program is the application of information technologies (computing, sensing, and communications) to surface transportation. Because of a reliance on these technologies, ITS will become increasingly dependent on information security. By understanding how to achieve and maintain secure systems, the ITS community can develop comprehensive information security practices and appropriate security policies for ITS programs. Subsequently, they can put these into practice.

This document presents the results from an information security analysis that was based on the National ITS Architecture. The ITS information security analysis comprised three assessments to identify and characterize the various threats to (1) the ITS subsystems, (2) their exchange of information, and (3) their supporting communications infrastructure. The assessments also provide recommended solutions (i.e., security services) that can be used to reduce or eliminate identified threats and to better protect ITS. While focusing on the threats and their impacts to ITS security, this report also provides necessary background information and a general understanding of information security. It addresses common information security issues as well as those that pertain specifically to ITS.

The conclusions and recommendations from this report address increasing information security awareness within the ITS community, the development of secure ITS operations, and the issue of future security activities within the ITS domain.

Suggested Keywords: information security, Intelligent Transportation Systems (ITS)

ACKNOWLEDGMENTS

The authors wish to thank Mr. Mike McGurrin, Mr. John Cerva, and Mr. Dan Gambel for their direction and guidance on this document. They authors also wish to thank Mrs. Debra Johnson for completing the final product.

TABLE OF CONTENTS

SECTION **PAGE**

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

PURPOSE

This document presents the results from an information security analysis of the Intelligent Transportation Systems (ITS). The objectives are to provide initial information security assessments within the surface transportation domain and to develop a foundation for further enhancements to ITS security.

This ITS information security analysis comprised three assessments to identify and characterize the various threats to the following:

- The ITS subsystems
- The ITS subsystems' exchange of information (i.e., data flows)
- The ITS subsystems' supporting communications infrastructure

The assessments also provide recommended solutions (i.e., security services) that can be used to reduce or eliminate identified threats and to better protect ITS. Since the conduct and results of each assessment complemented the other two, an integrated, more complete security analysis of the ITS National Architecture is provided (figure ES-l).

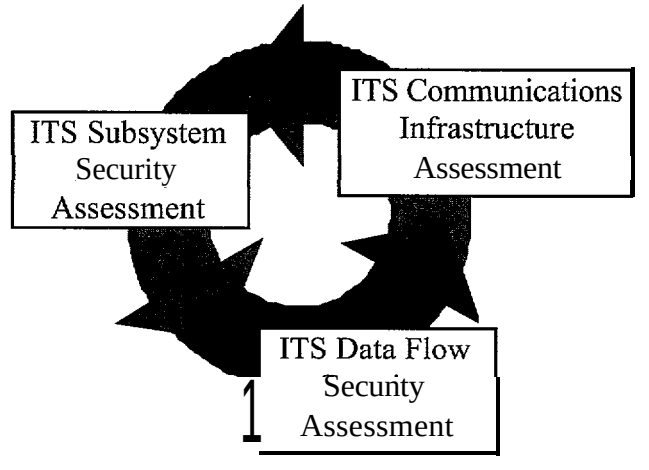


Figure ES-l. ITS Security Analysis Approach

BACKGROUND

The ITS program is the application of information technologies (computing, sensing, and communications) to surface transportation. The need to protect against the vulnerabilities of and threats to these technologies is growing as rapidly as the technologies themselves. The increasing reliance on new technologies and technology-enabled services suggests that organizations' future needs for information security will be significant. Consequently, ITS will become increasingly dependent on information security.

Until recently, the Federal Government paid little attention to researching and addressing the information security needs of the government and commercial sectors that do not process classified information. However, on 15 July 1996, President Clinton signed Executive Order 130 10, "Critical Infrastructure Protection," that established a commission to foster the protection of national infrastructures considered vital to the security of the United States. These critical infrastructures include, among others, electrical power systems, banking and finance, telecommunications, and transportation.

Additionally, and more specifically, activities of the National Science and Technology Council (NSTC) Transportation Research and Development Committee are currently focused on investigating information security within the transportation domain. As such activities proceed and as ITS continues to incorporate emerging information technologies, it becomes increasingly important for the U.S. Department of Transportation (USDOT) to consider appropriate action (e.g., information security awareness and development).

INFORMATION SECURITY OVERVIEW

The focus of this document is the assessment and identification of particular threats to ITS and the recommendation of security services to counter those threats. This involves an overview of information security components fundamental to the assessment process, including the following:

- **The objectives required to secure a system.** Objectives include the following:
  - Confidentiality (e.g., protecting personal records)
  - Integrity (e.g., providing accurate financial transactions)
  - Availability (e.g., guaranteeing timely services)
  - Accountability (e.g., tracing system activity)
- **The threats that could undermine the objectives.** Threats originate from both internal and external sources and are categorized as those causing the following:
  - Denial of service: preventing a system from operating as intended
  - Disclosure: acquiring sensitive information through unauthorized channels
  - Manipulation: modifying information
  - Masquerading: posing as an authorized entity to access information
  - Replay: re-transmitting valid information under invalid circumstances
  - Repudiation: denying an action
- **The security services to counter the threats.** Security services are those protections that must be provided to ensure the secure operation of a system and to fulfill the confidentiality, availability, integrity, and accountability objectives. Those security services of particular interest to this analysis include the following:
  - Authentication: verifying user identities
  - Confidentiality: protecting private and personal information
  - Integrity: maintaining information accuracy

- Non-repudiation: preventing users from denying their actions
- Access Control: limiting system resources to properly authorized users
- Auditing: recording system operations and the users who perform them
- Availability: protecting against denial-of-service attacks
- System security management: providing physical, manual, and automated controls

INFORMATION SECURITY ANALYSIS APPROACH AND METHODOLOGY

The National ITS Architecture provides a common structure for the design of ITS. It consists of several documents (e.g., logical architecture, physical architecture, implementation strategy, etc.) that define a framework from which various ITS design approaches can be developed.

The logical architecture document presents a functional view of 30 interrelated ITS user services. These services are defined as part of the ITS National program planning process and are deigned to provide for travelers, traffic management operators, transit operators, commercial vehicle owners and operators, state and local governments, and others.

The physical architecture document identifies four types of subsystems: traveler, center, roadside, and vehicle. These subsystem types comprise nineteen particular ITS subsystems. In more detail, the physical architecture then describes each of these subsystems, as well as terminators -- other subsystems (e.g., DMV) and users (emergency vehicle driver) related to surface transportation operations.

The physical architecture document also describes the exchange of information among ITS subsystems and terminators (i.e., data flows). Along with the communications infrastructure, the subsystem operations and their related data flows support the logical architecture functions and hence provide the ITS user services. Therefore, a broad ITS security analysis (as depicted in figure ES-l) originates from the ITS subsystem assessment.

- **Subsystem Security Assessment**

  Assessing the various threats to the ITS subsystems involved several activities, including the following:

  - Review of the National ITS Architecture
  - Identification of major ITS subsystem functionality and interaction with other ITS subsystems and non-ITS terminators
  - Examination of the ITS data flows and resultant security analysis
  - Examination of the ITS communications infrastructure threat impacts
  - Development of threat scenarios

  The subsystem security assessment provides a detailed analysis for readers most interested in ITS subsystem operations. Section 4 documents the subsystem assessment and incorporates the findings from the two other assessments: the detailed security assessment of the data flows using the ITS communications infrastructure (Appendix A) and the high-level security assessment of the ITS communications infrastructure (Appendix B).

- **Data Flow Security Assessment**

  The ITS data flow assessment involved a detailed review of the complete data flow structure. Security threat categories and security services were identified for each of the physical data flows. This process involved several activities, including the following:

  - Reviewing the content of each physical data flow
  - Reviewing the content of all constituent logical data flows
  - Considering collectively the content, intended function, and constraints of each complete data flow
  - Considering the proposed transmission method and any of its inherent vulnerabilities
  - Identifying potential threat categories applicable to the collective data flow
  - Identifying appropriate security services(s) to thwart the threats belonging to the noted threat categories

  Appendix A contains the results of the ITS data flow assessment.

- **Communications Infrastructure Assessment**

  The communications infrastructure assessment entailed a high-level analysis of the following five types of ITS communications technologies used for ITS operations:

  - Wireline
  - Two-Way Wide-Area Wireless
  - One-Way Wide-Area Wireless
  - Dedicated Short-Range Communications (DSRC)
  - Vehicle-to-Vehicle

  The intent of the assessment was to identify the impacts to ITS in the event of a major communications denial of service. Denials of communications service include, but are not limited to the following: major power outages; degraded service, degraded performance, or interruptions; and unavailable services to some or all users, applications, regions, or devices. Appendix B contains the results of the high-level analysis of the ITS communications infrastructure.

The approach to documenting these assessments included illustrating various threats and their potential impacts on ITS. With ITS is in its infancy and few large-scale deployments of ITS, broader and more encompassing security-related incidents are rare. Incident scenarios used throughout this document illustrate what might often seem to be minor inconveniences of little or no consequence to particular public agencies, private corporations, or the general public. Although significant and costly on an individual basis, the many specific scenarios might tend to obscure or undermine a greater issue.

ITS was established to develop a National transportation infrastructure that is economically efficient and environmentally sound, provides the foundation for the Nation to compete in the global economy, and moves people and goods in a safe and energy efficient manner. Either a major security-related incident (e.g., the destruction of an entire ITS facility) or a

gradual system deterioration from an aggregate of individual security-related incidents could lead to a complete collapse of ITS services. Such extensive losses compromise ITS objectives and would have significant impact on how the general public conducts their day-to-day lives and operations.

The broader impact of such occurrences is easier to comprehend by recalling just some the many ITS benefits that might be lost:

- Improved Safety -- Using a real-time traffic adaptive freeway control system, the Minnesota Department of Transportation has decreased its accident rate by 25 percent and improved response times to incidents by 20 minutes.
- Reduced Traffic Congestion -- FAST-TRAC, a project consisting of adaptive signal control, automated traffic monitoring and other ITS technologies, has increased vehicle speeds by 19 percent during peak hours in Oakland County, Michigan.
- Improved Public Transportation -- The Winston-Salem Transit Authority reports that its Automatic Vehicle Location (AVL) system has decreased paratransit passenger waiting time by 50 percent.
- Reduced Commercial Spending -- The commercial and public sector fleets provide a variety of economic benefits from ITS, and retailers reduce inventory and overhead costs with "just-in-time" delivery improved by ITS applications.
- Reduced Government Spending -- The ADVANTAGE I-75 project, which allows properly-equipped commercial vehicles to travel the I-75 corridor with minimal stoppage, cut weigh station operating costs by up to $160,000 annually; electronic credentials checking and safety inspections save another $4.5 to $9.3 million annually.
- Reduced Pollution -- An independent environmental firm studying the impacts of Oklahoma's PIKEPASS automatic toll system found that cars and trucks using PIKEPASS lanes emitted up to 30% less pollution than those vehicles operating in the manned toll lanes.

The possibility and potential consequences of losing these ITS benefits -- benefits that the public has become accustomed to -- should not be overlooked while reviewing some of the finer details and specific security-related scenarios addressed in this document.

CONCLUSIONS AND RECOMMENDATIONS

By understanding how to achieve and maintain secure systems, the ITS community can develop comprehensive information security practices and appropriate security policies for ITS programs. Subsequently, they can put these into practice. The following **summarize** Mitretek's conclusions and recommendations to help accomplish these goals.

- **Information Security Awareness and Policy Development**

1. *The surface transportation community is largely unaware of the significance of information security. Secure ITS will require an enhanced awareness **of** information security issues and the continued development **of** information security policy. State and local ITS implementors will need to be more cognizant of information security, and the industry as a whole will need to pursue the development and implementation **of** information security policy.*

ITS information security awareness and policy development should include the following activities:

- Developing an ITS information security program that provides guidance to those who will oversee the acquisition, installation, operation, and maintenance of ITS-based systems. High level overviews could provide both management and field personnel with strategic information for implementing and maintaining necessary information security needs

- Clarifying ITS information security policy and its applicability (if any) at national, state, and local levels. Apart from the ITS industry's ***Fair Information*** *and Privacy Principles,* little effort has been expended to address information security within ITS. The government and the private sector must work together to develop a strategy for protecting ITS and its supporting transportation infrastructure. Policy makers should encourage participation at various government levels as well as within the private sector and should disseminate potential policy for public review.

- Coordinating with the Presidents Commission on Critical Infrastructure Protection and its Information Protection Task Force (IPTF), the National Security Telecommunications Advisory Committee (NSTAC) Information Infrastructure Group (IIG), the National Science and Technology Committee (NSTC), and the International Institute for Surface Transportation Policy Studies (IISTPS). Collaboration among these groups' security efforts could expedite both security awareness and security policy development within the surface transportation community.

- **ITS Security Analysis**

1. *Due to the scope* ***of*** *the National ITS Architecture documents, information* ***security*** *requirements were not thoroughly considered. Currently, there is neither a Security Architecture nor a Security Policy* ***for*** *ITS that, at minimum, articulates high-level ITS security objectives.*

   - Support the information security awareness and policy development activities noted above. Resulting security requirements should be adopted consistently throughout ITS (e.g., subsystems, data flows, and supporting communications infrastructures).

2. *Since ITS encompasses a wide range* ***of*** *information (e.g., HAZMAT, traffic control, safety, financial, and personal privacy), it is also susceptible to various attacks. Either intentional or accidental incidents that disrupt or compromise ITS could lead to significant public safety and emergency response effectiveness concerns, corruption* ***of*** *financial transactions and records, violation* ***of*** *citizen privacy, and a loss* ***of*** *ITS credibility.*

   - ITS system designs should include measures to protect against a wide range of security threats. Security services (e.g., authentication, access control, audit, etc.) and the infrastructures to support such services must be integrated into the overall system design to provide adequate security. Due to the rapid evolution of information technologies, no security solutions will be permanent, but it is essential to develop a foundation on which further enhancements in ITS security can be developed.

3. *ITS executes two general types of processes:*

   Mission-Critical Processes *-- Functions such as traffic control and emergency response must operate continuously and the data exchanges involved cannot be delayed.*

   Delay-Tolerable Processes *-- Functions such as special event coordination information for use in strategic traffic planning can be rescheduled if processing or communications services are unavailable.*

   - Most ITS subsystems execute both mission-critical and delay-tolerable processes in performing their intended functions. Therefore, the following conditions must be satisfied:

     The software, hardware, data, and communications technologies involved must be available and operable to support the mission-critical processes.

     Appropriate security services must operate to ensure such processes' correct operation and performance.

     The proper system security management practices must be in place to ensure that unavailable systems are promptly made available again.

4. *Effective, efficient and secure ITS operations require properly trained personnel to manage and operate ITS subsystems. The use of proper security services (e.g., authentication, access control, auditing, etc.) to combat both internal and external threats require significant planning, design, and interoperability considerations. Employee training and awareness should be considered as supplements to, not substitutes for, automated security techniques.*

   - Management should address both intentional and accidental "insider" and "outsider" threats by means of proper authentication, access control and auditing mechanisms. Provide employee training to supplement these automated mechanisms. Consider using background checks for ITS personnel in critical positions.

5. *ITS relies on the collaborative operation of many individual subsystems. These subsystems, in turn, depend on communications technologies that are expected to operate without interruption, error, or delay. The denial-of-service impacts presented within this document illustrate the potential consequences of such dependencies when backup facilities are not provided.*

   - Develop contingency plans for backup, recovery, and degraded performance of ITS operations. Consider the use of both redundant systems and geographically and electronically diverse communications. Develop plans for ITS subsystem backup, recovery, "off-nominal"/crisis response, and down-time avoidance.

6. *The security assessments reveal that ITS uses four types of data, each of which needs to be adequately protected against unauthorized disclosure, manipulation and, in some* cases, *replay.*

   Mission-Related Data *-- Traffic management data, for example, are used to control traffic signals and variable message signs; the emergency management facilities use real-time traffic and vehicle-location information to respond to emergencies. This type of data has a critical sensitivity to manipulation.*

Personal and Private Information *-- Many ITS subsystem functions require the identities **of** vehicle drivers by their names, Social Security Numbers, credit-card IDS, and current locations. This type **of** data has a critical sensitivity to unauthorized disclosure.*

Control Information *-- Communications technologies require specific transactions to configure the proper connections between ITS subsystems. Additionally, traveler information software employs configuration options to display information in private or commercial vehicles. This type **of** data has a critical sensitivity to manipulation and replay.*

Summary and Statistical Data *-- Many ITS subsystems provide summaries **of** their operations **for** use by traffic planners in forecasting traffic and road conditions. The aggregated data is often more important to such planners than detailed or specific information. This type **of** data has a critical sensitivity to disclosure (business data) and replay.*

- Identify appropriate data types to allow the proper protection of information and to subsequently provide safe and secure ITS operations. Include the use of standard formats, metrics, and levels of protection for ITS data flows.

7. *The hardware and software comprising ITS subsystems should be interoperable. While open to flexibility, system designs (including any supporting communications infrastructures) should consider appropriate standards to aid interoperable, and therefore, more effective more efficient, and more secure ITS operations.*

   - Adopt existing standards (or if necessary establish new standards) to allow for subsystem interoperability and secure ITS operations. Consider the standards for infrastructures that may be needed to support these subsystems (e.g., the Public Key Infrastructure required for managing public encryption keys).

- **Continuation of ITS Information Security Activities**

1. *By identifying the range **of** potential threats (i.e., the threat categories) **for** the ITS subsystems, their supporting transportation infrastructure, and the information exchanged among these systems, the National ITS Architecture security analysis has established a basis **for** more complete and specific ITS information security needs. Some aspects **of** regional or local system designs/implementations will differ, but each should be able to use these assessment results **for** identifying initial needs and **for** continuing more comprehensive ITS security efforts*

   Future ITS information security activities should include the following:

   - Verifying the security assessments described and presented in this document. The verification process would not on only contribute to security awareness (along with participation in oversight activities), but it would also provide a basis for further and more detailed security efforts.

   - Conducting an information security assessment of a system that is currently implementing (or will be implementing) parts of the National ITS Architecture. Paper analyses provide numerous benefits, including the ability to make necessary corrections early in the design phase. However, to maximize benefits for those who will later build to an architecture (e.g., the National ITS Architecture), the analysis of an existing system would provide significant and realistic feedback.

SECTION 1

INTRODUCTION

Intelligent Transportation Systems (ITS) rely on a growing number of information technologies. The ITS industry's reliance on these technologies subsequently increases the information security threat within transportation systems. By understanding the objectives of a secure system, threats that may compromise those objectives, and services that counter those threats, the ITS community can develop an awareness of system dependencies (e.g., telecommunication networks) and systems vulnerabilities that threaten the operation of surface transportation systems (and potentially National Security). Subsequently, the ITS community can begin to develop appropriate security policies and implementation strategies for surface transportation systems.

1.1 PURPOSE

The objective of this task is to assess information security within the surface transportation domain and to provide transportation professionals with initiative for securing ITS information. Accordingly, this process involves developing an awareness of information security within the ITS community, and demonstrating the existence of ITS security threats.

As part of this task, three information security assessments have been performed to identify and characterize various threats to the ITS subsystems, their supporting communications infrastructure, and their exchange of information. The assessments also provide recommended solutions (i.e., security services) for reducing or eliminating such threats and protecting ITS.

1.2 SCOPE

Initially this document describes the objectives of a secure information system, identifies the security threats that could compromise those objectives, and discusses the different security services to counter those threats. In more detail, this document then focuses on the three information security assessments. The following assessments were based on the National ITS Architecture and comprise an integrated yet high-level analysis of ITS information security.

- ITS Subsystem Security Assessment: a detailed assessment identifying security threats to all of the subsystems defined in the National ITS Architecture and recommending the appropriate security services to counter identified threats

- ITS Communications Infrastructure Assessment: a high-level assessment identifying the security threats to the communications infrastructure that supports the operation of the ITS subsystems

- ITS Data Flow Security Assessment: a detailed assessment identifying security threats to all of the data flows (carried by the communications infrastructure) between ITS subsystems and other components and recommending the appropriate security services to counter identified threats

Due to the high-level nature of architecture analyses (in contrast to the more detailed analysis of a specific system design) the assessments were conducted in accordance with the following considerations:

- The threat analyses are based on identifiable threat categories (e.g., denial of service) and not on specific threats (e.g., theft, vandalism). Specific threats are discussed and related to appropriate threat categories.

- Recommended solutions are identified at the security service level allowing implementors the flexibility to select specific solutions (i.e., security mechanisms) for their particular application of the National ITS Architecture. Identifying specific security mechanisms to implement recommended services would have restricted system design flexibility or contradicted existing system designs.

- The National ITS Architecture defines the communications infrastructure in a generic fashion (e.g. "wireline" as opposed to a "dedicated Tl line", etc.), and therefore, the communications infrastructure assessment identifies threats and recommends services accordingly (i.e., based on "wireline", "wide-area wireless", etc. communications in general).

- The ITS data flow security assessment did not consider physical security (e.g., locks or guards to secure a facility), personnel security (e.g., background checks), or operational security (e.g., procedures for protecting an organization's sensitive activities) aspects. These aspects of security were not considered directly applicable to data flows. However, the ITS subsystem security assessment did make physical, personnel, and operational security considerations.

While primarily focusing on the noted security assessments, this document also provides necessary background information and a general understanding of information security (including security policy and security oversight activities). It addresses common information security issues as well as those that pertain specifically to ITS.

1.3 ORGANIZATION

This document is divided into five sections and six appendices:

- Section 2 provides a background of information security and its relation to ITS.
- Section 3 discusses the concept of information security (e.g., objectives, threats).
- Section 4 documents the assessment of the ITS subsystems and associates the analysis with the data flow and communications infrastructure assessments.
- Section 5 offers conclusions and recommendations.
- Appendix A documents the assessment of the ITS data flows.
- Appendix B documents the assessment of the ITS communications infrastructure.
- Appendix C provides supplemental information regarding policy documents.
- Appendix D exemplifies real-world information system attacks.
- Appendix E discusses information security mechanisms.
- Appendix F provides specific examples of implementing security services within ITS.

SECTION 2

BACKGROUND

For years, the highway transportation community sought to solve its problems primaily by building more roads. However, this approach alone is no longer sufficient. The industry must also optimally manage their resources to maximize efficiency. On 18 December 1991, President Bush signed the Intermodal Surface Transportation Efficiency Act (ISTEA) providing authorizations for highways, highway safety, and mass transportation for the next six years. Provisions for the years beyond FY 1997 will be decided by the next transportation authorization bill (referred to as NEXTEA).

The purpose of these acts is clearly depicted in their statement of policy, "... to develop a National Inter-modal Transportation System that is economically efficient, environmentally sound, provides the foundation for the Nation to compete in the global economy, and will move people and goods in an energy efficient manner." The ISTEA enabled the establishment of the ITS program, which seeks to apply information technologies to accomplish these goals.

To maximize the potential of ITS technologies, system design solutions need to provide coordinated and integrated operations, and to support interoperable equipment and services. The National ITS Architecture -- a product of the ITS program -- provides the guidance necessary to ensure system, product, and service interoperability without restricting the design options for ITS implementors.

This section focuses on the significance of securing information within ITS. With a knowledge of general information security issues, the policy or policies behind these issues, and how these issues relate to ITS information technologies, the reader will have a better understanding of the ITS information security assessments discussed in subsequent sections of this document.

2.1 GENERAL INFORMATION SECURITY ISSUES

The Information Age is enabled by information infrastructures that use advanced sensing, computing, and communications capabilities -- collectively referred to as information technologies. These information technologies appear in virtually every sector of the economy and are designed to facilitate the application of new financial, educational, environmental, health care, transportation, and personal services.

Secure and highly efficient information infrastructures are vital to the national security and economic growth of the U.S. since both the Government and private industry rely on these infrastructures for their day-to-day operations. The "National Security Strategy of Engagement and Enlargement," issued by the White House in February 1995, discusses the necessity of economic growth to U.S. national security. The document also recognizes that the information infrastructures facilitating this growth extend to many aspects of American society (e.g., finance, energy, transportation) but are vulnerable to accidental, environmental, or malicious attacks that could result in sustained outages and widespread disruption.

Transportation (or ITS) information infrastructures allow traveler information systems to collect and disseminate information on traffic conditions and transit schedules. Traffic management systems use these technologies to decrease congestion and traffic incidents.

Similar benefits and services are provided by information technologies for public transit systems, commercial vehicle subsystems, and emergency management systems. The loss or disruption of such services can have a wide range of consequences. For example, while those systems supporting traffic and emergency management functions have direct and significant impact on public safety, those systems supporting traveler information and commercial vehicle functions may have less impact on public safety but still affect the National economy.

As the availability and use of information technologies grow, so do the information infrastructures. The result is a shared communications infrastructure of resources that facilitate decentralized operations and the sharing of information. Public and private transportation organizations (e.g., state Departments of Transportation (DOT's)) may now connect internal private facilities to external public facilities; they may use public networks to create virtual private networks among geographically distributed departments or divisions; and they may allow the public to access their systems and services directly. However, along with the benefits of these shared infrastructures and these new technologies come new risks. Extensive interconnections within and between information infrastructures across the public and private sectors have further increased their vulnerability and have provided existing and potential adversaries with a means to jeopardize U.S. interests.

Although hackers, criminals, foreign enemies, or unauthorized users could disrupt the nation's transportation systems, these systems could just as easily be disrupted by a regional power failure, a natural disaster like a tornado or hurricane, or a telecommunications outage. Peter H. Daly, a Treasury Department expert in electronic commerce who was appointed to the President's Commission on Critical Infrastructure Protection in Summer 1996 states, "The probability of a major system failure sometime down the road, let's say in this next decade, at this point appears to be more likely from these interdependencies and unseen partnerships than from an attack" [American Banker, 1997].

On 6 March 1997, the Computer Security Institute (CSI) announced the results of its second annual "Computer Crime and Security Survey" that used questions submitted by the Federal Bureau of Investigation (FBI) International Computer Crime Squad's San Francisco office. Survey participants included security practitioners in a variety of U.S. corporations, government agencies, financial institutions, and universities. Survey results indicated that the number of organizations that experienced some form of intrusion or other unauthorized use of computer systems within the last 12 months rose from 42 percent in 1996 to 49 percent in 1997 [CSI, 1997]. Respondents reported a diverse array of attacks and revealed that they were being frequently probed from several locations-both internally and through remote dial-in and Internet connections. Disturbingly, over 50 percent of the respondents indicated that they still do not have a written policy on how to deal with network intrusions. Over 20 percent do not know if they have been attacked, and more than 82 percent of those who had experienced intrusions indicated that they did not report it to law enforcement -- due mostly to fears of negative publicity [CSI, 1997].

Public and private service providers have long been concerned about the tradeoffs allowing information systems to be accessible to all who need the information versus sufficiently securing the information and the information systems in which it resides. An environment that is open to everyone is not secure, while an environment that is closed to everyone is secure but not useful.

The need to protect against the vulnerabilities of an open environment is growing as rapidly as the technologies themselves. The increasing reliance on new technologies and

technology-enabled services suggests that organizations' future needs for information security will be significant. With the growing societal dependence on information infrastructures and their importance in meeting national economic and security interests, protecting these infrastructures has become essential.

2.2 INFORMATION SECURITY OVERSIGHT AND POLICY

Federal, state, and local governments and private industry rely heavily on information technologies to meet their individual, operational, and financial needs. Inadequately controlled or protected information systems can lead to the corruption, unauthorized disclosure, and/or theft of resources. Such actions can have serious consequences, including, for example, the inability to perform intended functions and provide required services (both critical and trivial); the waste, loss, misuse, or misappropriation of funds; the potential for legal and safety liabilities; and the loss of organizational credibility.

2.2.1 Federal Government Oversight

Until recently, the Federal Government paid little attention to researching and addressing the information security needs of the government and commercial sectors that do not process classified information. Currently, no organization or entity within the Federal government has the responsibility for promoting information security in the private sector or for coordinating information security efforts between government and non-government parties: the National Security Agency (NSA), for example, has primary responsibility for information security in the classified domain, while the National Institute of Standards and Technology (NIST) has authority for information security only in unclassified government information systems (occasionally the private sector adopts the Federal Information Processing Standards that NIST is responsible for setting). The Security Policy Board (SPB) does coordinate and recommend some Presidential directives for U.S. security policies, procedures, and practices, but only for government information. Other entities supported by the Federal government have some influence over information security, yet have little policy-making authority. These include:

- Computer Emergency Response Team (CERT)
- Information Infrastructure Task Force's (IITF) National Information Infrastructure Security Issues Forum
- Computer System Security and Privacy Advisory Board (CSSPAB)
- National Counterintelligence Center (NACIC)
- Private organizations (via membership in Government sponsored activities)

On 15 July 1996, President Clinton signed Executive Order 13010, "Critical Infrastructure **Protection,"** which established a commission to foster the protection of national infrastructures considered so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States. These critical infrastructures include, among others, electrical power systems, banking and finance, telecommunications, and transportation.

The mission of the President's Commission on Critical Infrastructure Protection includes assessing the vulnerabilities of, and threats to, these critical infrastructures; addressing the legal and policy issues regarding the protection of these infrastructures; and recommending a comprehensive national policy and implementation strategy for protecting these critical infrastructures. Threats to these critical infrastructures, as defined by the Commission,

include those to tangible property (i.e., physical threats) as well as those to the information or communications components that control the critical infrastructures (i.e., cyber threats).

While the Commission is conducting its analysis and until the President has an opportunity to consider and act on its recommendations, the Infrastructure Protection Task Force (IPTF), established within the Department of Justice and chaired by the Federal Bureau of Investigation, will undertake interim activities. Among their activities, the IPTF will utilize existing expertise (Federal and non-Federal) to coordinate the provision of expert guidance to critical infrastructures, and provide training and education on the methods of reducing the vulnerabilities of the these infrastructures.

The IPTF is not to be confused with the Information Assurance Task Force (IATF), one of two task forces overseen by the Presidents National Security Telecommunications Advisory Committee (NSTAC). [Note: the IATF was recently renamed the Information Infrastructure Group (IIG)]. President Reagan created the NSTAC by Executive Order 12382 in September 1982 to provide advice and information to the President and the Executive Branch regarding policy and enhancements to national security and emergency preparedness (NS/EP) telecommunications. The NSTAC established the IATF to serve as the focal point for identifying the potential impacts of new technologies on NS/EP telecommunications, and for assessing the information assurance threats to, and the vulnerabilities of, the information or communications components that control critical infrastructures. These include those infrastructures (e.g., banking and finance, and transportation) considered by the Commission on Critical Infrastructure Protection. The National Communication System (NCS) Office of Information Assurance is working with the NSTAC IATF (now the NSTAC IIG) to obtain these objectives.

Additionally, and more specifically, activities from the National Science and Technology Council (NSTC) Transportation Research and Development Committee are currently focused on investigating information security within the transportation domain. As such activities continue to probe transportation-related security, and as ITS continues to incorporate emerging information technologies and to become more dependent on various information infrastructures, it becomes increasingly important for the U.S. Department of Transportation (DOT) to consider Federal guidance on information security. (See appendix C for a listing of information security policy documents for Federal systems as well as for privacy policy documents and guidance for ITS systems.)

2.2.2 State and Local Government and the Private Sector

A security policy indicates the set of high-level rules governing how sensitive or critical information within an organization is protected. Potential ITS security policies or governing security documents should take into account the Federal Government's guidance on providing appropriate information security for ITS. However, ITS will be implemented by state and local governments as well as by privately owned companies, and policy will most likely be derived from state/local **or** private Information Resource Management (IRM) plans. Efficient, economical, and cooperative plans developed by state and local transportation agencies would parallel Federal guidance.

Although few state or local transportation organizations have official policies on security, they are (or will be) required to comply with state IRM policies and are encouraged to follow IRM guidance regarding the security of their systems. For example, the IRM plan for the state of Texas is intended to assist in the implementation of an adequate security program to protect the automated information resources within the various agencies of the Texas state government (including transportation). The security standards and policy are to be considered as required procedures and controls to be implemented as part of any Texas

government agency's information security program. The state's optional guidelines are meant to assist agencies in the interpretation and implementation of the standards and are recommended as effective security practices. Each state agency is encouraged to evaluate the policy, standards, and guidelines to determine whether more stringent requirements are necessary given the individual agency's authority and function.

The content of security policies and their enforcement practices in the private sector cover a broad spectrum. Security policies can range from virtually non-existent to various degrees of enforcement. At the weaker end, companies &at do have a security policy do not always enforce it or keep it current and are often susceptible to various threats. Companies with stronger security enforcement use either a combination of internal security protections (e.g., strict access control) and external protections (e.g., firewalls) -- a proactive approach; or they implement stringent auditing of user activity -- a reactive approach.

Because many information infrastructure components are owned and operated by the private sector, it is essential that the Government and private sector work together to develop a strategy for protecting these components and ensuring their continued operation. In the case of transportation, there is no regulatory mandate for a Federal agency such as the DOT to intervene or direct private companies to take specific security precautions, nor is there any requirement for the DOT to react in the case of an attempt at unauthorized access to a private transportation system. However, the Federal government can promote awareness among the private sector by making private companies aware of the potential vulnerabilities and costs of such incidents and the advantages of taking prudent precautions.

The adequate protection of information from various threats is only slowly becoming a realization within the surface transportation community. Through ITS America, the industry has pursued privacy issues by developing a set of "Fair Information and Privacy Principles." While not addressing information security as a whole, these principles were prepared in recognition of the importance of protecting individual privacy within ITS. They have been adopted by ITS America in draft final form and are intended to educate and guide transportation professionals, policy makers, and the public as they develop guidelines for specific ITS projects.

2.3 RELATING SECURITY ISSUES AND POLICY TO ITS

To achieve the goals of the ISTEA, the ITS program developed a set of user services (e.g., Travel and Transportation Management) based upon anticipated benefits for various ITS users. The services are in various stages of maturity, and a few will require significant research and development before they can be deployed. The provision of these services will depend on various transportation information systems. In turn, these systems rely on the growing number of information technologies and the further development of a transportation infrastructure that are potentially vulnerable to many information security threats.

With an awareness and general understanding of information security issues, one can comprehend the potential threats to a secure ITS environment. Furthermore, one can place into context the present oversight activities and the developing policy and guidance (both general and transportation specific) for the protection of vulnerable information. Collectively, this information develops a background for the following ITS information security needs assessments.

SECTION 3

INFORMATION SECURITY OVERVIEW

This section presents an overview of information security components fundamental to the information security assessment process. This process involves a high-level analysis of information security components that include:

- Objectives required to secure a system
- Threats that could undermine the objectives
- Security services to counter these threats

Figure 3-l depicts the major components comprising the security assessments. Note that the components presented here are not all inclusive. This section is not intended as a tutorial encompassing all aspects of information security; rather it is to acquaint the reader with the security components used in this specific assessment. Section 4, Subsystem Security Assessment, appendix A, ITS Data Flow Security Assessment, and appendix B, Communications Infrastructure Assessment, address the particular ITS security threats and services.

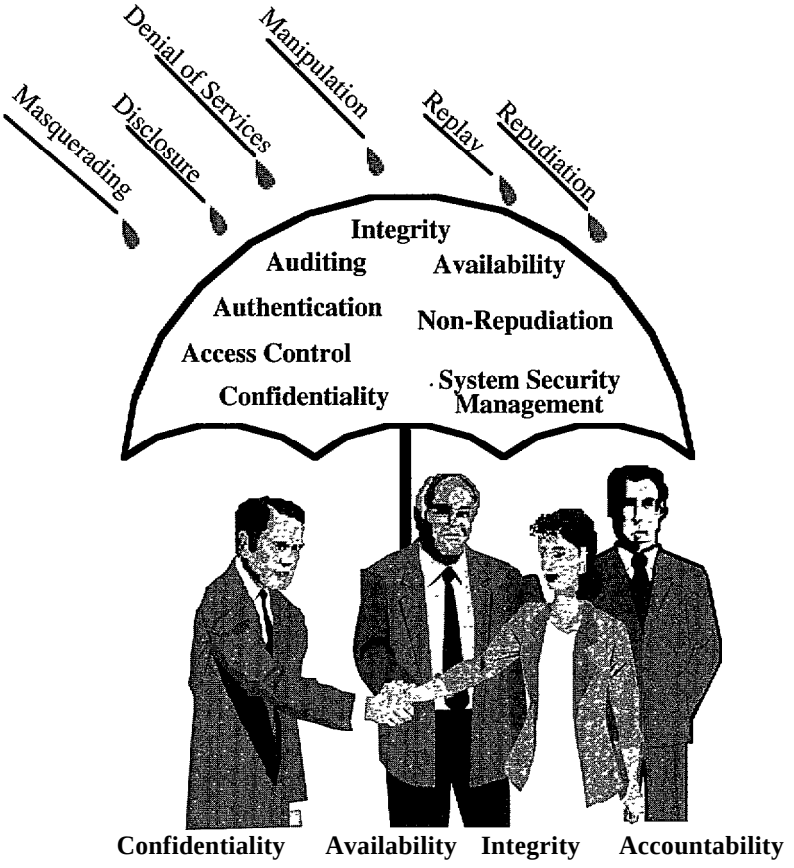


Figure 3-l. ITS Information Security Assessment Components

3.1 OBJECTIVES

In protecting any automated information system, there are four primary objectives: confidentiality, integrity, availability, and accountability. Often a security policy will contain the objectives or goals of a system.

- Confidentiality: ensuring that the data and system are not disclosed to unauthorized individuals, processes, or systems (e.g., protecting trucking company records).
- Integrity: ensures that the data is preserved in regard to its meaning, completeness, consistency, intended use, and correlation to its representation (e.g., providing accurate toll collection transactions). Also the ability to ensure that the system is preserved to perform its intended function in a sound manner and is protected from deliberate or inadvertent modification.
- Availability: ensuring that the data and system are accessible and usable to authorized individuals and/or processes (e.g., guaranteeing emergency vehicles timely incident data)
- Accountability: ensuring that transactions are recorded so that events may be recreated and traced to users or processes. This includes not only what was done (e.g., a payment for traveler services was made), but also who did it (i.e., who made the payment). In automated information systems, the objective accountability is usually achieved by use of auditing, which ties actions to the entities performing the action at a specific time.

Meeting and maintaining these objectives effectively minimizes the risk of corruption, unauthorized disclosures, theft of resources, legal and safety liabilities, financial loss, and loss of organizational credibility.

3.2 THREAT CATEGORIES

A threat is any circumstance or event that has the potential to cause harm to a system. Specific threats to which any system is exposed fall into three categories: natural disaster, accidental, and intentional. Specific threats are discussed in section 3.3. The specific threats to the confidentiality, integrity, availability, and accountability of ITS are categorized as those causing denial of service, disclosure, manipulation, masquerading, replay, and repudiation. These six threat categories are applicable to most automated information systems and represent the various potential impacts of the individual and specific threats identified in section 3.3. As noted in section 2.1, the 1997 CSI/FBI survey reported a diverse array of attacks. Understanding the applicable threat categories affected by these attacks provides a basis for understanding the security services to counter the threats. Due to the high-level nature of an architectural assessment, as opposed to the more detailed assessment of a specific system implementation, analysis is based on identifiable threat categories (as opposed to specific threats). Threat category identification is used in the three ITS security assessments. Figure 3-2 illustrates security threat categories as they relate to ITS. The following subsections describe each of the noted threat categories with examples as depicted in figure 3-2.

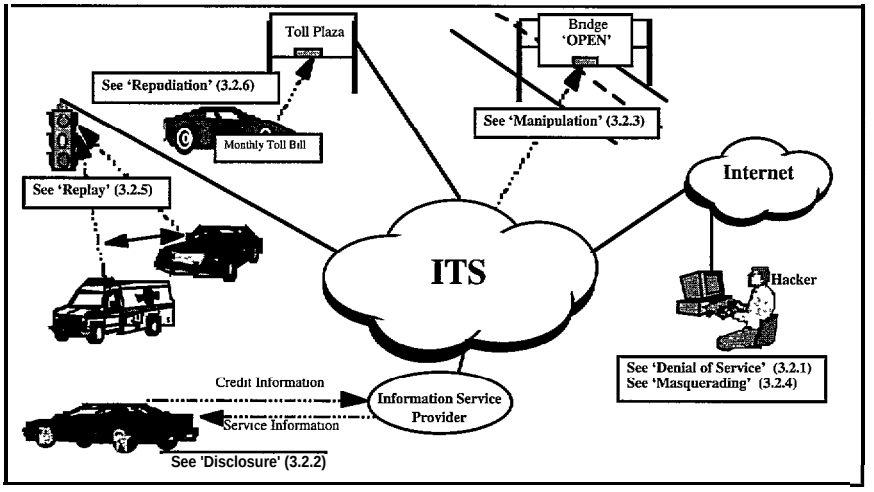


Figure 3-2. Threat Categories and ITS Operations

3.2.1 Denial of Service

Denial of service pertains to any action or series of actions that prevent any part of a system from functioning as intended. Preventing a system or subsystem from functioning properly threatens system availability. Denial of service threats consist of intentional, accidental, or natural events, and they can take on many forms and can target particular parts of a system. Traditional attacks involve the introduction of malicious code that causes the system to perform unauthorized functions and/or become unavailable to authorized users. Other forms of attack range from modification of system resources to flooding attacks that render part or all of the system unavailable. Natural disaster threats such as earthquakes and tornadoes can also cause denial of service.

A scenario relevant to the National ITS Architecture might involve a hacker bombarding an ITS subsystem with message traffic. Such action potentially prevents authorized and sometimes critical messages from passing through to the intended system (e.g., messages from an emergency vehicle to an emergency management facility).

3.2.2 Disclosure

Disclosure is the acquisition of sensitive (e.g., personal, financial) information through unauthorized channels such as users, processes, or other systems. Disclosure threats consist of intentional or accidental events. Disclosure impacts the confidentiality of information and subsequently impacts privacy -- a fundamental personal or organizational expectation. As noted earlier in section 2.1, personal privacy is one of the most highly visible security issues facing ITS. As databases of personal information from ITS systems grow, a wide variety of organizations may begin proposing secondary uses for the information. Consequently, any information that identifies a traveler with locations, services, etc. must be protected against disclosure.

The information contained in and exchanged between mobile ITS users and their information service providers exemplify one of many opportunities for disclosing information within ITS. However, through actions like the "Driver's Privacy Protection Act of 1994" and the "Fair Information and Privacy Principles", the ITS community has

attempted to prohibit unnecessary disclosure and to protect the personal privacy of licensed drivers and users of ITS.

3.2.3 Manipulation

Manipulation involves the modification of system information whether being processed, stored, or transmitted. It can include the removal or replacement of information or the resequencing of data to produce unauthorized effects. Manipulation threats consist of intentional, accidental, or natural events that jeopardize the integrity of a system.

In the ITS domain, manipulation might involve the modification of roadway data to display inappropriate or incorrect information (e.g., indicate that a bridge is "open" while just the opposite is true). Other examples might include falsifying financial information, incorrectly indicating payment for transit services, or manipulating "hazardous materials" information such that it now reflects safe and non-hazardous materials onboard a commercial vehicle.

3.2.4 Masquerading

Masquerading is the attempt by an unauthorized user or process to gain access to a system by posing as an authorized entity. If successful, the unauthorized entity could then obtain access to other information and processes that would normally be unobtainable. Masquerading threats consist of intentional or accidental events.

Within ITS, masquerading might involve an unauthorized user (e.g., hacker) who illegally gains access to a variable message sign (VMS) through dial-up lines, the Public Switched Telephone Network (PSTN), or the Internet. The masquerader may now have the ability to create or modify roadway data as indicated above. Another example may involve unauthorized users gaining access to personal traveler information at an information service provider facility or obtaining access to service and payment data at one of several other ITS locations.

3.2.5 Replay

Replay is the re-transmission of valid messages under invalid circumstances to produce unauthorized effects. Depending upon the messages or actions reproduced, replay can have a severe impact on the integrity of a system. Replay threats consist of intentional or accidental events. A common occurrence of replay involves the theft of a message that is later used to execute the same series of actions.

In the ITS domain, replay might involve the illegal capture of information used to control traffic signals in emergency situations. These messages might later be replayed by the thief eager to reach his/her destination and subsequently endanger other commuters relying on accurate signaling. Another example involves the capture and replay of a traveler's credit identity so as to associate that traveler with a toll or parking service charge rather than the one who "stole" the information.

3.2.6 Repudiation

Repudiation is the successful denial of an action. Repudiation allows either the sender or receiver to deny the action occurred. This typically affects the integrity of the system and applies to all types of electronic transactions. Repudiation threats consist of intentional or accidental events.

Within ITS, threats of repudiation are present when using the automated toll collection facilities. Using the automated toll payment scheme without the proper security safeguards, a traveler could deny traveling through a particular automated toll plaza and refute the debit to his account. Using an older manual method at the toll plaza, a traveler could request a receipt at the time of the transaction thus proving that the toll was paid. In some current implementations of the automated toll plaza, such as the EZ-Pass system in Florida, travelers using a form of credit payment receive a monthly or quarterly itemized statement. This form of receipt, although provided to the traveler after the fact, constitutes a means for preventing repudiation.

3.3 SPECIFIC THREATS

The threat categories in the previous section represent the various impacts of individual and specific threats. Since each specific threat may have numerous impacts, it may be associated with more than one threat category. The associations of specific threats with threat categories are illustrated in table 3-l (Note: specific threat definitions are from [CSI, 1993]. Theoretically, individual specific threats may indirectly affect threat categories other than those identified in this table. However, only the direct and most applicable threat/threat category associations have been identified.

Table 3-1. Threat/Threat Category Associations

Threat Categories / Specific Threats	Denial of Service	Disclosure	Manipulation	Masquerading	Replay	Repudiation
Natural Disaster Threats						
Acts of Nature	X					
Accidental Threats						
Accidental Disclosure		X				
Configuration Error	X	X	X			
Electrical Disturbance	X		X		X	
Electrical Interruption	X					
Environmental Failure	X					
Fire	X					
Hardware Failure	X		X		X	
Liquid Leakage	X					
Operator/User Error	X	X	X	X		X
Resource Consumption	X					
Software Error	X	X	X	X	X	X
Telecommunciations Interruption	X		X		X	
Intentional Threats						
Alteration of Data	X	X	X	X	X	X
Alteration of Software	X	X	X	X	X	X
Bomb Threat	X					
Eavesdropping		X				
Employee Sabotage	X		X			
Enemy Overrun	X	X	X			
Fraud			X	X	X	X
Intentional Disclosure		X		X		
Resource Consumption	X					
Riot/Civil Disorder	X	X	X			
Strike	X	X	X	X		
Terrorism	X	X	X			
Theft	X	X	X			
Unauthorized Use	X	X	X	X	X	X
Vandalism	X	X	X			

As illustrated in table 3-1, there are three general types of specific threats to which any system is exposed: natural disaster, accidental, and intentional. Among the accidental and intentional, threats stem from two **sources** -- insiders and outsiders.

Insider attacks range from accidental file deletions by system administrators or users to deliberate system reconfiguration or data theft/destruction/modification by disgruntled employees. Because insiders have greater access to an organization's information systems, they were previously considered to be a more significant threat to the security. However, survey responses indicate the conventional wisdom that most information security problems are internal is no longer true [CSI, 1997]. The threat from within has not diminished, but the threat from the outside has risen dramatically due to Internet usage. Now, slightly less than half of the respondents to the 1997 CSI/FBI survey indicated that security incidents were a result of insider activity [CSI, 1997]. Meanwhile, outsider attacks might include: someone who gains credentials to appear as an insider; hackers who attempt to access systems through the Internet or dial-up services (sometimes only for the "challenge"); former employees who still have active system accounts; and thieves or information brokers hired by competitors, terrorists, or foreign governments.

The specific threats to which ITS may be exposed are described in the following sections. Some examples of real world information system attacks are provided in appendix D.

3.3.1 Natural Disaster or Acts of Nature Threats

Acts of nature include earthquake, flood, hurricane, landslide, lightning, sandstorm, snow and ice, tornado, tsunami, volcanic eruption, and windstorm. All of these acts of nature can cause a denial of service; however, they are difficult to counteract or prevent and are inevitable in many geographical areas.

3.3.2 Accidental Threats

Accidental threats are considered unintentional acts or events that can cause harm to a system. For the purpose of this assessment, these threats are identified and defined as follows:

- **Accidental Disclosure:** an unauthorized or premature accidental release of proprietary, financial, personal or otherwise sensitive information.
- **Configuration Error:** includes the improper configuration of hardware, software, communication equipment, or operational environment.
- **Electrical Disturbance:** a momentary fluctuation in the electrical power source consisting of either a voltage surge (peak), voltage dip, or interruption of less than one half hour.
- **Electrical Interruption:** a long term disruption in the electrical power source, usually greater than one half hour.
- **Environmental Failure:** an interruption in the supply of controlled environmental support provided to the data processing operations (e.g., air quality, air conditioning, humidity, heating and water).
- **Fire:** an incident affecting data processing either through heat, smoke, or suppression agent (e.g., sprinklers, Halon, fire extinguishers, etc.) damage.
- **Hardware Failure:** a unit or component failure sufficient enough to cause delays in processing or loss of operations.

- **Liquid Leakage:** an incident involving liquid from sources other than floods (e.g., burst or leaking pipes, discharge of sprinklers).
- **Operator/User Error:** an improper or otherwise ill-chosen act by an employee that results in processing delays, equipment damage, or lost or modified data.
- **Resource Consumption:** any use of computer resources (e.g., processing time, storage capacity) that results in partial or complete loss of available system resources.
- **Software Error:** any extraneous or erroneous data in the operating system or application programs that result in processing errors, data output errors, or processing delays.
- **Telecommunications Interruption:** any unit or component failure sufficient to cause interruptions in the telecommunications between computer terminals, remote or distributed processors, and host computing facilities.

3.3.3 Intentional Threats

Intentional threats are considered deliberate acts or events with the intent of causing harm to a system. For the purpose of this assessment, these threats are identified and defined as follows:

Alteration of Data: an intentional modification, insertion, deletion of data -- by authorized or unauthorized user -- that compromises the data produced, processed, controlled, or stored by the processing system.

Alteration of Software: an intentional modification, insertion, or deletion of operating system or application system programs -- by authorized or unauthorized user -- that compromises the data, programs, system, or resources controlled by the system. This includes malicious code such as logic bombs, Trojan horses, trapdoors, and viruses.

- **Bomb Threat:** a notification -- true or false -- of the existence of an explosive device at a facility.
- **Eavesdropping:** a deliberate act of listening to communications between two or more parties without authorization or consent.
- **Employee Sabotage:** a deliberate action taken by an employee, group of employees, or non-employees working together with an employee to disrupt organizational operation.
- **Enemy Overrun:** a forceful occupation of an activity or facility by those with intentions detrimental to government or organization bodies.
- **Fraud:** a deliberate unauthorized manipulation of hardware, software, firmware, or data with the intent of financial gain for the perpetrator.
- **Intentional Disclosure:** an unauthorized or premature intentional release of proprietary, financial, personal, or otherwise sensitive information.
- **Resource Consumption:** any use of computer resources, including processing time or storage capacity, which results in deliberate partial or complete loss of available system resources.
- **Riot/Civil Disorder:** a group at unrest -- organized or unorganized -- that causes widespread and uncontrollable suspension of law and social order.
- **Strike:** an organized employee action -- union or non-union, legal or illegal -- designed to halt or disrupt normal business operations.

- **Terrorism:** a deliberate and violent action taken by employees or non-employees whose motive goes beyond the act of sabotage and towards an extremist political statement.
- **Theft:** the unauthorized appropriation of hardware, software, firmware, storage media, data processing equipment, or sensitive data.
- **Unauthorized Use:** an unauthorized use of computer equipment or programs. This includes browsing files and using resources for personal use.
- **Vandalism:** the malicious and motiveless destruction or defacement of property.

3.4 SECURITY SERVICES

As noted in section 3.2, the high-level nature of an architecture assessment suggests deriving recommended security services from identifiable threat categories (as opposed to specific threats). Threat category identification is used in the security assessments reported in this document. Once the threat categories have been ascertained, the applicable security services necessary to counter those threats can be determined. Security services are those protections that are commonly provided to ensure secure operations of a system and fulfill the confidentiality, integrity, availability, and accountability objectives. Security services are implemented by various techniques, commonly referred to as security mechanisms. While information security threats cannot be eliminated through the use of any single tool, the proper application of information security services will help maintain the confidentiality, integrity, availability, and accountability of transmitted and/or stored information.

Information security services fall into eight categories: authentication, confidentiality, integrity, non-repudiation, access control, auditing (to achieve accountability), availability, and system security management. Note that while section 4, ITS Subsystem Security Assessment, calls upon all of these services; appendix A, ITS Data Flow Assessment, will reference only the authentication, integrity, confidentiality, and non-repudiation services (those most appropriate for data flow or information exchange). Also note that four of the security services (confidentiality, integrity, availability, and accountability) are also objectives of a secure system. The objective of accountability in information systems is achieved by the audit function that allows tracing specific events to the specific entities that initiated those events at a specific time.

Table 3-2 indicates the relationships between the six threat categories and the eight applicable security service protections. However, it does not reflect any indirect relationships between threat categories and services. For example, if a user's password is disclosed (the primary threat), it could lead to manipulation, denial of service, and/or masquerading attacks (the secondary or indirect threats). For the purposes of this assessment, confidentiality -- the protection that thwarts disclosure -- does not reflect the protections used to guard against manipulation, denial of service, and masquerading threats. To indicate all possible relationships between threat categories and security services goes beyond the purpose of this section.

Section 4 and appendix A indicate which of the security services are required for each ITS subsystem and each ITS data flow respectively. Using both tables 3-l and 3-2, the reader can map a specific threat to the required security services needed to counter or minimize the impact of a threat attack. Appendix E contains information regarding the mechanisms and techniques for implementing these security services.

Table 3-2. ITS Threat Category and Security Service Mapping

Security Services / Security Threats	Authentication	Confidentiality	Integrity	Non-Repudiation	Access Control	Auditing	Availability	System Security Management
Denial of Service					X		X	X
Disclosure		X			X			X
Manipulation			X		X	X		X
Masquerading	X							
Replay	X							
Repudiation				X				

3.4.1 Authentication

Authentication is the means of verifying the identity of users of other entities (e.g., process, external systems) prior to granting access to a requested resource. Authentication specifically counters the threat of masquerading. Typically, a user identifies himself or herself to the system, then authenticated his/her identity by providing a second piece of information that is known only by the user. Authentication can be implemented in varying degrees of strength. Other security services such as access control and audit depend on user authentication, since they vase their decisions on the user's identity. A system process typically has a predefined process ID that indicates the validity of the process. Likewise, external systems interfacing with another system will require a predefined system ID.

Using tables 3-1 and 3-2, any specific threat associated with either the masquerading or replay threat category will require authentication security services(s). For example, the prevention of masquerading due to operator/user errors will require some form of authentication.

Without user authentication, there can be no individual access control or accountability,. For example, perhaps an information service provider supports public-access data that is hosted on a web server. Public information on the web server is intended to be read-only information, such as transportation routes. However, to access other information on the web server, the customer must have a valid user ID and password (or other authentication mechanism). This provides identity as a basis for access control and accountability. For the public-access sections of the web server there is no access control granularity; access is "yes" or "no". Accountability would only be at the level of origin address (i.e., the IP address of the customer) for public access.

The need for authentication at the data flow level is illustrated by the "emergency vehicle driver inputs" data flow between the Emergency Vehicle Subsystem (EVS) and the Emergency Management Subsystem (EM) (described in sections 4.4.2 and 4.2.2 respectively). This data flow contains specific incident information so the emergency management facilities can direct an appropriate response. It also contains routing details so

that traffic management facilities might enable a “green wave” for the emergency vehicle(s). Authentication that this message is coming from a valid emergency vehicle subsystem is critical to ensure accurate, timely, and appropriate emergency response.

3.4.2 Integrity

Integrity is noted as one of the objectives in protecting any automated information system. It is also a security service used to support information accuracy and thus minimize the threat of manipulation. Information integrity plays an important role in highly distributed systems (i.e., a mesh of system components/applications) such as those within ITS. Basic integrity services (e.g., error-detection/error-correction) are inherently provided by the lower layers of many current communication protocols; however, in certain situations additional integrity mechanisms are required. Data flows such as those involving financial transactions or emergency-related incidents often require more information integrity than is provided by the protocols.

Using tables 3-l and 3-2, any specific threat associated with the manipulation threat category will require integrity security service(s). For example, preventing or minimizing manipulation due to sabotage requires some form of integrity.

An ITS subsystem example in which integrity is required is in the distribution of software. For example, if a user downloads an ITS program onto his personal computer, or executes a Java applet from an ITS web site, the user needs a way to ensure that the program or applet has not been modified or infected with a virus. One way to do this is with integrity mechanisms such as cryptographic checksums or digital signatures. If the program is altered, the checksum or signature will no longer be valid.

A particular ITS data flow that requires additional integrity is “fare and payment status”. This data flow between the Transit Vehicle Subsystem (TRVS) and the Transit Management Subsystem (TRMS) (described in sections 4.4.3 and 4.2.9 respectively) may comprise a request for payment processing as well as a confirmation of payment, data about advanced fares and tolls, and fare collection violation information (i.e., personal information on potential transit violators). This data flow highlights the necessity for providing sound and accurate information (i.e., information integrity). It not only contains important financial information, but also distinguishing personal information -- both of which should be valid.

3.4.3 Confidentiality

Confidentiality, like integrity, is identified as one of the objectives in protecting any automated information system. It is also a security service used to support that objective and counter the threat of disclosure. Given that privacy is a highly visible issue within today’s society, confidentiality services -- which may help provide privacy -- are frequently required. For example, the increasing number of electronic transactions referencing a user’s identity and associated personal information will undoubtedly require some form of protection.

Using tables 3- 1 and 3-2, any specific threat associated with the disclosure threat category will require confidentiality security service(s). For example, the prevention of disclosure due to a system configuration error will require some form of confidentiality.

Two ITS subsystems where confidentiality is required are Emergency Management (EM) and Freight and Fleet Management (FMS) (described in section 4.2.4). For example, if a

snooper was able to obtain sufficient information to masquerade as one of these subsystems, freight or emergency vehicles could be rerouted. Another likely occurrence would be drug dealers gaining information and then masquerading as a legitimate commercial carrier. Freight vehicles could be sent to an ambush location. Emergency vehicles could be stolen and used to commit crimes. Likewise, a trucking firm could snoop data processed/stored in an FMS and learn company trade practices or travel routes of other competitors.

The "traveler information request" data flow and its "traveler information" response between the Vehicle Subsystem (VS) and the Information Service Provider Subsystem (ISP) (described in sections 4.4.4 and 4.2.5 respectively) are ITS data flows that require confidentiality. These contain information on traveler routing plans, financial transactions, credit identity, credit value, and consumer interests. The significant quantity of personal information in either of these data flows clearly identifies the need for confidentiality. Other data flow requirements may have only a fraction of the personal or financial information, yet most would require the same level of confidentiality.

3.4.4 Non-Repudiation

Non-repudiation guarantees that the source of a transmission cannot later deny sending the transmission and that a receiver cannot deny receiving a transmission. Threats to this security service are countered by using non-repudiation mechanisms. In the paper-transaction world, examples of non-repudiation mechanisms include official receipts and notarized signatures. In the automated world, non-repudiation mechanisms include digital signatures with signed protocol acknowledgments -- the electronic equivalent of a hand-written signature or a signed record of receipt.

Using tables 3-l and 3-2, any specific threat associated with the repudiation threat category will require non-repudiation security service(s). For example, the prevention of repudiation due to fraud will require some form of non-repudiation.

An example of a subsystem that needs non-repudiation is the Personal Information Access Subsystem (PIAS) (described in section 4.5.1). The traveler could request services and not pay for them, or pay for them (with a credit card) and later have the charges reversed by denying that the services were received. Because the Information Service Provider (ISP) subsystem provides so many services to travelers, often for a fee, it will require non-repudiation services as well.

Among the ITS data flows, most non-repudiation needs center around financial transactions. In particular, the ITS data flow "transaction status" that provides rideshare, digital map, and other service payment confirmation from a financial institution to the ISP will require some form of non-repudiation.

3.4.5 Access Control

Access control limits the resources of a system to only those users, programs, processes, and other systems that are properly authorized. Access control builds on authentication and helps to ensure confidentiality, integrity, availability, and accountability. After authenticating an entity, further restriction of system access minimizes exposure to information or resources that could lead to disclosure, modification, and/or denial of service.

Access control applies to the data flow controlling software (i.e., the processes in the subsystem) and not directly to the data flows or external messages transmitted between subsystems and terminators. For this reason, access control is appropriate within the subsystem security assessment discussion, yet not within the data flow security assessment discussion. Access control should be implemented in some form within each ITS subsystem. Using tables 3-l and 3-2, any specific threat associated with the denial of service, disclosure, or manipulation threat categories will require access control security service(s).

Within all ITS subsystems, software modifications and upgrades should be subject to access controls. These access controls will prevent unauthorized modification of software, either intentionally or by accident. To prevent unauthorized modifications, an operating system may selectively allow read, write, or execute privileges.

3.4.6 Auditing

The accountability objective can be achieved through auditing and policies (e.g., if an employee accesses data for which he/she is not authorized, then the employee may be terminated). Auditing is used to trace activities of a system user -- typically done by associating an event with a specific user. Examples of user/event activities include system login, resource accessing, and device reconfiguration. Auditing is usually accomplished through system or application audit trails. In order to ensure that the accountability of a system is maintained, audit trails must be protected from unauthorized modifications. Generally, only the system or application is permitted to alter the audit trail files, and only authorized auditors (and backup processes) are permitted to read them.

Auditing helps to maintain the integrity of the system; however, it is a reactive process. An audit trail captures system activity as it happens, but it does not prevent the activities **from** occurring. If users are aware of the system auditing process, they may be deterred from misusing system resources.

Like access control, auditing applies more to the data-flow-controlling process than to the data flow. The controlling process can record transactions and alert administrators to unauthorized activity. However, the vastness of ITS subsystems may create large and complex audit trails, so audit reduction facilities should be incorporated to minimize the amount of information recorded. Using tables 3-l and 3-2, any specific threat associated with the manipulation threat category will require auditing security service(s).

Auditing can be used to detect unauthorized updates to software modules. For example, suppose a programmer on the Remote Traveler Support (RTS) subsystem accidentally replaced a module in the Roadway Subsystem (RS). If updates were logged and reviewed, the reviewer could observe that the programmer had made a mistake and take corrective action.

3.4.7 Availability

The availability security service protects against denial of service attacks. To ensure system availability, one should consider using system, data, and communications back-ups; protecting and restricting ITS subsystem access; and protecting system configurations. Availability mechanisms are not directly applicable to individual data flows; however, their implementation at the data-flow-controlling process level is important in ensuring that ITS messages are transmitted and received as required. Using tables 3-l and 3-2, any specific

threat associated with the denial of service threat category will require availability security service(s).

Critical ITS communications facilities require backup mechanisms. For example, if wireline communications are down, perhaps cellular or wide area wireless communications could be used. Less time-critical facilities could be protected with time-delay backups. For example, servers that take orders for map information might suffer a disk drive failure. Restoring recent backups to a new disk drive and bringing it online would provide delayed access to the map-ordering facilities.

3.4.8 System Security Management

Systems security management is the means of providing security controls throughout the system life-cycle. This security service is typically implemented by a combination of physical, manual, and automated controls. This includes the definition, implementation, and enforcement of the following:

- Security policies and procedures
- Roles and responsibilities
- System configuration
- Operational security
- Personnel security
- Physical security

As ITS is deployed, the opportunities to exploit system vulnerabilities increase, and organizational systems security management becomes a necessity. Using tables 3-l and 3-2, any specific threat associated with the denial of service, disclosure, or manipulation threat categories will require system security management.

One example of systems security management is the assignment of user IDS and privileges. Another example is having policy that states users be given access to the services and files that they need for their jobs, and nothing more. Nowhere is this more important than the configuration management of systems such as web servers. Only authorized users should be allowed the privileges of a system administrator. This is controlled on a user by user basis. Accidentally assigning system administrator privileges to the wrong person, or allowing any user to change the web server's configuration, could result in denial of service, disclosure of private or proprietary information, or destruction of data.

System configuration management provides the means for ensuring that all aspects of the system are configured to provide an effective, efficient, and secure operating environment. For ITS, system configuration would involve not only the internal ITS subsystem interfaces, but also the interfaces with non-ITS entities (e.g., terminators). Interfaces should be designed and implemented such that each specific interface has minimal and closely controlled functionality in providing system access. Using tables 3-l and 3-2, any specific threat associated with the denial of service, disclosure, or manipulation threat categories will require (and should have) system configuration security service(s).

Accidental configuration errors could be as harmful as intentional configuration changes. For example, suppose a fleet manager misconfigures enrollment data or incorrectly transcribes the enrollment information for one driver to the application of another driver. When requesting tag information for a particular enrolled commercial vehicle, an operator at the Commercial Vehicle Check Subsystem (CVCS) could receive incorrect information or potentially no enrollment data at all.

SECTION 4

ITS SUBSYSTEM SECURITY ASSESSMENT

This ITS information security analysis comprised three assessments to identify and characterize the various threats to (1) the ITS subsystems, (2) their exchange of information, and (3) their supporting communications infrastructure. Used as a basis to document the findings of the analysis, the ITS subsystem assessment references the two other assessments: a high-level security assessment of the ITS communications infrastructure and a detailed security assessment of the data flows using that infrastructure. Since the conduct and results of each assessment complemented the other two, an integrated and more complete analysis of the ITS National Architecture resulted (figure 4-2).

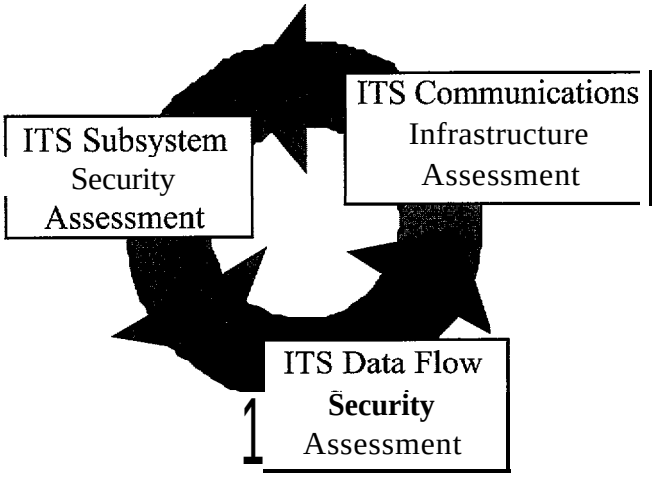


Figure 4-1. ITS Security Analysis Approach

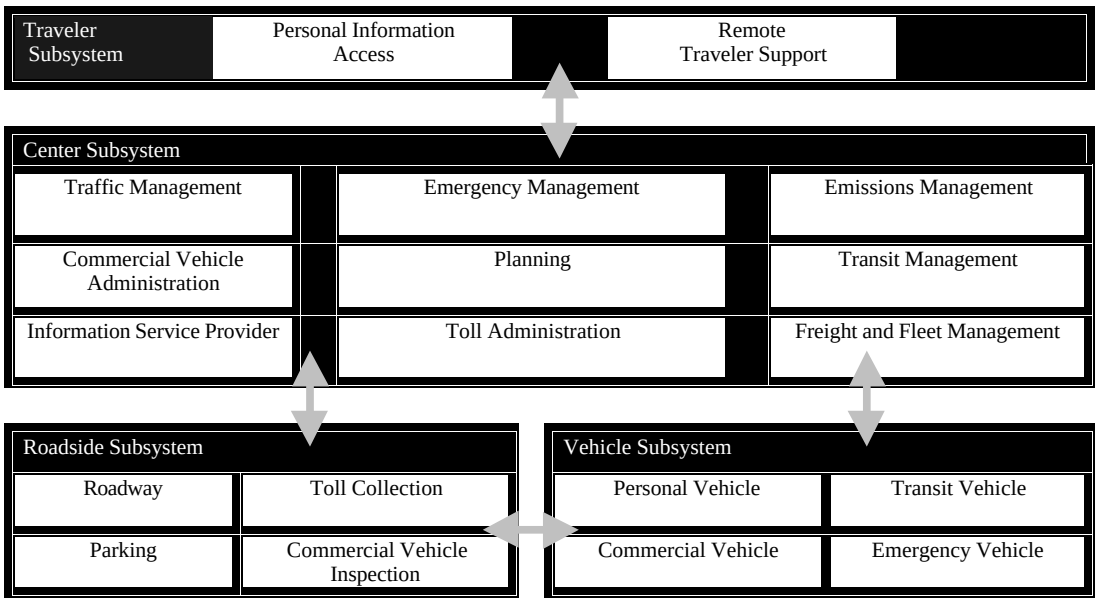
While appendices A and B respectively document the data flow and the communications infrastructure assessments, Mitretek describes the ITS subsystem security assessment here. First the approach and methodology are described; then, the findings of the subsystem assessment (including impacts on ITS operations and references to/from the other assessments); and finally, a brief discussion of the applicable security services.

4.1 APPROACH AND MEHTODOLOGY

The National ITS Architecture provides, a common structure for the design of ITS. It consists of several documents (e.g., logical architecture, physical architecture, implementation strategy, etc) that define a framework from which various design approached can be developed. However, the National ITS Architecture is not a systems design.

The logical architecture document presents a functional view of 30 interrelated ITS user services. These are defined as part of the ITS National program planning process an dare designed to provide for travelers, traffic management operators, transit operators, commercial vehicle owners and operators, state and local governments, etc.

The physical architecture document identifies four types of subsystems: traveler, center, roadside, and vehicle. These subsystem types comprise nineteen particular ITS subsystems. In more detail, the physical architecture then describes each of these subsystems, as well as terminators—other subsystems (e.g., DMV) and users (emergency vehicle driver) related to surface transportation operations. Figure 4.1 illustrates ITS subsystem relations.



Source: National ITS Architecture

4-2. ITS Architecture Subsystem Relations

The physical architecture also describes the exchange of information among ITS subsystems and terminators (i.e., data flows). Along with the communications infrastructure, the subsystem operations and their related data flows support the logical architecture functions and hence provide the ITS user services. Therefore, a broad ITS security analysis originates from the ITS subsystem assessment.

To assess the security of the ITS subsystems, the following activities were performed:

- Reviewed the National ITS Architecture in its hardcopy, World-Wide Web, and Compact Disk-Read Only Memory (CD-ROM) versions
- Identified each subsystem's major functions, inputs, outputs, and data communications services
- Identified the other ITS subsystems and terminators (i.e., non-ITS sources and destinations) with which the subsystem exchanges information or on which the subsystem depends for the information
- Examined the ITS data flows and the results of the data-flow analyses (Appendix A) to clarify information exchanged between subsystems and terminators
- Examined the ITS communications infrastructure (Appendix B) to determine impacts of losing planned communications technologies and services
- Determined the importance of the information exchanges to the operations of the particular subsystem, other ITS subsystems, and ITS in general
- Developed scenarios to determine the impacts of the 6 threat categories (discussed in section 3.2) on the operations of the subsystem

Sections 4.2 through 4.5 discuss the ITS subsystems by type (i.e., center, roadside, vehicle, or traveler). For each subsystem, there is a description of major functions and a discussion of potential impacts on these functions as a result of the following categories of threats:

- Denial of Service
- Disclosure of sensitive information (e.g., name, credit-card number, current location)
- Manipulation
- Masquerading
- Replay
- Repudiation

The data flow assessment acknowledges that all ITS data flows are subject to denial of service attacks.

The approach to documenting this analysis included illustrating various threats and their potential impacts on ITS. With ITS is in its infancy and few large-scale deployments of ITS, broader and more encompassing security-related incidents are rare. Incident scenarios used throughout this document illustrate what might often seem to be minor inconveniences of little or no consequence to particular public agencies, private corporations, or the general public. Although significant and costly on an individual basis, the many specific scenarios might tend to obscure or undermine a greater issue.

ITS was established to develop a National transportation infrastructure that is economically efficient and environmentally sound, provides the foundation for the Nation to compete in the global economy, and moves people and goods in a safe and energy efficient manner. Either a major security-related incident (e.g., the destruction of an entire ITS facility) or a gradual system deterioration from an aggregate of individual security-related incidents could lead to a complete collapse of ITS services. Such extensive losses compromise ITS objectives and would have significant impact on how the general public conducts their day-to-day lives and operations.

The broader impact of such occurrences is easier to comprehend by recalling just some the many ITS benefits that might be lost:

- Improved Safety -- Using a real-time traffic adaptive freeway control system, the Minnesota Department of Transportation has decreased its accident rate by 25 percent and improved response times to incidents by 20 minutes.

- Reduced Traffic Congestion -- FAST-TRAC, a project consisting of adaptive signal control, automated traffic monitoring and other ITS technologies, has increased vehicle speeds by 19 percent during peak hours in Oakland County, Michigan.

- Improved Public Transportation -- The Winston-Salem Transit Authority reports that its Automatic Vehicle Location (AVL) system has decreased paratransit passenger waiting time by 50 percent.

- Reduced Commercial Spending -- The commercial and public sector fleets provide a variety of economic benefits from ITS, and retailers reduce inventory and overhead costs with "just-in-time" delivery improved by ITS applications.

- Reduced Government Spending -- The ADVANTAGE I-75 project, which allows properly-equipped commercial vehicles to travel the I-75 corridor with minimal stoppage, cut weigh station operating costs by up to $160,000 annually; electronic credentials checking and safety inspections save another $4.5 to $9.3 million annually.

- Reduced Pollution -- An independent environmental firm studying the impacts of Oklahoma's PIKEPASS automatic toll system found that cars and trucks using PIKEPASS lanes emitted up to 30% less pollution than those vehicles operating in the manned toll lanes.

The possibility and potential consequences of losing these ITS benefits -- benefits that the public has become accustomed to -- should not be overlooked while reviewing some of the finer details and specific security-related scenarios addressed in this document.

For each subsystem, a figure is provided to illustrate the other ITS subsystems and terminators with which the subsystem interacts, as well as a sampling of the significant types of information exchanged. Figure 4-3 describes the symbols used in such figures.

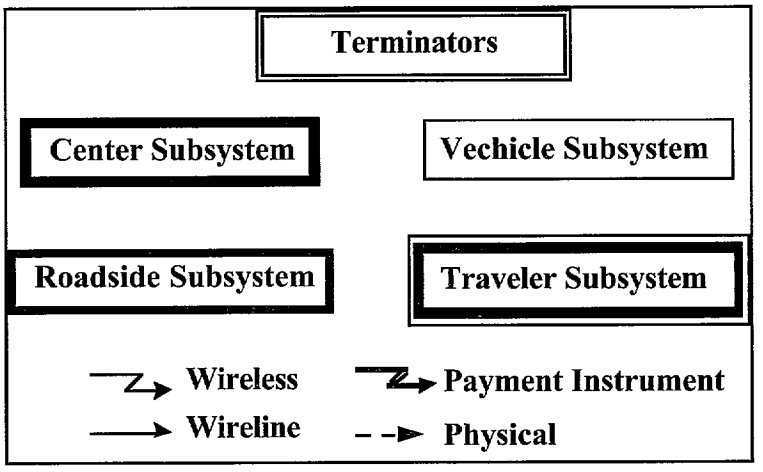


Figure 4-3. Symbology Used in Subsystem Data Flow Figures

4.2 CENTER SUBSYSTEMS

Center subsystems deal with those functions normally assigned to public/private administrative, management, or planning agencies. This section describes the nine ITS center subsystems.

4.2.1 Commercial Vehicle Administration Subsystem

The Commercial Vehicle Administration Subsystem (CVAS) is a center subsystem that operates at one or more fixed locations in a region; the CVAS may be managed by a branch or section of a state's division of licensing, motor vehicles, or taxation. Data communications between the CVAS and the other ITS subsystems and terminators are via wireline communications. While the ITS architecture design links the CVAS to other center subsystems over a public or private wireline network, its connections to other subsystems and terminators (e.g., roadside check facilities) may be through leased or owned twisted-wire pairs, coaxial cable, or fiber optics.

The CVAS performs the following commercial vehicle management functions:

- Issue and maintain credentials information for commercial-vehicle operators, drivers, and vehicles
- Collect fuel taxes, weight/distance taxes, and other fees associated with commercial vehicle operations within the state or region

- Issue hazardous material (HAZMAT) and oversize/overweight permits
- Exchange information with commercial-vehicle roadside checkstation facilities
  - Safety check results and violations
  - Accident information
  - International border crossing clearances
- Exchange credentials and credentials violation information with enforcement agencies and other CVAS entities
- Provide statistical summaries to the Planning Subsystem
- Collect carrier safety ratings from government agencies
- Respond to queries from authorized parties regarding credentials, safety, international-border, and payment information

Figure 4-4 illustrates associated ITS subsystems and terminators and provides exemplary data flows. Tables A-la and A-lb contain the analyses for all CVAS data flows.

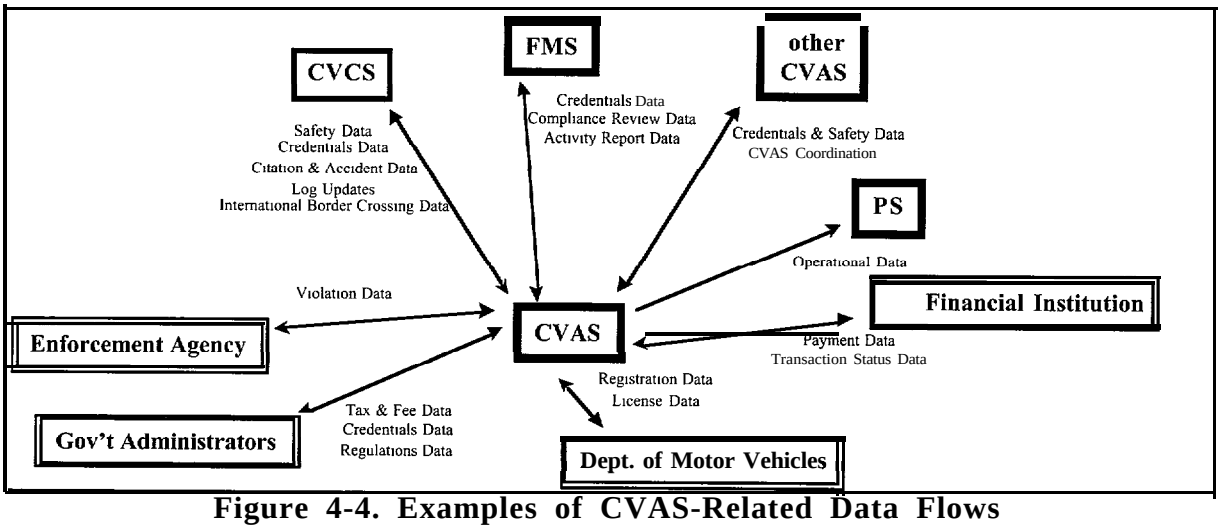


Figure 4-4. Examples of CVAS-Related Data Flows

- **Impact of Denial of Service**

  CVAS operations can be delayed, prevented, or mishandled in several ways.

  Absent or Inoperable CVAS Devices. If the CVAS computer system is inoperable due to system errors, maintenance, or repairs, all of the computer systems at the roadside checkstations could neither access the CVAS for credentials and safety information nor transmit their inspection results to the CVAS.

Absent, Inaccessible, or Unreadable Data. A CVAS computer system error could make the information that it contains unreadable. Depending on the backup-and-recovery procedures followed at both the CVAS computer system site and the roadside checkstations, the CVAS information may not be the most current. Without the most current information, roadside inspectors might have to perform more time-consuming manual inspections.

Absent or Unexecutable Software. If the CVAS software is accidentally or intentionally deleted, roadside inspectors could not automatically verify credential and safety information for the commercial drivers that stop at or pass through their stations. Obtaining such information directly from the drivers would cause delays; if the information were incorrect, drivers with violations or safety problems could be permitted to pass.

Wireline Communications Loss. The CVAS depends on fixed wireline communications for all of its interfaces with other ITS subsystems and terminators. Therefore, CVAS functions could be delayed or prevented if the computer systems involved cannot connect to the wireline, or if the wireline itself has been disabled (e.g., a leased line or cable has been cut), or if other wireline operating conditions occur (e.g., network saturation) (see paragraph B.2.1). For regularly scheduled transmissions (such as the transfer of daily roadside checkstation logs to the centrally located CVAS), delays of up to a few hours could be tolerated and the transmission rescheduled after the problem has been solved.

The loss of wireline communications between a roadside checkstation and the CVAS would prohibit the exchange of roadside inspection data. Without the most current information from the CVAS, more time-consuming manual inspections would have to be performed. Such inspections would cause delays at the roadside checkstation as well as the connecting highways and arterial roadways. Furthermore, unsafe vehicles or commercial vehicle operators with violations could be passed through.

A loss of wireline communications between the CVAS and a financial institution could delay or prevent the institution's prompt payment of taxes and fees for the operators, drivers, and/or vehicles. With the CVAS databases indicating no payments, roadside checkstations' queries would reflect erroneous information and thus cause inspection delays.

A loss of wireline communications between the CVAS and government agencies could delay or prevent the CVAS's receipt of carrier safety ratings. Such a loss could also prevent the government agencies' receipt of quarterly roadside facility activity reports from the CVAS. Without the safety ratings, inspections could be delayed and unsafe vehicles might go unrecognized.

- **Impact of Disclosure**

CVAS may use public or private wide-area or local-area networks. Hackers are known to penetrate computer systems using these types of communications. As noted in the data

flow assessment (see tables A-la and A-lb), sensitive information such as the credentials, citation, and accident data stored in the CVAS could be disclosed if the subsystem is attacked.

- **Impact of Manipulation**

  Wireline users who have obtained access to the CVAS databases could modify the information to reflect incorrect enrollment information, inspection results, or violations information. Depending on the CVAS computer system's auditing capabilities, such modifications might go undetected.

- **Impact. of Masquerading**

  An unauthorized user who has gained access to the CVAS database may have done so by masquerading as an authorized user. Data identified in the data flow analysis as requiring additional integrity during transmission will require similar protection while in storage. Depending on the authorized user's access privileges, the masquerader may be limited regarding the specific data that he or she can read, copy, or modify. However, if the unauthorized user is masquerading as a database administrator or the computer system administrator, he or she could read, copy, or modify significant information (e.g., database definitions and user privileges, computer-system configuration files and ID/password records). With such information, the masquerader could make the CVAS computer system and software inoperable or make its information inaccessible, unreadable, or incorrect.

  As noted in the data flow assessment, all data exchanged between CVAS and other subsystems or terminators are subject to masquerade attacks. Authentication is required for all subsystem interaction (e.g., user, external data exchange).

- **Impact of Replay**

  Users who have obtained access to routers, switches, or other network interfaces associated with CVAS wireline communications may be able to intercept and copy messages exchanged between the CVAS and the roadside inspection stations. To make a particular roadside checkstation's computer system inaccessible to others, such users could bombard the computer system by continually replaying messages previously sent to the roadside checkstation (see table A-la).

- **Impact of Repudiation**

  Tables A-la and A-lb indicate the specific CVAS transactions subject to repudiation. Depending on whether and to what extent the credentials-related transactions of a commercial vehicle driver and the CVAS are verified (e.g., driver signature) and logged, commercial vehicle drivers could deny the enrollment and safety information currently on record for them. Determining which information is correct could delay inspections.

4.2.2 Emergency Management Subsystem

The Emergency Management (EM) subsystem is a center subsystem that creates, stores and utilizes emergency response plans to facilitate coordinated responses among various emergency centers. The primary mission of this subsystem is to support public safety through emergency organizations such as the police, fire fighters, search-and-rescue detachments, and HAZMAT response teams.

The EM uses real-time traffic and vehicle location information to further aid in the dispatch of emergency vehicles and crews. The EM also allows emergency vehicles to invoke a "green wave" capability that controls the traffic flow on the route used by the emergency vehicle. This subsystem also interacts with the Traffic Management and Transit Management Subsystems to facilitate its response to major emergencies. The EM subsystem communicates with the various subsystems and terminators using wide-area wireless and wireline communications.

The EM performs the following functions:

- Communicate emergency status to travelers, emergency vehicles, and other relevant entities, such as the media, 911 calls, and traffic management
- Provide an interface for the emergency operator and vehicle drivers
- Receive emergency incident information from the automated mayday messages and 9 11 calls originating from a vehicle or a traveler
- Acknowledge requests for emergency assistance from a traveler, vehicle, or emergency operator
- Determine incident response needs
- Communicate with commercial fleet managers to assess HAZMAT information for vehicles involved in or near an incident scene
- Manage the allocation of emergency services
- Assess response status based upon emergency vehicle locations and available emergency vehicles
- Dispatch emergency vehicles to an incident and provide known details on the incident to emergency vehicle drivers and crews
- Request emergency vehicle routing
- Enable "green wave" capability for the emergency vehicles
- Update digitized map data used for route planning

- Track emergency vehicles responding to an incident

Figure 4-5 illustrates associated ITS subsystems and terminators and provides exemplary data flows. Tables A-4a and A-4b contain the analyses for all EM data flows.

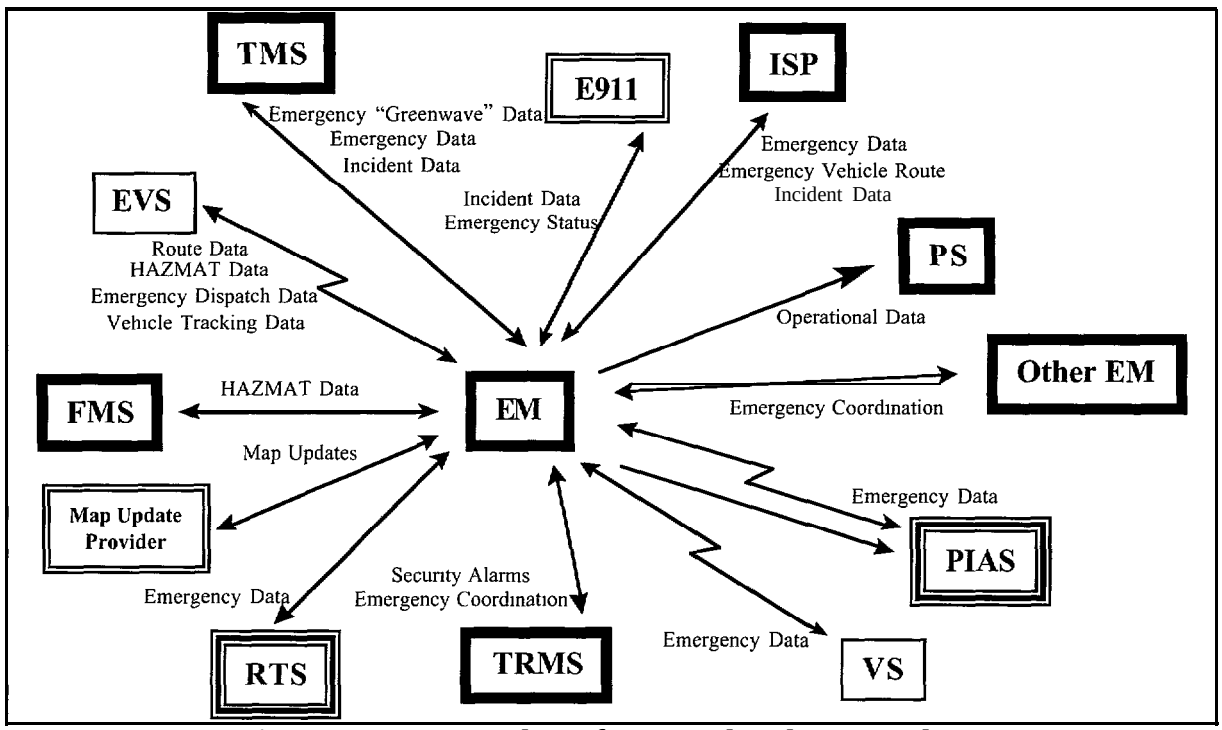


Figure 4-5. Examples of EM-Related Data Flows

- **Impact of Denial of Service**

  EM operations can be delayed, prevented, or mishandled in several ways.

  Absent or Inoperable EM Devices. If the EM computer system is inoperable due to system errors, repairs, or a power outage, it might not be able to exchange information with the ITS subsystems and other parties (e.g., 911 operators) until the problem is solved.

  Absent, Inaccessible, or Unreadable Data. An EM computer system error or a data storage error could make the EM's set of automated responses unreadable or inaccessible. If automated back-up copies of the responses are not immediately available, EM personnel would have to resort to following the hardcopy versions of the plans and responses, and manually performing the actions usually accomplished automatically. Such operations would delay EM's emergency responses.

  Absent or Unexecutable Software. If the EM's emergency vehicle tracking and monitoring software is inoperable or has programming errors, EM personnel might select

the wrong vehicles and personnel to respond to an emergency or provide a route that does not take into account the latest traffic conditions. Such operations would delay or prevent EM's emergency responses.

Loss of Wireline Communications. The loss of the EM's wireline communications would remove its ability to provide route planning and coordinated response. For example, if the EM could not receive HAZMAT information from the Freight and Fleet Management Subsystem (FMS) the emergency vehicle driver and crew may arrive at the incident and expose themselves and others to unsafe or hazardous conditions. Without the HAZMAT information, the emergency response crew may not know that they need to evacuate area communities. In some incidents the actions of the emergency vehicle crew could result in an escalation of the incident due to the improper handling of the HAZMAT situation.

Loss of Wide-Area Wireless Communications. A loss in the wireless communications will impact critical request and response transmissions between the EM and the emergency vehicles.

- **Impact of Disclosure**

Although no personal, financial or organizationally sensitive information is being transmitted, the EM is still subject to threats of disclosure, such as eavesdropping (see appendix B). An eavesdropper's ability to "listen to" the information provides the ability to capture and potentially modify or replay the information. These threats are discussed in more detail below.

- **Impact of Manipulation**

Tables A-4a and A-4b show that the majority of emergency data is subject to manipulation attacks. Since it is possible for someone to eavesdrop and capture the emergency-related information transmitted across either the wide-area wireless or the wireline communications systems used by the EM, the eavesdropper could also manipulate emergency data being transmitted. Such manipulations could cause emergency vehicles to be re-routed or false information to be provided to emergency vehicle drivers.

- **Impact of Masquerading**

The data flow assessment reflects that there is also the potential for an individual to masquerade as an emergency vehicle driver or other emergency service employee and provide false or misleading information.

- **Impact of Replay**

If an individual can eavesdrop and capture information during transmission, he or she could also replay it -- with or without making modifications to it. Continuous replay of messages could congest the system. The time and effort needed to distinguish the original emergency-related messages from the replayed ones could cause inappropriate or delayed

response. However, a determination was made during the data flow analysis to allow replay of messages as modeled after the 911 call system. This places the burden of detection replayed messages on the 911 system, but it does so in the interest of not missing a real request.

- **Impact of Repudiation**

  As noted in table A-4a, emergency acknowledgments from the EM are susceptible to repudiation attacks. Travelers could potentially hold responsible parties liable for not responding to their emergency requests.

4.2.3 Emissions Management Subsystem

The Emissions Management Subsystem (EMMS) is a center subsystem that monitors and manages pollution levels from vehicle emissions. Through the use of individual vehicle sensors and roadside sensors, this subsystem provides air quality managers with the ability to monitor and manage air quality for a particular geographical region. For each geographical region, the emissions are measured and the information collected is processed and used to identify areas exceeding safe pollution levels. For areas with unsafe pollution levels, notification is made to traffic management which implements strategies intended to reduce emissions in and around the problem areas. The emissions data of individual vehicles, which are collected by the roadside sensors as part of the Roadway Subsystem, are also processed and monitored to identify the vehicles that exceed the state's or region's standards. The EMMS uses wireline and wide-area wireless communications.

The EMMS performs the following functions:

- Obtain emission and pollution levels from vehicle and roadside sensors in a particular geographical region
- Receive environmental data (weather conditions such as snow, ice, fog, humidity) from roadside sensors
- Process emission data to identify vehicles and areas which exceed safe pollution levels
- Notify the Traffic Management Subsystem (TMS) and traffic operations personnel of current (and potentially unsafe) pollution levels at particular geographical regions
- Provide traffic operations personnel with the ability to access and update the pollution reference data used to determine unsafe pollution levels
- Provide the Roadway Subsystem with the vehicle emission criteria
- Record pollution levels and data in a log for use by other subsystems
- Provide pollution data logs to the Planning Subsystem for future planning

- Request an updated, digitized map of the geographical region with the pollution levels indicated

Figure 4-6 illustrates associated ITS subsystems and terminators and provides exemplary data flows. Tables A-5a and A-5b contain the analyses for all EMMS data flows.

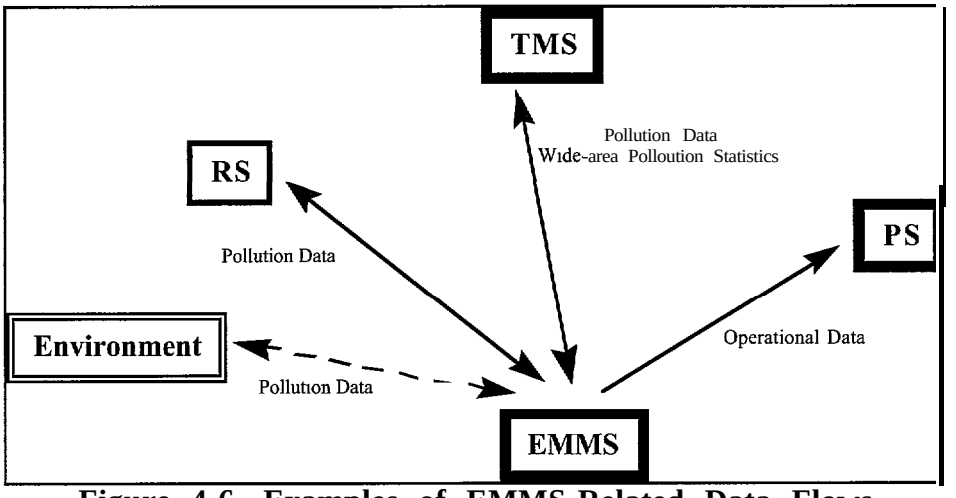


Figure 4-6. Examples of EMMS-Related Data Flows

- **Impact of Denial of Service**

  EMMS operations can be delayed, prevented, or mishandled in several ways.

  Absent or Inoperable EMMS Devices. If a roadside sensor that captures vehicle emissions data is inoperable, no emissions data will be collected by that sensor. If the sensor is at a location where a large volume of vehicles pass, the data loss could cause the pollution levels in the area to go under-reported.

  Absent, Inaccessible, or Unreadable Data. A computer virus could make the pollution data logs stored at the EMMS computer site unreadable. Depending on the EMMS backup-and-recovery procedures, the data logs that are available may not be the most current. The unavailable information could delay the EMMS pollution reduction activities and plans.

  Absent or Unexecutable Software. If the EMMS software that reads the sensor data has been damaged or deleted (either accidentally or intentionally), then the emissions measurements for a state or region could not be calculated and the vehicles that exceed the state's or region's pollution standards could not be identified.

  Loss of Wireline and Wireless Communications. If either communications service is lost, the pollution data cannot be transmitted to other subsystems for monitoring, mapping, or planning activities. The impact of this loss of service will potentially affect the

safe levels of pollution, and the EMMS may not be able to inform other ITS subsystems or the individual traveler of heavy or unsafe pollution areas.

- **Impact of Disclosure**

  The data flow assessment indicates that none of the EMMS data flows are subject to disclosure (i.e., they do not contain sensitive data).

- **Impact of Manipulation**

  The manipulation of pollution data through accidental or intentional means can cause incorrect pollution data to be processed. Acceptable pollution and emissions criteria levels could be modified. Therefore, unsafe levels would not be identified. This could place travelers or residents of the affected areas at risk.

- **Impact of Masquerading**

  As noted in tables A-5a and A-5b, all EMMS transmissions are susceptible to masquerade attack. Vehicle sensors could be modified or cloned to transmit acceptable emissions data and unsafe vehicles could masquerade as "safe" vehicles. Such masquerading threatens the integrity of the system and the validity of the pollution data used for planning and traffic management.

- **Impact of Replay**

  Since emissions data are primarily transmitted over wireline paths and consist of non-sensitive emissions data, the data flow analysis concluded that the impact of a replay attack on the EMMS is low.

- **Impact of Repudiation**

  There is little threat of repudiation for the EMMS (see tables A-5a and A-5b).

4.2.4 Freight and Fleet Management Subsystem

The Fleet and Freight Management Subsystem (FMS) is a center subsystem that manages commercial vehicles and the transport of their cargoes. This includes monitoring and tracking cargo and vehicle locations, and cooperating with non-commercial vehicle shippers (e.g., air freight and rail services) to ensure that the commercial-vehicle legs of intermodal shipments move safely and promptly. The FMS also provides several administrative capabilities, including the electronic enrollment of commercial vehicles, drivers and operators for their particular routes, the electronic filing of trip reports, and the generation of activity reports and fleet maintenance information. The FMS uses wireline communications to exchange information with the Emergency Management and Commercial Vehicle Administration subsystems, as well as the route-generation process/provider. The FMS uses wide-area wireless communications with the vehicle's Commercial Vehicle Subsystem (CVS).

The FMS performs the following functions:

- Provide activity reports of vehicles to commercial vehicle managers periodically or when required
- Allow fleet managers to do the following:
  - Schedule fleet maintenance and verify that the maintenance work was performed
  - Monitor the safety of commercial vehicle drivers
  - Retrieve commercial vehicles' on-board data processed from sensor inputs
  - File trip reports electronically
  - Purchase ITS credentials electronically
  - Track HAZMAT cargoes
  - Respond to EM requests for HAZMAT information
- Allow commercial vehicle managers to do the following:
  - Enter the carrier, driver and vehicle data into commercial vehicles' on-board tags
  - Read the tags of commercial vehicles
  - Retrieve vehicle routing information, and vehicle and cargo locations
  - Pay for electronic credentials and tax filings
  - Generate static routes for vehicles
  - Provide driver instructions
- Provide routing information to commercial vehicle drivers
- Allow roadside checkstation inspectors to retrieve and check commercial vehicles' electronic credentials data

Figure 4-7 illustrates associated ITS subsystems and terminators and provides exemplary data flows. Tables A-7a and A-7b contain the analyses for all FMS data flows.

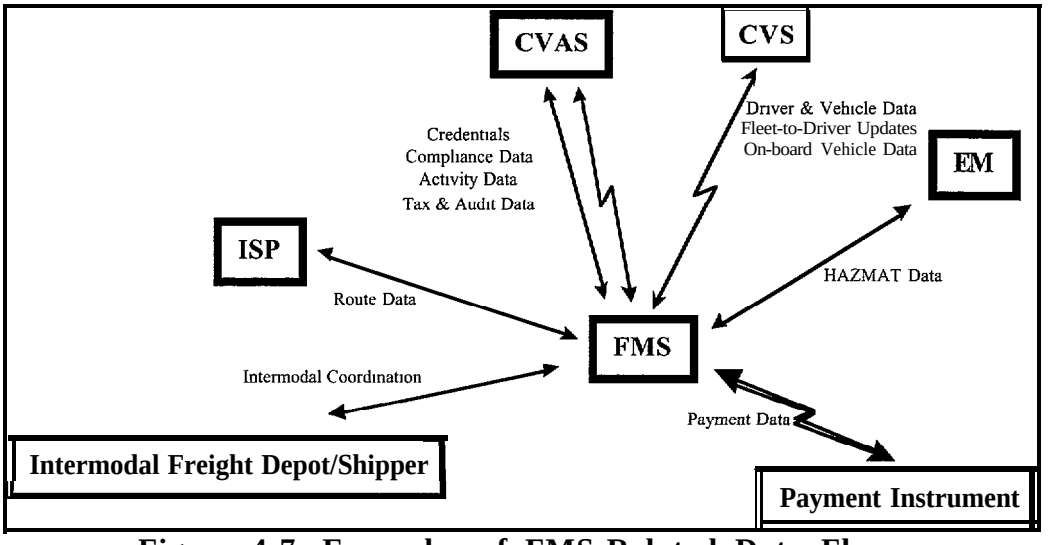


Figure 4-7. Examples of FMS-Related Data Flows

- **Impact of Denial of Service**

  FMS operations can be delayed, prevented, or mishandled in several ways.

  Absent or Inoperable FMS Devices. If the commercial vehicle's on-board processor(s) or sensors are absent due to repair or accident, fleet managers would not be able to retrieve the information read from the vehicle's sensors. Therefore, they would not be able to monitor the vehicle's and driver's safety.

  Absent, Inaccessible, or Unreadable Data. A virus attack on the FMS computer system could make the HAZMAT information that it stores and manages unreadable. Without the most current and correct HAZMAT information, fleet managers could not assist the EM in managing commercial vehicles carrying hazardous cargoes in the vicinity of an accident.

  Absent or Unexecutable Software. If the FMS software that processes and sends credentials applications to the CVAS cannot be executed, commercial vehicles and drivers would be delayed in getting their electronic credentials. Commercial vehicles would be forced to undergo manual inspections at the roadside checkstations.

  Loss of Wireline Communications. If the wireline communications between the FMS and EM were lost, EM could not access the FMS computer system for information regarding HAZMAT carriers in the vicinity of an accident.

Loss of Wide-Area Wireless Communications. If the wide-area wireless communications between the fleet manager and the commercial vehicle were lost, the fleet manager would not be able to track and monitor the commercial vehicles in his **or** her jurisdiction.

- **Impact of Disclosure**

  As noted in tables A-7a and A-7b, since the FMS computer system(s) contain sensitive data, the majority of FMS data exchanges are subject to threats of disclosure. If an unauthorized user gains access to the credentials information in the FMS computer system (e.g., information identifying how the applicant will pay for his or her credentials), the user could use the information to charge other items against the applicant's account. These data require protection in storage as well as during transmission.

- **Impact of Manipulation**

  A disgruntled employee with access to the FMS tax filings database could modify commercial vehicle operators' accounts to reflect that taxes have not been paid or that more taxes are due. Depending on the particular state's rules for paying taxes, such modifications could prevent or delay commercial vehicle operators from obtaining their ITS credentials.

  The data flow assessment indicates that similar financial and safety transmissions are subject to manipulation attack. As indicated in tables A-7a and A-7b, these data flows require additional integrity protection beyond that provided by the transmission protocol. Similar integrity protections should be applied to these data while in storage.

- **Impact of Masquerading**

  Tables A-7a and A-7b reflect the significance of the masquerade threat to FMS data and operations. One with access to the FMS's wide-area wireless communications service could masquerade as a fleet manager to read on-board commercial vehicle databases containing proprietary route, safety, and sensor information. With such information, masqueraders could attempt to hijack the vehicle and/or detain the driver(s).

- **Impact of Replay**

  The FMS is subject to replay attacks; specifically, data exchanges over wireless interconnects (see tables A-7a and A-7b). The impact to on-board safety and credential data is a significant public safety concern.

- **Impact** of **Repudiation**

  As noted in tables A-7a and A-7b, specific driver and vehicle information exchanged between the FMS and the commercial vehicle are subject to repudiation attacks. Unless messages received from fleet managers are logged on-board the commercial vehicle, commercial vehicle drivers could deny receiving any new instruction.

4.2.5 Information Service Provider

The Information Service Provider (ISP) is a center subsystem that provides an informational infrastructure to connect providers with consumers, and to gather the market information needed to assist in maintaining and planning service improvements.

The ISP collects, processes, stores, and disseminates traveler information to subscribers and the public at large. The information available includes:

- Basic advisories, such as weather and local event information
- Real-time traffic conditions, including speed, congestion and construction locations
- Real-time transit schedule and parking information
- Yellow pages information
- Ride matching information

The ISP broadcasts some information to travelers, such as road conditions and traffic advisories. In addition, travelers may obtain specific information by submitting requests for directions or route plans. ISP calculates the route, then returns the calculated plans to the user. The traveler may obtain the information through the Personal Information Access Subsystem, the Remote Traveler Support Subsystem, and various Vehicle Subsystems via wireline, basic one-way (broadcast), and personalized two-way communications. Reservation services are also provided in advanced implementations.

Figure 4-8 illustrates associated ITS subsystems and terminators and provides exemplarv data flows. Tables A-8a and A-8b contain the analyses for all ISP data flows.

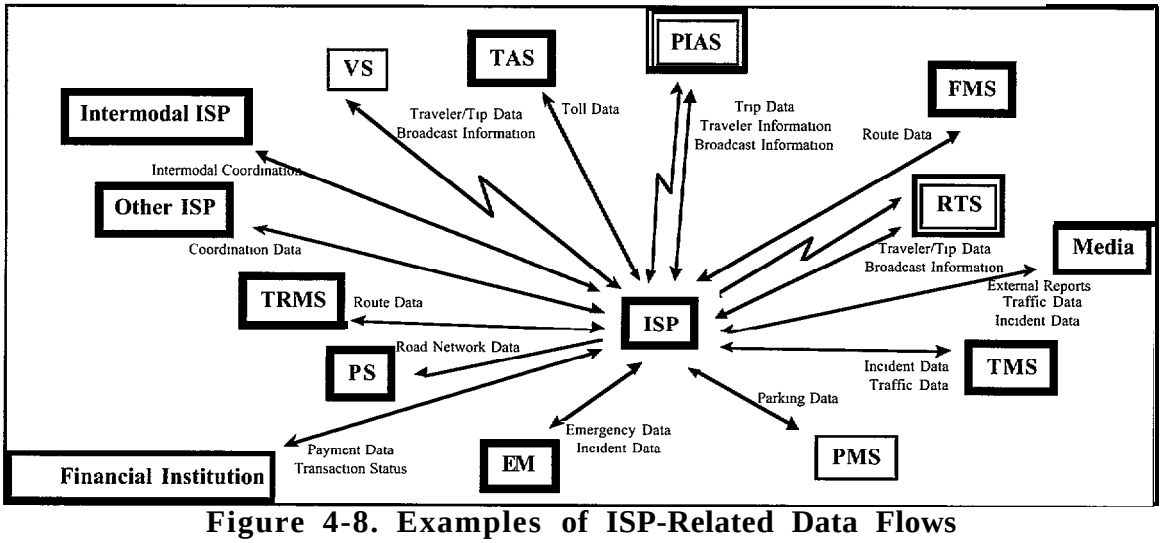


Figure 4-8. Examples of ISP-Related Data Flows

- **Impact of Denial of Service**

  ISP operations can be delayed, prevented, or mishandled in several ways.

  Absent or Inoperable ISP Devices. If an ISP's computer system is inoperable, then the ISP could not receive and respond to requests for the particular information that it provides. If the information regards traffic or weather conditions, then its unavailability could enhance traffic problems or allow drivers to travel in hazardous weather conditions.

  Absent, Inaccessible, or Unreadable Data. If a computer-system error makes ISP-related traffic information inaccessible, then the travelers requesting such information might not learn of the traffic conditions affecting their routes in time to change.

  Absent or Unexecutable Software. If the software that calculates routes for travelers has been deleted from the ISP's computer system (either accidentally or intentionally), incorrect routes could be provided to travelers; such routes could prolong their trips and possibly lead them into congestion.

  Loss of Wireline Communications. Losing wireline communications would isolate the ISP from its information sources. Although it could receive requests from the traveler, it could not satisfy those requests, resulting in delays, traffic disruption, and a loss of ITS credibility.

  Loss of Wide-Area Wireless Communications. The loss of wide-area wireless communications, even temporarily, could cause traffic disruptions, particularly after travelers have become accustomed to using their onboard devices for weather, advisory, and routing information.

- **Impact of Disclosure**

  As noted in the data flow assessment, sensitive information (e.g., credit and traveler identity, traveler location, etc.) is provided by the ISP. If such information were captured either during transmission or while stored in the ISP computer system(s), it could be used to make unauthorized purchases. These types of information are particularly vulnerable when provided by wide-area wireless communications -- a primary service for an ISP (see B.2.2).

- **Impact of Manipulation**

  Hackers could gain access to the ISP computer system(s). By manipulating data such as tip route recommendations, the hacker could send a specific traveler or a group of travelers to the wrong location. For example, a visiting dignitary could be directed to an ambush site. In a more subtle attack, traffic could be redirected to pass by a vendor's location in the hope that the vendor would get more business from such access. Even minor errors in accident locations, for example, could cause emergency vehicles to respond to the wrong location.

  ISP data flows subject to manipulation threats are indicated in tables A-8a and A-8b.

- **Impact of Masquerading**

  Masquerading attacks could be very disruptive. If an attacker could masquerade as the ISP, they could send out false information, either as a response to an individual request or in a broadcast message. For example, terrorists could send out false weather information warning of an impending tornado; alternatively they could override critical information about a blizzard. The first attack could cause widespread panic; the second attack might result in accidents or stranded vehicles and travelers.

  In a more personal masquerading attack, a stalker could use ride-sharing inquiries to screen for potential victims and set up rendezvous with unsuspecting riders. Tables A-8a and A-8b reflect the significance of masquerade attacks on ISP data.

- **Impact of Replay**

  As indicated in tables A-8a and A-8b, ISP is subject to the replay of payment request messages.

- **Impact of Repudiation**

  Onlookers contributing to the increasing traffic congestion at an accident scene could deny receiving advisories or detour instructions.

4.2.6 Planning Subsystem

The Planning Subsystem (PS) is a center subsystem that provides planning information and support for facilitating the deployment and operation of ITS services.

The PS collects operational data from other subsystems (Toll Administration, Transit Management, and Commercial Vehicle Administration) and makes it available to transportation planners and the Traffic Management Subsystem (TMS). PS data may also be used to simulate system operation and predict workloads. Additionally, the PS exchanges data with map update providers to facilitate map changes, which are then fed back into the simulation and traffic management functions. Wireline communications is the only type of communications used by the PS.

Figure 4-9 illustrates associated ITS subsystems and terminators and provides exemplary data flows. Tables A-11a and A-11b contain the analyses for all PS data flows.

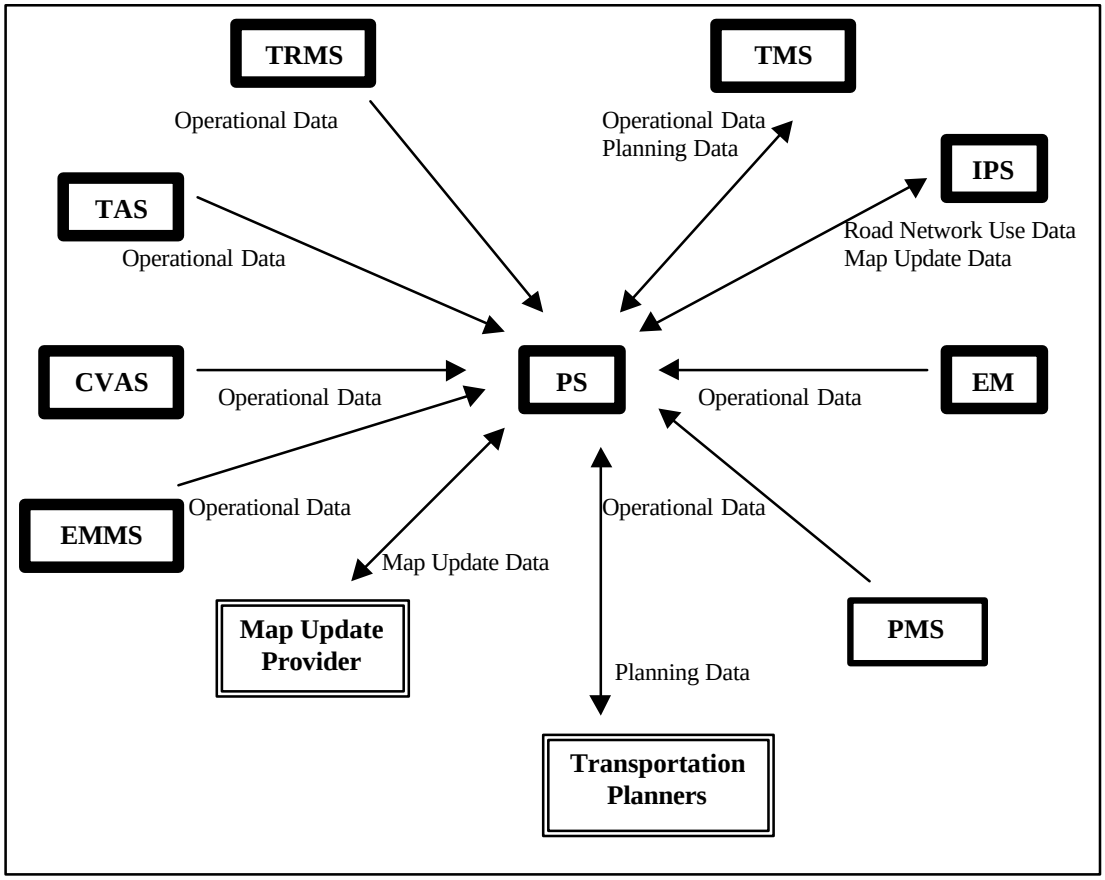


Figure 4-9. Examples of PS-Related Data Flows

- **Impact of Denial of Service**

PS operations can be delayed, prevented, or mishandled in several ways.

Absent of Inoperable PS Devices. If the PS Computer system is inoperable, it cannot collect and process the operational data it receives from other OTS subsystems.

Absent, Inaccessible, or Unreadable Data. The operational data that the PS stores and processes could be inaccessible or unreadable. Depending on the timeliness of backup-and-recovery procedures, the available information may not be the most current or complete. Without current information, transportation planners could overlook problems--or the symptoms of problems--that require their attention.

Absent or Unexecutable Software. If the PS simulation and forecasting software has been deleted from the PS computer system (either accidentally or intentionally), transportation planners will not be able to determine the results of proposed solutions nor predict future traffic and work loads.

Loss of Wireline Communications. Most of the data collected by PS is for statistical analysis and performance analysis. Thus, if communications were temporarily lost, data collection and the resulting analysis would be delayed. This would delay map updates and impair simulations.

Two other subsystems would likely be impaired by information delays; the Traffic Management and Emergency Management subsystems that requiring planning statistics to accurately forecast and manage traffic. These subsystems could continue to function, but the information would not be current.

- **Impact of Disclosure**

  As noted in tables A- 11 a and A-l 1 b, only data transmitted to the EM are subject to disclosure threats. Although the computer systems contain few sensitive data, they must be protected.

- **Impact of Manipulation**

  PS data consists primarily of statistical data used for future parking and traffic plans. Inaccurate or improperly modified data could impact short- and long-range planning for road repair and improvement. As noted in tables A- 11 a and A- 11 b, all data exchanges are subject to the threat of manipulation. However, the type of data being transmitted does not indicate the need for any additional integrity protection.

- **Impact of Masquerading**

  As noted in tables A-l 1 a and A-l lb, masquerading could pose a problem to the PS. An attacker posing as another subsystem could send false operational data to the PS and affect the trip routing, traffic management, and possibly emergency management functions.

- **Impact of Replay**

  Replay attacks on the PS are considered of negligible impact to ITS (see tables A- 1 la and A-l lb).

- **Impact of Repudiation**

  Unless the subsystems providing operational data to the PS keep a log of their transactions or the PS logs these transactions, responsible parties could deny the provision (or omission) of such information. If the data in question cannot be provided at a later time, transportation planners would have to base their simulations and forecasts on incomplete information.

4.2.7 Toll Administration Subsystem

The Toll Administration Subsystem (TAS) is a center subsystem that provides general payment administration capabilities to support the electronic assessment of tolls and other usage fees. The TAS uses wireline communications exclusively in its interactions with other ITS subsystems.

The TAS performs the following functions:

- Support the collection of both pre-payment and post-payment transportation fees
- Set up and administer escrow accounts to support pre-payment operations
- Support fee collection operations with the Toll Collection Subsystem (TCS), the Parking Management Subsystem (PMS), and the Transit Management Subsystem (TRMS)
- Set and administer the pricing structures
- Support the implementation of road pricing policies in coordination with the Traffic Management Subsystem (TMS)
- Provide toll payment violation information to the appropriate enforcement agency

Figure 4-10 illustrates associated ITS subsystems and terminators and provides exemplary data flows. Tables A-14a and A-14b contain the analyses for all TAS data flows.

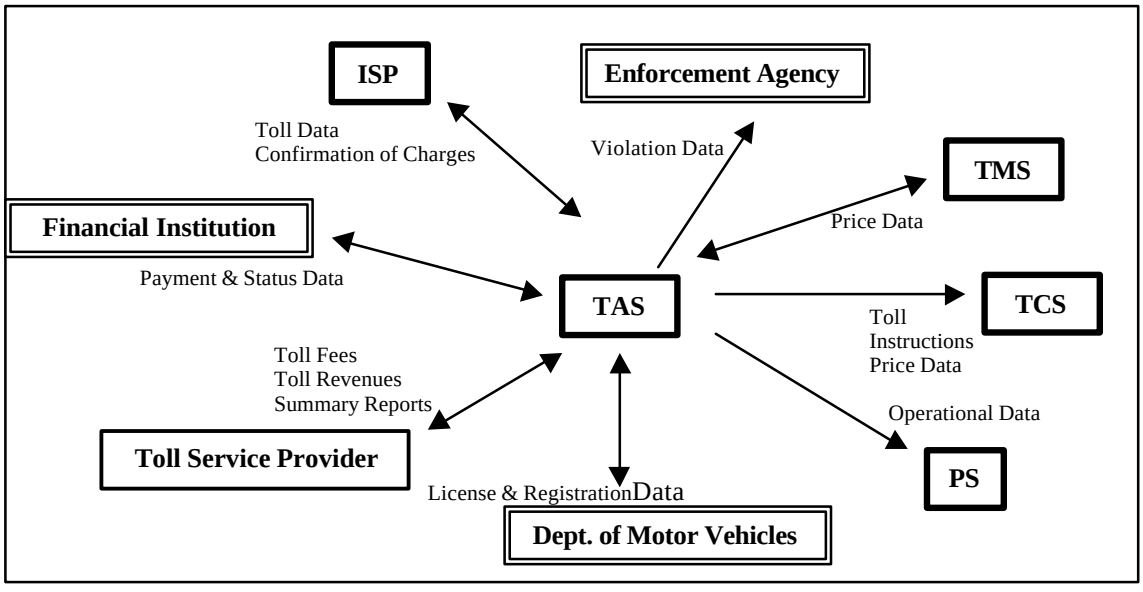


Figure 4-10. Examples of TAS-Related Data Flows

- **Impact of Denial of Service**

  TAS operations can be delayed, prevented, or mishandled in several ways.

  Absent or Inoperable TAS Devices. If the TAS computer system is inoperable due to system errors or repairs, other ITS subsystems could not access the TAS toll instructions, toll reviews, and summary reports, etc.

  Absent, Inaccessible, or Unreadable Data. If the TAS's toll payment violation data are deleted, then the identities of the toll payment violators and the details of their violations could not be sent to the appropriate enforcement authorities for proper action (e.g., fines and penalties).

  Absent or Unexecutable Software. If the TAS software that requests payments of drivers' toll charges from financial institutions is inoperable, such payments could not be collected.

  Loss of Wireline Communications. Loss of wireline communications would delay the transmission of payment data to financial institutions and the transmission of toll-fee, price change, and other operational data exchanged with the Toll Collection Subsystem (TCS). TAS communications loss would also delay the exchange of license and registration information with the DMV, as well as the violation information passed to an enforcement agency. Some details and examples are discussed below.

- **Impact of Disclosure**

  The threats of disclosure to the TAS are the potential unauthorized dissemination of toll revenue and pricing data as well as operational data. Of more importance, as noted in the data flow assessment, is the potential unauthorized disclosure of license, registration, and violation information.

- **Impact of Manipulation**

  The manipulation of TAS data could be detrimental to the revenue collection process and cause substantial bookkeeping and budgeting problems. The manipulation of toll pricing data would have a similar impact.

  The improper alteration of license, registration, and/or violation data could result in not only offenders escaping violation, but also embarrassment and inconvenience to those falsely accused of a violation.

  Tables A-14a and A-14b reflect the TAS data flows subject to manipulation threats.

- **Impact of Masquerading**

  A masquerade could lead to the negative impacts discussed in the preceding paragraph (i.e., the changing of toll rate, revenue, or violator data). The significance of masquerade threats is reflected in tables A-14a and A- 14b.

- **Impact of Replay**

  As noted in tables A-14a and A-14b, the replay of payment and payment request messages produces the obvious accounting errors that may cost a state or local agency resources.

- **Impact of Repudiation**

  The TAS would suffer impact from repudiation of its payment-related and violation-related messages.

4.2.8 Traffic Management Subsystem

The Traffic Management Subsystem (TMS) is a key center subsystem that provides data processing of traffic, incident, and pollution data. It also provides management capabilities and frequently interacts with other ITS subsystems (e.g., the Roadway and Information Service Providers). The TMS coordinates transit signal priority, emergency-vehicle signal preemption, and signage data with other ITS subsystems, including highway-rail intersections. The TMS exclusively uses wireline communications for the exchange of data with other ITS subsystems.

The TMS also performs the following functions:

- Monitor and manage traffic flow
- Detect and verify traffic incidents
- Support High-Occupancy Vehicle (HOV) lane management and coordination, road pricing, reversible lane facilities, and other “demand management” policies and procedures that can alleviate congestion and influence mode selection
- Monitor and manage maintenance work, and disseminate maintenance work schedules and road closures
- Coordinate with rail operations regarding highway traffic management at highway-rail intersections
- Control the devices used for automated highway system (AHS) traffic and vehicle control

Figure 4-l 1 illustrates associated ITS subsystems and terminators and provides exemplary data flows. Tables A-l 6a and A-16b contain the analyses for-all TMS data flows.

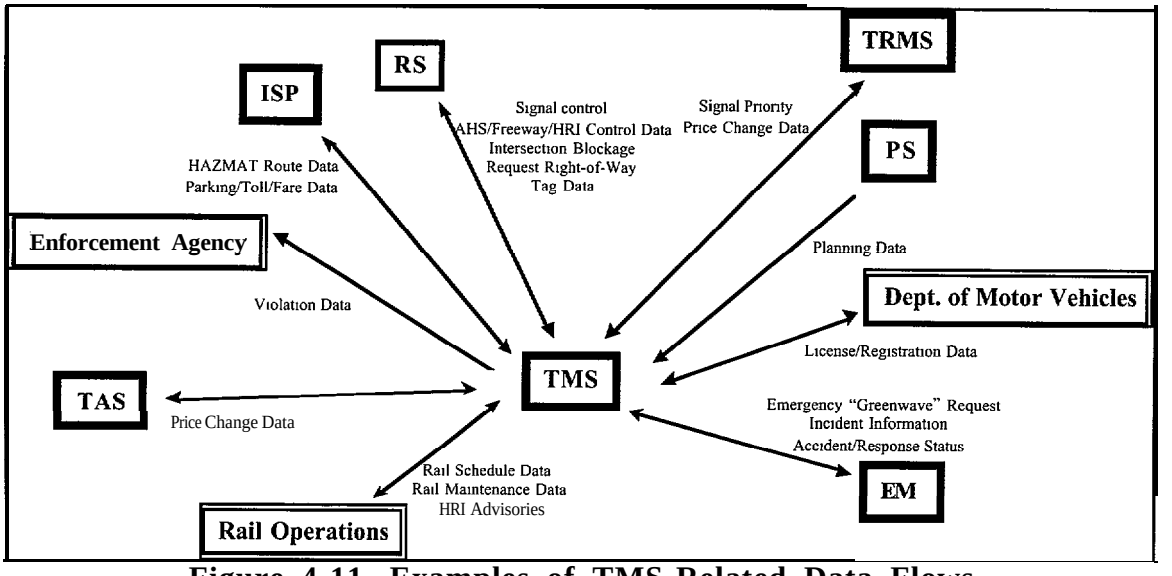


Figure 4-11. Examples of TMS-Related Data Flows

- **Impact of Denial of Service**

  TMS operations can be delayed, prevented, or mishandled in several ways.

  Absent or Inoperable TMS Devices. If the appropriate freeway ramp meters and lane usage signals are inoperable, the HOV lanes that they control could not be managed and the preferential treatment of vehicles in the HOV lanes could not be provided.

  Absent, Inaccessible, or Unreadable Data. A computer virus in the TMS computer system could delete or make unreadable the traffic data that are continuously received from the traffic and vehicle probes placed in roads and highways. Without this information, traffic management personnel could not analyze traffic or detect accidents.

  Absent or **Unexecutable Software.** If the TMS signal-control software is inoperable or has programming errors (either accidentally or intentionally included), traffic managers could not monitor and manage the traffic flows in major intersections nor detect and verify traffic incidents.

  Loss of Wireline Communications. As noted above, the TMS uses wireline communications for its data exchanges with other subsystems. Since much of that data deals with public safety information and must be processed in "real time," the loss of TMS communications may have catastrophic impacts (see paragraph B.2.1). For example, the TMS would be unable to exchange vital information concerning public safety in a timely fashion. Without current and accurate information from other ITS subsystems, TMS

simply could not perform its functions properly. Examples of the types of messages that would be affected include:

- Emergency vehicle "greenwave" data
- Route plan for HAZMAT shipments
- Incident data
- AHS, freeway, and highway-rail intersection control data
- Signal control and priority status
- Intersection blockage
- Request for right-of-way
- Vehicle tag data
- License/registration data
- Violation information to enforcement agencies
- Pollution data
- Operational data, which includes current incident and traffic data
- Planning data
- Road network use (e.g., parking lot, toll, and transit fare data)
- Price change data

- **Impact of Disclosure**

  As identified in the data flow assessment, the TMS processes and transmits sensitive data (e.g., HAZMAT, violation data). The disclosure of HAZMAT routes would be advantageous to a serious criminal or terrorist effort. Since the TMS also processes personal information (e.g., license, registration, and vehicle tag information), its unauthorized disclosure raises serious concerns regarding personal privacy.

- **Impact of Manipulation**

  As identified in the data flow assessment, some of the data that the TMS processes (e.g., highway-rail intersection (HRI) and traffic signal data) are essential to public safety. Manipulation of these processes would pose a significant threat to the general public. The alteration of any such messages or related stored data could lead to or contribute to major accidents. The TMS makes an appealing target for those intent on creating either a diversion or simply creating havoc.

- **Impact of Masquerading**

  A masquerade could lead to the impacts discussed in the preceding paragraphs. More or less serious impacts might also result from a range of potential perpetrators including mischievous hackers, disgruntled employees, or criminals and terrorists. A perpetrator masquerading within the TMS (e.g., a TMS facility employee) would be able to alter

messages vital to public safety. Control of TMS messages that direct surface street signals, HAZMAT routes, AHS control data, or highway-rail intersection (HRI) control data could be used to the perpetrator's benefit and to the detriment of law enforcement and public safety. Tables A-16a and A-16b reflect the significance of masquerade threats.

- **Impact of Replay**

  Although the TMS processes and transmits traffic control and safety data, the data flow assessment resulted in no recommendation of special protection from replay attacks. This is due to the contents of constituent data flows.

- **Impact of Repudiation**

  As noted in tables A-16a and A- 16b, the potential impacts of TMS message repudiation are considered minimal.

4.2.9 Transit Management Subsystem

The Transit Management Subsystem (TRMS) is a center subsystem which collects operational data from transit vehicles and supports both strategic and tactical planning affecting both vehicles and drivers. In addition to the transit vehicles, the TRMS frequently interacts with other ITS subsystems and financial institutions. The TRMS relies on both wireline and wireless interfaces.

The TRMS performs the following functions:

- Provide travelers with real-time travel information, continuously updated schedules, schedule adherence information, transfer options, and transit routes and fares
- Monitor key transit locations with both video and audio systems
- Provide automatic alerting of operators and police of potential incidents, including support of traveler-activated alarms
- Support the TMS with integrated traffic signal prioritization
- Provide vehicle routing for fixed and flexibly routed transit services
- Provide optimized vehicle and driver assignments
- Coordinate transit vehicle maintenance management with schedule tracking
- Determine usage ("ridership") levels of transit services
- Implement fare structures reflecting usage levels
- Automate the planning and scheduling of public transit operations

Figure 4- 12 illustrates associated ITS subsystems and terminators and provides exemplary data flows. Tables A-17a and A-17b contain the analyses for all TRMS data flows.

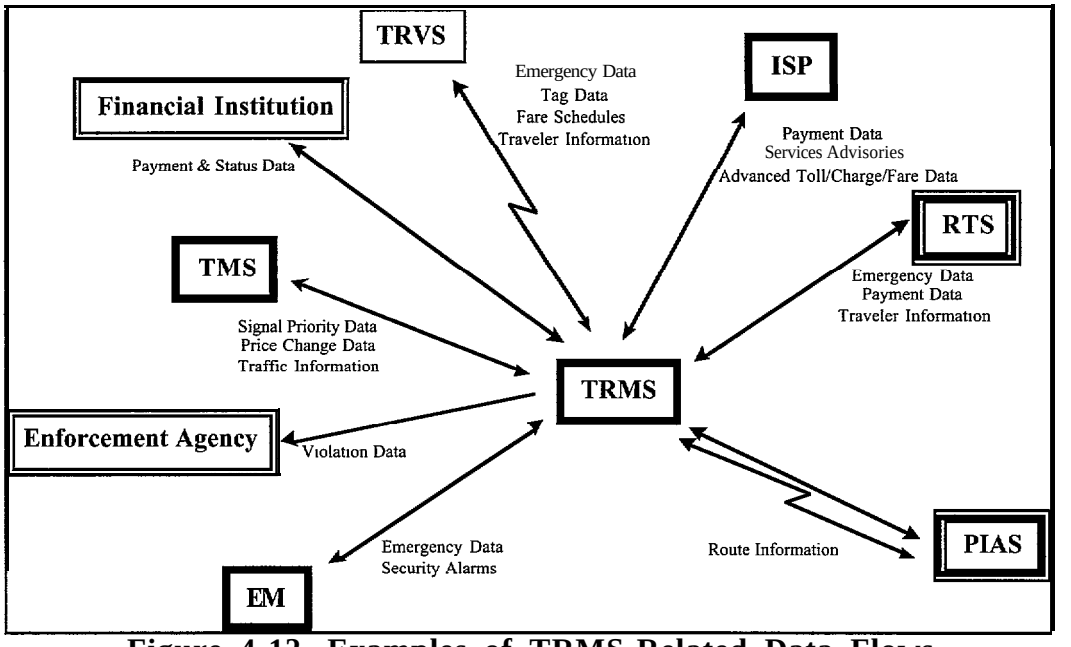


Figure 4-12. Examples of TRMS-Related Data Flows

- **Impact of Denial of Service**

  TRMS operations can be delayed, prevented, or mishandled in several ways.

  Absent or Inoperable TRMS Devices. If TRMS computer systems are inoperable due to system errors, maintenance or repairs, the TRMS could not communicate with other ITS subsystems and financial institutions. Specifically, TRMS could not provide travelers with real-time travel information or transit vehicle operators/systems with automated alerts or transit signal prioritizations.

  Absent, Inaccessible, or Unreadable Data. If the TRMS's fare-collection violation data are deleted, then the identities of the fare-collection violators and the details of their violations could not be provided to the appropriate enforcement authorities for proper action (e.g., fines and penalties).

  Absent or Unexecutable Software. If the TRMS software used to generate transit routes is inoperable, the maps illustrating these routes could not be generated.

  Loss of Wireline Communications. If wireline communications were lost, the TRMS would be unable to effkiently exchange vital information concerning public safety. Examples of the type of TRMS message exchanges that could be affected include:

- Emergency information with the EM, the TMS, and the Remote Traveler Support subsystem (RTS)
- Messages containing financial and fare data with the ISP and the RTS
- Confirmation of payment and bad-payment updates with financial institutions
- Intermodal information with inter-modal service providers

Loss of Wide-Area Wireless Communications. Loss of the two-way wireless communications would prohibit the TRMS from communicating with transit vehicles. This would result most significantly in the inability to transmit emergency information to such vehicles.

Although the impact is less severe when fare and schedule data are not transmitted to the transit vehicle, or when traveler/trip route information is not transmitted to the traveler, these situations would be an inconvenience to the traveler.

- **Impact of Disclosure**

Unauthorized disclosure of emergency and security alarm information is often not in the public interest. As noted in the data flow assessment, the TRMS also transmits and receives financial information, some of which pertains to an individual citizen. Improper disclosure of this information could result in legal actions from offended and/or wronged citizens. Additionally a traveler's identity and trip routing information could be used by criminal and/or terrorist organizations.

- **Impact of Manipulation**

Some of the emergency and security data that the TRMS processes is essential to public safety. Unauthorized or improper manipulation of these data would pose a significant and real threat to the general public. The financial, payment, and transaction status messages that the TRMS exchanges with other systems may be an appealing criminal target (see tables A-17a and A- 17b).

- **Impact of Masquerading**

A masquerade could lead to the impacts discussed in the preceding paragraphs. In addition, a masquerade within the TRMS could result in mis-information regarding security, emergency, transit driver instructions, financial, traveler identity and/or trip route, etc. All could easily be used for unlawful and/or militant purposes. Tables A-17a and A-17b indicate the significance of masquerade attacks on TRMS.

- **Impact of Replay**

As noted in tables A-17a and A-17b, TRMS messages dealing with payments are targets for replay attacks, presumably with criminal intent.

- **Impact of Repudiation**

  Also as noted in tables A-17a and A- 17b, financially related TRMS messages are also targets for repudiation. Also note that the repudiation of a security message has the potential to make it appear as though the incident did not occur.

4.3 ROADSIDE SUBSYSTEMS

This section describes the four ITS roadside subsystems. These subsystems include functions that require convenient access to a roadside location for the deployment of sensors, signals, programmable signs, or other interfaces with travelers and vehicles of all types.

4.3.1 Commercial Vehicle Check Subsystem

The Commercial Vehicle Check Subsystem (CVCS) is a roadside subsystem that provides for and manages the automated checks and inspections of commercial vehicles at roadside checkstations. By means of roadside sensors and hand-held devices that use dedicated short-range communications (DSRC) (radio-frequency and/or infrared communications), commercial vehicles in motion can be identified, and their credentials, characteristics (e.g., weight, height, number of axles), and trip plans can be checked against the most current CVAS records. The inspection results are collected at each visited roadside checkstation, recorded on the commercial vehicle's on-board database, and sent via wireline communications to the CVAS for access by each roadside facility that operates in the commercial vehicle's planned route.

The CVCS performs the following functions:

- Identify and verify commercial vehicle credentials for a particular commercial vehicle, operator, driver, and trip
- Identify safety problems and report them to the commercial vehicle driver, the driver's fleet manager, the CVAS site, and the proper authorities
- Automatically request the commercial vehicle to pull in (for possible inspection or re-inspection) if any of the following occur:
  - The vehicle does not have on-board tag data
  - The vehicle's on-board tag data cannot be read or interpreted
  - A safety problem has been detected
  - The lock tag attached to a vehicle's cargo has been changed
  - The information from the roadside sensors or from the vehicle's on-board database is inconsistent with CVAS records
- Record inspection results on the relevant databases, lists (e.g., safety-problem list), and logs residing on the vehicle, at the roadside checkstation, and at the CVAS site

- Allow roadside inspectors to override the automated pass or fail (pull-in) decision and to add comments to inspection results

- Verify the driver, trip, and cargo information of commercial vehicles going through border crossing points, and check for compliance with import/export and immigration regulations

- On a daily basis, transmit a copy of the roadside facility log, which records all activities that occurred at the roadside facility, to the CVAS for further processing

Figure 4-13 illustrates associated ITS subsystems and terminators and provides exemplary data flows. Table A-2a and A-2b contain the analyses for all CVCS data flows.

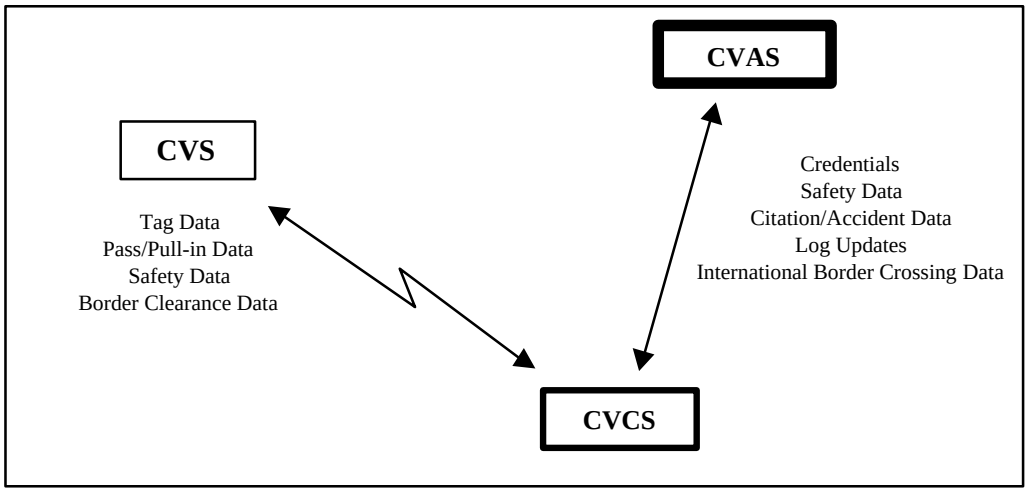


Figure 4-13. Examples of CVCS-Related Data Flows

- **Impact of Denial of Service**

  CVCS operations can be delayed, prevented, or mishandled in several ways.

  Absent or Inoperable CVCS Devices. A commercial vehicle may not have the necessary DSRC tag or on-board database on which the CVCS depends, or the inspector's hand-held device may be broken. If these devices are inoperable, then automated checks and inspections cannot be performed and their results cannot be recorded in the roadside, vehicle, and CVAS database.

  Absent, Inaccessible or Unreadable Data. A software virus may delete log data on the roadside inspection station's computer system or make the system's records unreadable or inaccessible. The roadside daily activity log is transmitted to the CVAS for processing and storage. If the CVAS information is incorrect or incomplete, checks and inspections of cleared vehicles may need to be performed again, and commercial vehicles' CVAS records r-initialized, The delays associated with such incidents could result in allowing unsafe vehicles or operators with safety violations to pass.

Absent or Unexecutable Software. The computer program in the inspector's hand-held device might verify the driver, trip, and cargo information. If the application software will not execute, then unsafe cargoes and drivers with violations could be passed through the roadside inspection stations. The same effects could occur if the computer program that reads roadside sensor data fails to generate a valid pull-in message.

Loss of Wireline Communications. Losing wireline communications with the CVAS will result in the inability to access the most current CVAS information, the requirement to perform the inspections manually, the corresponding delays in roadside checkstation operations, and the possibility allow unsafe vehicles or operators with safety violations to pass. Prior inspections, for which records exist in the CVAS, may need to be performed again.

Loss of DSRC. A commercial vehicle's DSRC signals may interfere with or jam the inspector's hand-held device radio. Until the offending vehicle departs or its radio is turned off, transmissions to and from other commercial vehicles, the hand-held device, and the roadside computer system will be prevented.

- **Impact of Disclosure**

  Depending on the care with which roadside check and inspection information is handled (e.g., disposing of hardcopy inspection results in wastebaskets accessible by the public), commercial vehicle drivers could learn of other commercial operators' sensitive information (e.g., trip plans and routes, results of inspections, etc.). Depending on the information disclosed, others might be able to modify inspection results, replay information, or masquerade as other drivers or roadside inspectors.

  If roadside inspectors intentionally or accidentally disclose methods for operating CVAS equipment, drivers (provided that they can get access to inspectors' hand-held devices) might be able to masquerade as inspectors to modify their check and inspection results.

  Tables A-2a and A-2b reflect the actual transmissions that are subject to disclosure threats.

- **Impact of Manipulation**

  As noted in tables A-2a and A-2b, CVCS processes and transmits sensitive data (e.g., safety, tag, and accident data). The unauthorized manipulation of such data could allow unsafe commercial vehicles on the roadway.

- **Impact of Masquerading**

  In addition to the masquerading impacts discussed with the impacts of disclosure, the DSRC tag of a commercial vehicle that has passed all checks and inspections could be stolen or cloned. The tag could then be used in a vehicle to masquerade as one that has passed all checks and inspections. Tables A-2a and A-2b indicate the significance of masquerade threats to CVCS.

- **Impact of Replay**

  Drivers with stolen hand-held devices could replay inputs to the CVCS (and eventually, to the CVAS) databases to and subsequently raise suspicion about the accuracy of all input, both valid and invalid. With information from roadside and CVAS computer systems reflecting such inconsistent conditions, commercial vehicle checks and inspections might need to be performed manually. Again, associated delays could result in unsafe vehicles to pass. Tables A-2a and A-2b show the specific CVCS data flows subject to replay attacks.

- **Impact of Repudiation.**

  Given the USC of toll-tag technology, the threat of repudiation is minimal (see tables A-2a and A-2b).

4.3.2 Parking Management Subsystem

The Parking Management Subsystem (PMS) is a roadside subsystem which manages parking lot usage and collects parking fees. The PMS uses DSRC for communications with the vehicle and wireline communications for exchange with most other subsystems.

The PMS performs the following functions:

- Provide parking-space availability status and reservation information to the ISP and the parking operator
- Provide parking lot payment violation information to the appropriate enforcement agency
- Accept tag information from the Vehicle Subsystem (VS)
- Send license requests to the DMV
- Accept parking payment fees without the use of cash
- Request payments for licenses and parking charges from the appropriate financial institution
- Assist in the detection, classification, and control of vehicles seeking parking spaces

Figure 4-14 illustrates associated ITS subsystems and terminators and provides exemplary data flows. Tables A-1Oa and A-10b contain the analyses for all PMS data flows.

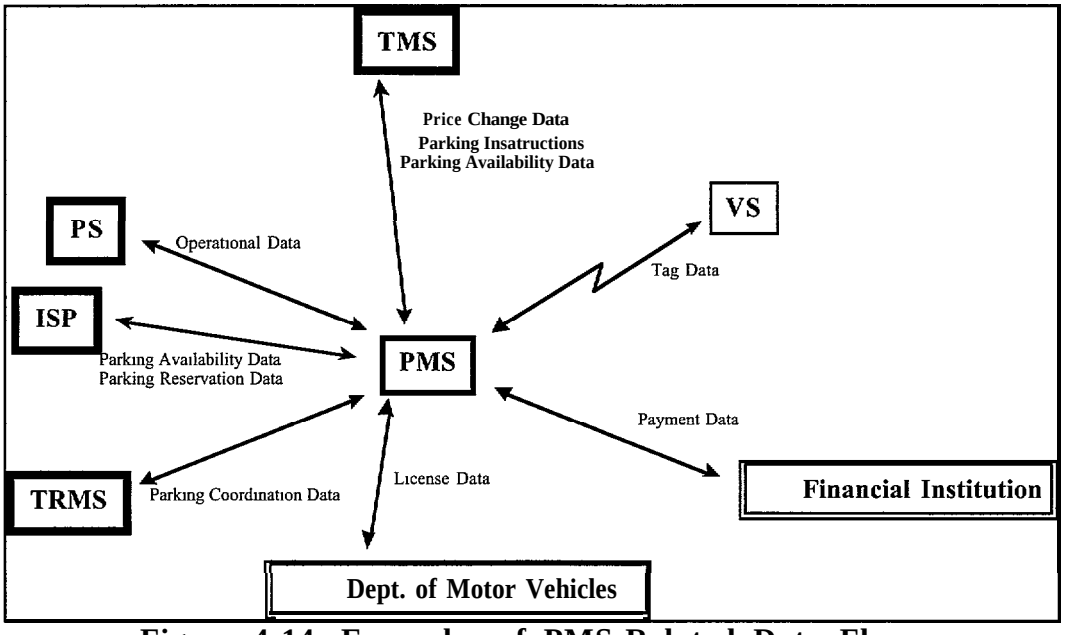


Figure 4-14. Examples of PMS-Related Data Flows

- **Impact of Denial of Service**

  PMS operations can be delayed, prevented, or mishandled in several ways.

  Absent or Inoperable PMS Devices. If the PMS computer system at a particular roadside location is inoperable, it could neither process automated payments nor provide real-time parking lot status to travelers.

  Absent, Inaccessible, or Unreadable Data. If the PMS's parking lot payment violation data are deleted, then the identities of parking lot payment violators and the details of their violations could not be sent to the appropriate enforcement authorities for proper action (e.g., fines and penalties).

  Absent or Unexecutable Software. If the PMS software that performs transactions with supporting financial institutions is inoperable, parking payments could not be collected in a timely fashion.

  Loss of Wireline Communications. If wireline communications were lost, the traveler would not be able to request or accept parking lot availability information. Without such information, the traveler would require additional time and fuel driving to find a lot with parking space available.

Furthermore, if wireline communications were lost, the PMS would not be able to send payment, license, or violation data to the appropriate destinations until such communications were restored.

Loss of DSRC. DSRC loss would delay or prohibit the PMS's transactions of payment, license, and violation data.

- **Impact of Disclosure**

Threats of disclosure to the PMS are minimal, but often involve the traveler's location and possibly include violation data (see tables A-1Oa and A-lob). The traveler's location data could be used for acts of theft, assault, etc.

Another, less harmful attack could occur if the traveler's standard parking location was collected and made available to local vendors. The vendors could then send various business solicitations to the traveler, actions that many would consider intrusive and disruptive.

- **Impact of Manipulation**

Damaged or altered violation or payment data could have negative effects ranging from embarrassment to theft. Unauthorized or repeated payment requests could result in the incorrect distribution of funds. Tables A-10a and A- 10b show the PMS data flows subject to the threat of unauthorized manipulation.

- **Impact of Masquerading**

A parking lot owner could masquerade as the operator of another parking lot, report that lot is full, and thus direct drivers to their parking lot. The threat of a masquerade attack is identified in as a threat to the majority of the PMS data flows.

- **Impact of Replay**

Replay of otherwise legitimate transactions might lead to the theft of funds; that is, repeated payment requests could result in improperly distributed funds (see tables A-1Oa and A-10b).

- **Impact of Repudiation**

As noted in tables A-10a and A-10b, PMS related parking reservations and financial transactions are subject to repudiation. Denial of such transactions could result in a loss of both system credibility and corporate revenue.

4.3.3 Roadway Subsystem

The Roadway Subsystem (RS) is a roadside subsystem that provides traffic management surveillance, signals, and signs for traveler information.

The RS also performs the following:

- Monitor emissions and environmental conditions, including weather and roadway sensors
- Manage High Occupancy Vehicle (HOV) lanes and reversible lanes
- Control access to and egress from an Automated Highway System (AHS)
- Provide intersection collision avoidance
- Monitor situations and transmit appropriate warnings and/or control actions to the approaching vehicles

The RS includes devices at intersections, including multimodal intersections, to control and monitor trffic These devices include:

- Highway Advisory Radio (HAR)
- Variable message signs
- Cellular call boxes
- Closed circuit television (CCTV) cameras
- Video image processing systems for incident detection and verification
- Vehicle detectors
- Traffic signals
- Grade-crossing warning systems
- Freeway ramp metering systems

The RS uses wireline communications for interaction with most other subsystems and DSRC for communications with vehicles.

Figure 4-15 illustrates associated ITS subsystem and terminators and provides exemplary data flows. Tables A-12a and A-12b contain the analyses for all S data flows

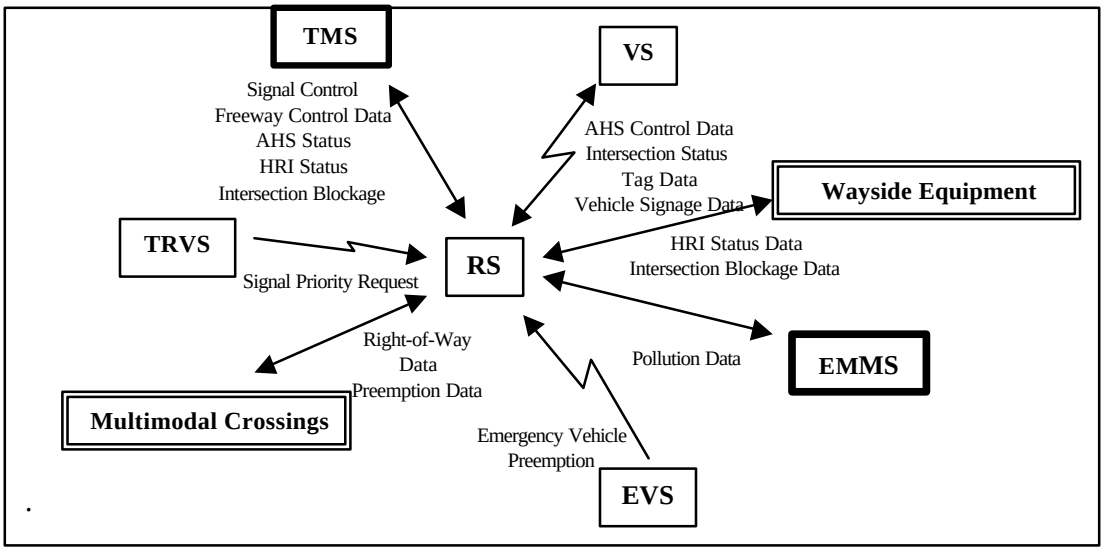


Figure 4-15. Examples of RS-Related Data Flows

- **Impact of Denial of Service**

  RS operations can be delayed, prevented, or mishandled in several ways.

  Absent or Inoperable RS Devices. The variable-message signs or CCTV cameras may be rendered inoperable due to vandalism or natural disaster. Without properopration of these roadside subsystems, operators would not be able to warn drivers of the highway and weather conditions that may jeopardize their safety.

  Absent, Inaccessible, or Unreadable Data. The traffic data could be deleted or made unreadable by a computer virus. Without such information, traffic could not be controlled.

  Absent or Unexecutable Software. If the software program that processes data from weather sensors is inoperable, travelers could not be warned of impending weather conditions, Without such information, travelers could arrive in congested or dangerous traffic conditions.

  Loss of WirelineCommunications. If wireline communications were lost, the RS would be unable to exchange several forms of time-sensitive information. Specifically, highway rail intersection (HRI), signal control, and right-of-way message would be affected, thereby potentially placing travelers in unsafe conditions.

  Loss of DSRC. DSRC loss would prohibit the RS from exchanging data with the ITS vehicle subsystems. Critical messages such as emergency vehicle preemptions, intersection status, and automated highway control data could not be provided.

- **Impact of Disclosure.**

  Persons who have obtained access, authorized or unauthorized, to the wireline communications between the RS and the Traffic Management Subsystem (TMS) could access **sensitive** roadside subsystem control data, personal vehicle tag data, etc. In the case of tag data, personal privacy could be violated. Tables A-12a an A- 12b show the RS transmissions subject to the threat of unauthorized disclosure.

- **Impact of Manipulation**

  Some of the information processed by the RS is essential to public safety (see tables A-12a and A-12b). Unauthorized or improper manipulation of this information would pose a significant threat to the general-public. This would include information controlling the following functions:

  - Intersection status, including highway-rail intersections (HRI)
  - Bridge crossing status and/or closing times and durations
  - Lane use
  - Collision avoidance
  - Sign and signal data (e.g., "approaching train' messages)

  The RS makes an appealing target for terrorists intent on creating either a diversion or simply creating havoc.

- **Impact of Masquerading**

  A masquerade could lead to the impacts discussed in the preceding paragraphs and have consequences ranging from embarrassing to life-threatening. An example of the former occurred recently in **a** northeast state where a hacker changed the information displayed on the variable message signs to display a message insulting to the Governor. More serious impacts could result from a perpetrators' control of the RS messages that direct surface street signals or signals near at-grade highway-rail intersections (HRI) (see tables A-12a and A-12b).

- **Impact of Replay**

  Tables A-12a and A-12b indicate the RS data flows subject to replay attacks, including the replay of control and intersection messages.

- **Impact of Repudiation**

  As noted in tables A-12a and A-12b, the threat of repudiation is considered minimal.

4.3.4 Toll Collection Subsystem

The Toll Collection Subsystem (TCS) is a roadside subsystem that interacts with vehicles to collect tolls and identify violators. The TCS allows vehicle operators to pay tolls without stopping their vehicles. The TCS communicates with vehicles using DSRC and with the Toll Administration subsystem using wireline communications.

Figure 4-16 illustrates associated ITS subsystems and terminators and provides exemplary data flows. Tables A-15a and A-15b contain the analyses for all TCS data flows.

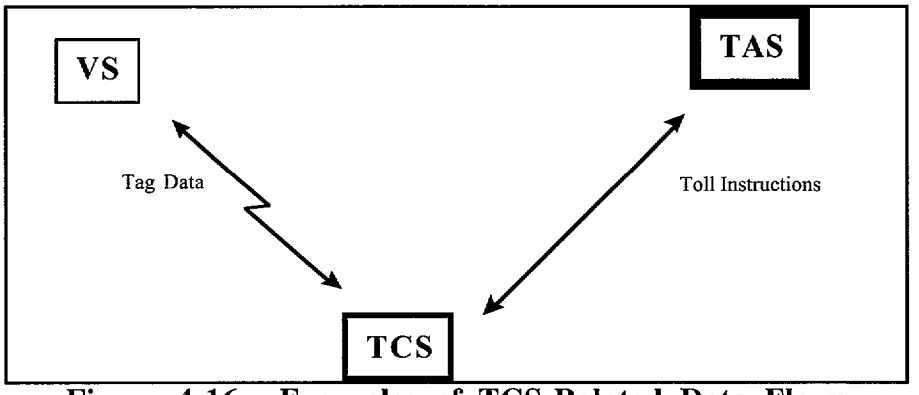


Figure 4-16. Examples of TCS-Related Data Flows

- **Impact of Denial of Service**

  TCS operations can be delayed, prevented, or mishandled in several ways.

  Absent or Inoperable TCS Devices. If the toll plaza's vehicle tag reader is inoperable, then the TCS could not identify the vehicle's characteristics required to calculate the appropriate toll.

  Absent, Inaccessible, or Unreadable Data. If the toll charge data stored on the toll plaza's TCS computer system are deleted or unreadable, the TCS could not calculate the tolls of the vehicles that pass.

  Absent or Unexecutable Software. If the TCS process that determines whether the vehicle driver is on its list of "bad toll payers" is inoperable, the TCS could not notify the appropriate enforcement authority of a potential violation.

  Loss of Wireline Communications. Should wireline communications be unavailable, any TCS-TAS transactions would be delayed.

  Loss of DSRC. Should DSRC be unavailable, the TCS would be unable to communicate with passing vehicles.

- **Impact of Disclosure**

  Several TCS transactions are potentially threatened by unauthorized disclosure. Toll transactions contain payment and violator data (see tables A-15a and A-15b), and the disclosure of such information could have legal repercussions.

- **Impact of Manipulation**

  The manipulation of TCS toll transaction messages, which include identification, payment and violator data, could be detrimental to the revenue-collection process and impede bookkeeping and budgeting functions. The improper alteration of such data could result in not only offenders escaping violation, but also embarrassment and inconvenience to those falsely accused of a violation. Tables A-15a and A-15b reflect the TCS messages subject to the threat of unauthorized manipulation.

- **Impact of Masquerading**

  A masquerade could lead to the incidents discussed in the preceding paragraphs (i.e., the changing of payment or violator data) as well as other negative impacts. As noted previously, the data flow assessment results reflect the significance of masquerade threats.

- **Impact of Replay**

  Toll transactions include data that confii payment and are therefore extremely susceptible to a replay attacks (see tables A-15a and A-15b). This could conceivably lead to a lawsuit by the wronged party. The replay of payment and payment request messages produces accounting errors that may cost a state or local agency significant resources.

- **Impact of Repudiation**

  The TCS could suffer various impacts from repudiation of its payment-related messages (see tables A-15a and A-15b).

4.4 VEHICLE SUBSYSTEMS

As implied, vehicle subsystems are installed in a vehicle. This section describes the four ITS vehicle subsystems.

4.4.1 Commercial Vehicle Subsystem

The Commercial Vehicle Subsystem (CVS) is a vehicle subsystem that resides in a commercial vehicle and provides the sensory, processing, storage, and communications functions required to support safe and efficient commercial vehicle operations.

The major components of the CVS include the following:

- Sensors for measuring trip conditions such as temperature, load leveling, acceleration and pressure; and driver/occupant conditions such as heart rate
- Electronic ID-tag identifying the commercial vehicle and containing the results of roadside inspections
- On-board processor(s), storage, and input/output devices to store, report, and exchange the commercial vehicle information that the CVS and other ITS subsystems provide, receive, or process
- Vehicle/cargo locating equipment (e.g., Global Positioning System (GPS)) to determine commercial vehicle locations and assist enforcement personnel or HAZMAT response teams in tracking HAZMAT carriers and commercial vehicles involved in an emergency
- On-board software to automatically generate a static route plans

The CVS performs the following functions:

- Enable commercial vehicles to pass through roadside checkstations along their routes without stopping unless safety checks are required or problems with clearing vehicles through border crossing checkpoints occur
- Store roadside inspection results (vehicle, cargo, and driver safety data) and cargo lock-tag status for access and review by commercial vehicle managers, fleet managers, and roadside inspectors
- Generate static routes for trips without taking any account of current or predicted traffic conditions along the routes
- Continuously collect, monitor, analyze, and log commercial-driver-safety information from on-board sensors, alert drivers of potential safety problems, and provide safety information to the CVCS
- Automatically collect vehicle location, mileage, fuel usage, distance traveled, and border crossing information for access and review by fleet managers and commercial vehicle managers
- Provide two-way wide-area wireless communications:
  - Between the commercial-vehicle driver and relevant managers (oral and keyboard inputs, audio and display/printer outputs)

- Between the commercial-vehicle CVS databases and the vehicle's relevant managers to access the vehicle's on-board data (routes, inspection results, safety information, and log data)

- Provide dedicated short-range communications (DSRC) between the commercial vehicle's CVS databases (ID tag and other storage) and a roadside checkstation's CVCS applications

- Enable commercial vehicle managers, fleet managers, or drivers to enter and read the following in the commercial vehicle's CVS databases (ID tag and other storage):

  - Commercial vehicle, driver, carrier, and trip information to enroll the vehicle for a particular route (CVS provides such information to the CVCS which later processes and transfers it to CVAS)
  - Other information required for the payment of necessary taxes and duties
  - Commercial-vehicle routing factors (e.g., time and vehicle constraints, desired arrival time) for automated generation of a static route for the trip

Figure 4-17 illustrates associated ITS subsystems and terminators and provides exemplary data flows. Tables A-2a and A-2b contain the analyses for all CVS data flows.

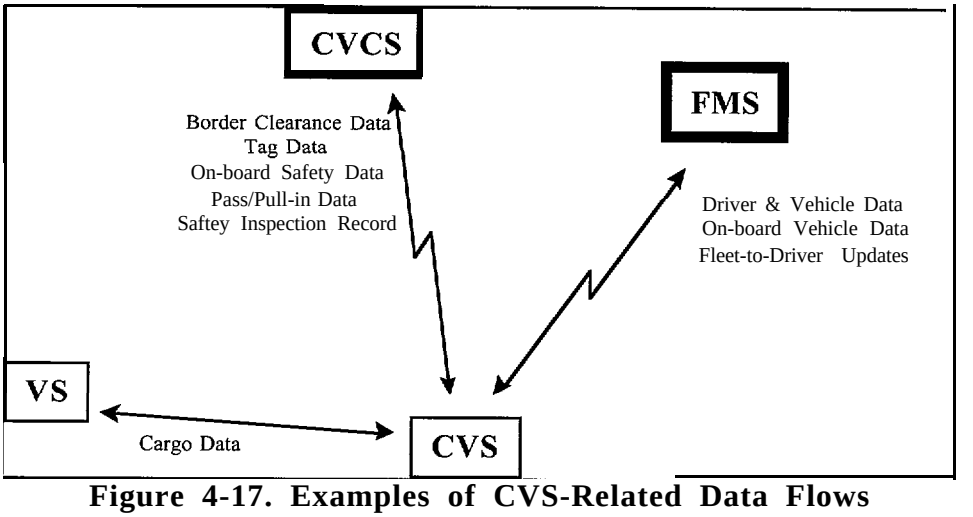


Figure 4-17. Examples of CVS-Related Data Flows

- **Impact of Denial of Service**

  CVS operations can be delayed, prevented, or mishandled in several ways:

  Absent or Inoperable CVS Devices. The commercial vehicle may not have the commercial vehicle DSRC tag, sensors, or on-board databases and processes on which the CVS depends. Without these components, the automated checks and inspections could not be performed and results could not be recorded. If the commercial vehicle is carrying

hazardous material but does not have the necessary vehicle/cargo locating equipment, enforcement personnel or HAZMAT response teams might not be able to locate, stop, **or** reroute the vehicle in an emergency situation.

Absent, Inaccessible, or Unreadable Data. A software virus could be accidentally or intentionally transmitted to each commercial vehicle with which the fleet manager communicates. Such a virus could delete or modify each commercial vehicle's CVS records and make any remaining CVS information unreadable or doubtful regarding its accuracy. The CVCS databases at roadside checkstations could also become infected with the same or different virus when the commercial vehicle transmits its infected data to the CVCS at the roadside checkstation. The CVCS applications could further spread the virus in its communications with other commercial vehicles.

With the loss of the commercial vehicle's CVS information, the reliability of any data transmitted to the CVCS is in question, and the automatic checks and inspections at roadside checkstations can not be performed. Subsequent delays in determining vehicles' correct enrollment, cargo, and trip information; and /or re-inspecting previously cleared vehicles could result in allowing unsafe vehicles or operators with credentials or safety violations to pass.

Absent or Unexecutable Software. If the commercial vehicle's route generation software is absent or inoperable, commercial vehicle drivers could choose routes that are unsafe or inappropriate. Malfunctioning CVS applications that process the commercial vehicle's sensor readings could report erroneous information about driver, vehicle, or cargo conditions and require drivers to pull in for unneeded inspections or safety checks.

Loss of Wide-Area Wireless Communications. Transmissions between the commercial vehicle driver and the commercial vehicle manager or fleet manager could be interrupted or blocked by accidental or intentional jamming of the wireless signals (see B.2.2). In addition, if there is high user demand for the communications system being employed (e.g., a cellular telephone service), the conversations could be distorted (e.g., crosstalk) or completely blocked. These types of interference would prohibit transmissions of new instructions or requests for mechanical roadside assistance. Impacts of such incidents might have significant effect on the many new and competitive "just-in-time" services offered by commercial carriers.

Loss of DSRC. If a CVS uses a DSRC technology that is incompatible with the roadside subsystems of various regional providers or transportation agencies, it will not be able to communicate with those roadside subsystems (e.g., CVCS). Without such a connection, several CVS functions cannot be performed.

Loss of Other Communications. The physical connections between the commercial vehicle's sensors and the on-board computer system could be cut, removed, or disconnected during regular operation or repair. Measurements of fuel usage, emissions, temperature, weight, and collision damage could go uncaptured. If conditions exceeded recommended or required limits, they could possibly jeopardize the safety of the driver, the vehicle, and the surrounding environment.

- **Impact of Disclosure**

  If others can access the CVS of other commercial carriers, they could read the on- board databases for route information, border-crossing information and inspection result: that the CVS makes available to commercial vehicle managers.

  Depending on the wireless communications method used (e.g., Enhanced Specialized Mobile Radio (ESMR), encrypted digital cellular telephone), the conversations between the commercial vehicle driver and the remote fleet manager or commercial-vehicle manager could be intercepted. The operator's cargo, routing, and delivery/pick-up information could be disclosed to competitors or potential thieves.

- **Impact of Manipulation**

  As noted in the data flow assessment (see tables A-3a and A-3b), transmissions between the Commercial Vehicle Check Subsystem (CVCS) and the Freight and Fleet Management Subsystem (FMS) are subject to manipulation threats. These messages contain commercial vehicle safety status, on-board HAZMAT, and financial/enrollment data that if accidentally or intentionally altered, could place the general traveling public in dangerous conditions.

- **Impact of Masquerading**

  As discussed above, if unauthorized users could assume roadside inspectors' identities and access their hand-held devices, they could modify the check and inspection results recorded for the vehicle inspections. With such capabilities, drivers could change the safety status of vehicles or drivers, thereby allowing the vehicle to pass through subsequent roadside checkstations. Depending on drivers' knowledge of the other information collected at roadside checks, they might be able to delete or decrease any assessed fines for safety violations as well as forego or delay the vehicle repairs that such violations might require. Tables A-3a and A-3b show the significance of the threat of masquerade to this subsystem's data.

- **Impact of Replay**

  A commercial driver knowledgeable of the CVS capabilities could arrange to continuously retransmit sensor data or tag data to the CVCS in an attempt to persuade inspectors that the commercial vehicle's CVS is operating incorrectly and must be turned off. With a CVS in need of repair and doubts about the reliability of the information transmitted to the CVCS, the commercial vehicle driver may be able to hide a safety problems or avoid enrollment requirements.

  Due to the nature of CVS data (i.e., safety, border clearance data), replay attacks are of significant impact to several CVS data flows (see tables A-3a and A-3b).

- **Impact of Repudiation**

  As noted in tables A-3a and A-3b, driver and fleet update massages are subject to the threat of repudiation.

4.4.2 Emergency Vehicle Subsystem

The Emergency Vehicle Subsystem (EVS) is a vehicle subsystem that provides processing, storage, and communications functions within the emergency vehicle in which it resides. The EVS includes two-way communications support using wide-area wireless technology for coordinated emergency response. In addition, each emergency vehicle is equipped with an automated vehicle location capability so that vehicle locations can be monitored, tracked, and managed. The EVS is designed to ensure that the appropriate emergency vehicle responds to each emergency situation.

The EVS performs the following functions:

- Provide the emergency vehicle driver with an interface to exchange:
  - HAZMAT information
  - Dispatch orders and information
  - Specific route plan
  - Incident status
- Provide the capability to request traffic signal priority and preemption (e.g., a green wave)
- Provide the ability to track the location of all emergency vehicles

Figure 4-18 illustrates associated ITS subsystems and terminators and provides exemplary data flows. Tables A-6a and A-6b contain the analyses for all EVS data flows.

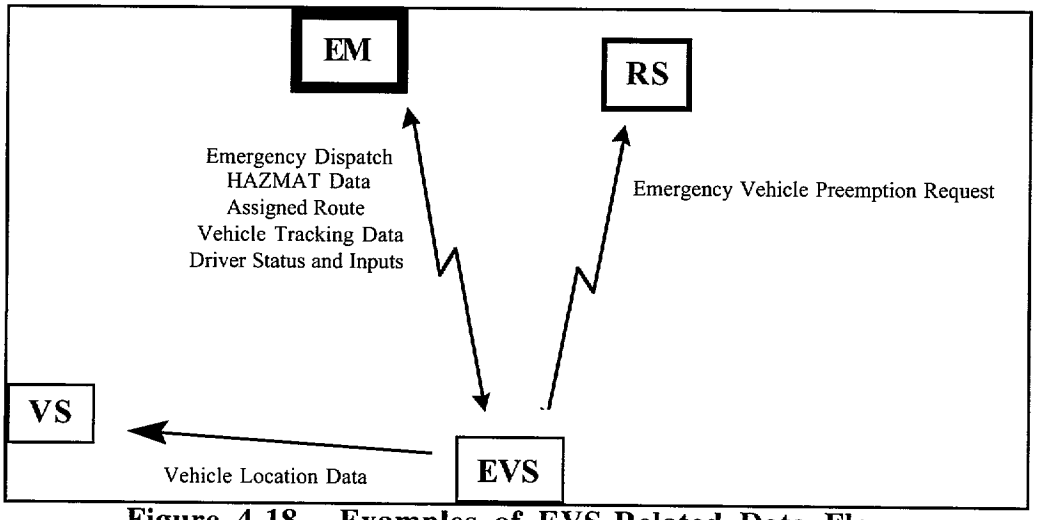


Figure 4-18. Examples of EVS-Related Data Flows

- **Impact of Denial of Service**

  EVS operations can be delayed, prevented, or mishandled in several ways.

  Absent or Inoperable EVS Devices. If the EVS computer system in an emergency vehicle is inoperable, the driver and EM personnel could not communicate with each other, and a prompt emergency response could not be accomplished.

  Absent, Inaccessible, or Unreadable Data. If the vehicle location data in the emergency vehicle is unreadable, then the Emergency Management subsystem (EM) could not track the vehicle's location and availability to respond to nearby emergencies. In addition, the route guidance capabilities in the vehicle might not be able to correctly direct the driver to an emergency.

  Absent or Unexecutable Software. If the EVS software that requests traffic-signal priority and preemption for the vehicle is inoperable, then the emergency vehicle would not be able to have local priority (i.e., green lights) at the traffic intersections.

  Loss of Wide-Area Wireless Communications. Any loss of communications between the emergency vehicle and the other emergency-related subsystems will result in the emergency vehicle receiving incomplete information. Such losses can cause the emergency vehicle to be delayed or to be inappropriately prepared for the emergency situation.

  If the emergency vehicle were unable to receive HAZMAT information, the driver and crew may arrive at the incident unprepared for unsafe or hazardous conditions. Improper handling of the HAZMAT situation could result in an escalation of the incident.

- **Impact of Disclosure**

  Based on the data flow assessment, unauthorized disclosure impacts to EVS are minimal (see tables A-6a and A-6b).

- **Impact of Manipulation**

  Manipulation of EVS data could cause emergency vehicles to be inappropriately re-routed. False information could be provided to emergency vehicle drivers (see tables A-6a and A-6b).

- **Impact of Masquerading**

  Along with the potential to manipulate data, there is also the potential for an individual vehicle to "masquerade" as an emergency vehicle. A criminal could steal or clone the equipment used by an emergency vehicle and then establish a "green wave" while fleeing from the scene of a robbery. This would also cause significant disruption to the local traffic. Tables A-6a and A-6b reflect the significance of masquerade attacks on EVS data.

- **Impact of Replay**

  Based on the data flow assessment (see tables A-6a and A-6b), the impact of EVS replay attacks are minimal.

- **Impact of Repudiation**

  Based on the data flow assessment, impact from the threat of repudiation is considered minimal (see tables A-6a and A-6b).

4.4.3 Transit Vehicle Subsystem

The Transit Vehicle Subsystem (TRVS) is a vehicle subsystem that primarily provides the sensory, processing, storage, and communications functions for the safe and efficient movement of passengers. The TRVS provides operational data to the Transit Management Subsystem (TRMS), receives transit network status updates and instructions, provides en route information to travelers, and provides security functions for both driver and passenger. Transit vehicles, like all vehicles -- personal, transit, commercial, and emergency -- contain the fundamental Vehicle Subsystem (VS). The TRVS uses wireline communications, DSRC, and wide-area wireless communications.

The TRVS performs the following functions:

- Provide a suite of communications capabilities, including:
  - Two-way voice communications between the transit vehicle driver and a facility
  - Two-way data communications between the transit vehicles and a facility
  - On-board safety sensor data transmitted from the transit vehicle to a facility
  - Data transmissions from individual facilities to a central facility for processing and analysis
- Provide security functions to monitor the safety of the transit vehicle using on-board safety sensors, processors and communications
- Furnish travelers with continuously updated real-time information from each transit system within the local area of jurisdiction
- Provide users with the latest available information on transit routes, schedules, transfer options, fares, real-time schedule adherence, current incidents conditions, weather conditions, and special events
- Support electronic fare collection
- Provide the capability for the transit vehicle to request signal priority or preemption

- Provide on-board trip monitoring to support fleet management, automatic vehicle location, automated mileage and fuel reporting, and auditing
- Collect transit vehicle maintenance data and automatically generate a preventative maintenance schedule for a particular transit vehicle
- Provide real-time condition monitoring on board the vehicle and automatic determination of optimum scenarios for schedule adjustment
- Collect accurate usage-level ("ridership") data

Figure 4- 19 illustrates associated ITS subsystems and terminators and provides exemplary data flows. Tables A-18a and A- 18b contain the analyses for all TRVS data flows.

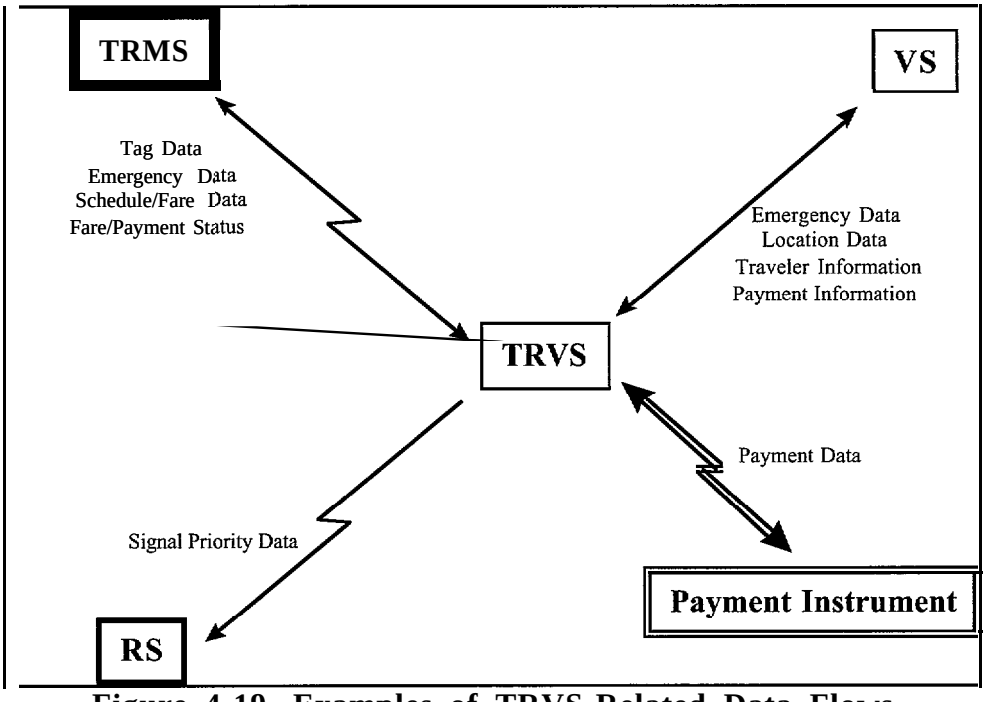


Figure 4-19. Examples of TRVS-Related Data Flows

- **Impact of Denial of Service**

  TRVS operations can be delayed, prevented, or mishandled in several ways.

  Absent or Inoperable TRVS Devices. The transit vehicle may not have the sensors for determining characteristics such as passenger loads and transit vehicle running times. Without this information, schedule deviations could not be determined and the operational data required for transit vehicle planning (e.g., bus size, number of buses, routes, and fares) could not be collected.

Absent, Inaccessible, or Unreadable Data. If the transit vehicle fare data in the TRVS are deleted or unreadable, transit vehicle fares could not be calculated.

Absent or Unexecutable Software. Similarly, having no transit vehicle fare data is equivalent to having an inoperable TRVS fare-calculation process. Without the process, transit vehicle fares could not be calculated.

Loss of Wireline Communications. The TRVS communicates with the VS, which is also on board the transit vehicle, via a wireline connection. The loss of this communications path would prevent the TRVS from exchanging traveler advisory and payment information as well as vehicle location data with the VS.

Loss of Wide-Area Wireless Communications. Loss of the wide-area wireless communications between the TRVS and the TRMS would isolate the transit vehicle. This would prevent the exchange of vital public safety information (e.g., emergency conditions or "mayday" messages) as well as financial information (e.g., fare and payment data).

Loss of DSRC. Loss of DSRC would prevent the TRVS from communicating with roadside subsystems for signal priority requests, etc. This loss would also prevent the roadside subsystems from communicating with the Vehicle Subsystem (VS) -- also on board the transit vehicle.

- **Impact of Disclosure**

TRVS transactions occasionally involve emergency information that is often not in the public interest. The TRVS also exchanges financial information, some of which pertains to an individual citizen. The improper disclosure of such information has substantial legal implications. A traveler's identity, trip routing information, etc. could also be disclosed to criminal and/or terrorist organizations (see tables A-18a and A- 18b).

- **Impact of Manipulation**

The emergency data that the TRVS processes are essential to general public safety. Unauthorized or improper manipulation of these data would pose a significant threat to the general public (see tables A-18a and A- 18b). Additionally, the payment messages processed by the TRVS may be an appealing criminal target. Manipulation of fare and fare violation data would at least temporarily corrupt the accounting systems until an audit or other corrective action was completed.

- **Impact of Masquerading**

A masquerade could lead to the impacts discussed in the preceding paragraphs. In addition, a masquerade within the TRVS could result in mis-information regarding emergency data, signal preemption, transit driver instructions, financial information, traveler identity, and/or trip route. All could be used for criminal and/or terrorist intentions. Tables A-8a and A- 18b reflect the significant threat of masquerade attacks on TRVS.

- **Impact of Replay**

  Replay of TRVS emergency or signal preemption data could pose a significant threat to the general public (see tables A-18a and A-18b). The TRVS messages handling financial transactions are also targets for replay attacks, presumably for criminal purposes.

- **Impact of Repudiation**

  Financially related TRVS messages are also obvious targets for repudiation (see tables A-18a and A-18b).

4.4.4 Vehicle Subsystem

The Vehicle Subsystem (VS) provides the sensory, processing, storage, and communications functions necessary to support efficient, safe, and convenient travel by personal automobile. Note that the VS is a subsystem that resides in *all* vehicles, whether they are personal, transit, commercial or emergency vehicles.

Among the services and information provided by the VS are the following:

- Current travel conditions
- Availability of services along the route and at the destination
- Route guidance resulting in an optimal route, as well as step-by-step guidance along the travel route
- Both one-way and two-way communications options support a spectrum of information services from low-cost broadcast services to advanced, pay for use personalized information services
- Collision avoidance functions provide “vigilant co-pilot” driver warning capabilities
- Support for automated vehicle operation through advanced communications with other vehicles in the vicinity and in coordination with supporting infrastructure subsystems
- Pre-crash safety systems
- Emergency notification messages

Figure 4-20 illustrates associated ITS subsystems and terminators and provides exemplary data flows. Tables A-19a and A-19b contain the analyses for all VS data flows.

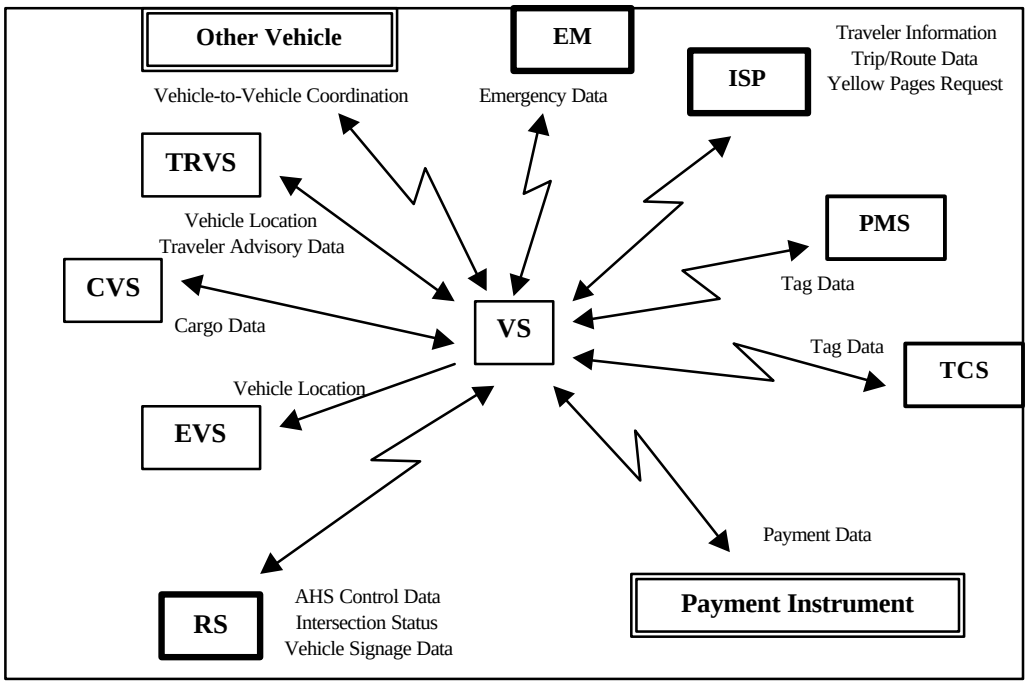


Figure 4-20. Examples of VS-Related Data Flows

- **Impact of Denial of Service**

  VS operation can be delayed, prevented, or mishandled in several ways.

  Absent or Inoperable VS Devices. The vehicle may have an inoperable vehicle IS tag or on-board processor(s) on which the VS depends. If so, then automated functions such as the payment of parking and tolls cannot be performed.

  Absent, Inaccessible, or Unreadable Data. A computer virus could render the vehicle's map data unreadable. Without this information, an optimal route, as well as step-by-step guidance to the desired destination, could be generated for the driver.

  Absent or Unexecutable Software. The VS software that reads and analyzes the vehicle's sensors data could have programming errors (either accidentally or intentionally introduced). Without such, software, the hazardous roadside conditions (e.g., flooding,

snow, freezing temperatures) might not be recognized and the driver would not be forewarned.

Loss of Wireline Communications. Note that the VS communicates with the specialized subsystems aboard transit, commercial, and emergency vehicles via a wireline connection (e.g. in-vehicle bus or LAN). The loss of this communications path would prevent the VS from exchanging control, location, emergency, intersection status, payment, and advisory information with the TRVS, CVS, and EVS.

Loss of Wide-Area Wireless Communications. Loss of the wide-area wireless communications would prevent the exchange of emergency information (e.g. a "mayday" message) with the EM. Less critically, this communications loss would also prevent the VS from exchanging traveler and trip information, "yellow pages" information, etc. with the ISP.

Loss of DSRC. DSRC loss would isolate the vehicle and possibly create a threat to public safety. Loss of this communications would prevent the vehicle from communicating with the RS, depriving the VS of AHS control, intersection status, and signage data.

Loss of Vehicle-to-Vehicle Communications. Vehicle-to-vehicle communications loss due to either intentional threats (e.g., roadside jamming), accidental threats (e.g., a hardware failure), or natural disasters would isolate the VS from systems in other vehicles. Platooning and other AHS functions that require a high degree of availability would be severely affected and subsequently create a significant threat to public safety.

- **Impact of Disclosure**

VS transactions occasionally involve information that is often not in the public interest (e.g., emergency or financial information). Some of this information might pertain to an individual, and the improper disclosure of such information could have substantial legal implications (see tables A-19a and A-19b).

- **Impact of Manipulation**

As noted in tables A-19a and A-19b, the emergency coordination, AHS control, intersection status, and weather condition data processed by the VS is essential to public safety. Unauthorized or improper manipulation of these data would pose a significant threat to the general public. Additionally, payment messages processed by the VS may be an appealing criminal target.

- **Impact of Masquerading**

A masquerade could lead to the impacts discussed in the preceding paragraphs. In addition, a masquerade within the VS could result in mis-information regarding payment or traveler identity data that could later be used with unlawful intent. The significance of the threat of a masquerade in VS is reflected in tables A-19a and A-19b.

- **Impact of Replay**

  Along with the financial-related massages, toll transactions are susceptible to replay attacks, presumably for illegal purposes (see tables A-19a and A- 19b).

- **Impact of Repudiation**

  The VS's financial-related messages are also targets for repudiation (see tables A-19a and A-19b).

4.5 TRAVELER SUBSYSTEMS

These subsystems represent platforms for ITS functions of interest to travelers or carriers (e.g., commercial vehicle operators) in support of multimodal traveling. They may be fixed (e.g., kiosks or home/office computers) or portable (e.g., a palm-top computer), and may be accessed by the public (e.g., through kiosks) or by individuals (e.g., through cellular phones or personal computers). This section describes the two traveler subsystems.

4.5.1 Personal Information Access Subsystem

The Personal Information Access Subsystem (PIAS) is a traveler subsystem that provides methods for the traveler to request and receive information concerning trip planning, trip routes, reservations, etc. from an Information Service Provider (ISP). The traveler may be using a hand-held personal digital assistant (PDA) or a personal computer from home or at work. Trip requests and responses are sent by wireline or wireless communications.

While en route, the traveler may use a portable device to generate an emergency notification to Emergency Management (EM), perhaps when the traveler observes an accident. The traveler might also request a route change in real time from the Transit Management Subsystem (TRMS) to avoid traffic congestion or construction. Real-time requests are generated using wide-area wireless communications. Responses are provided by either wireline or wireless communications.

Finally, the PIAS may request and receive payments from a payment instrument such as a smart card or automatic teller machine (ATM) card. Payment requests and the corresponding payments are provided with localized hardware, such as a pinstripe or smart card reader.

Figure 4-21 illustrates associated ITS subsystems and terminators and provides exemplary data flows. Tables A-9a and A-9b contain the analyses of all PIAS data flows.

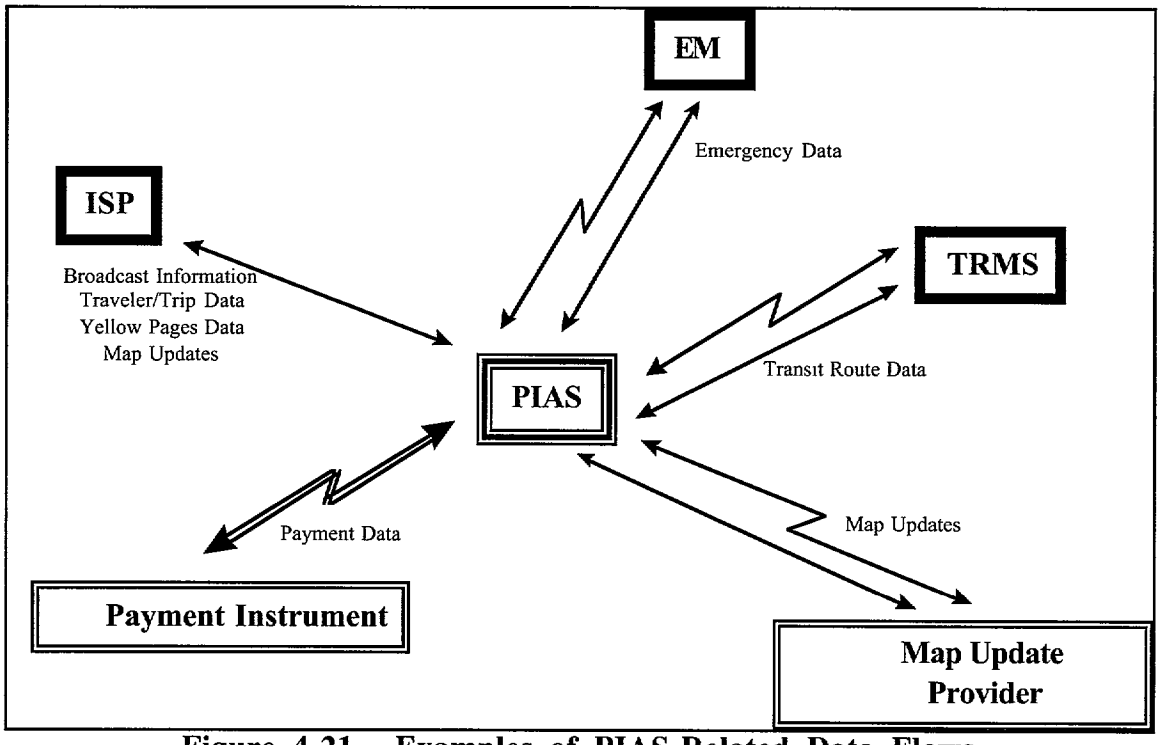


Figure 4-21. Examples of PIAS-Related Data Flows

- **Impact of Denial of Service**

  PIAS operations can be delayed, prevented, or mishandled in several ways.

  Absent or Inoperable PIAS Devices. If a traveler's PDA is inoperable (e.g., the battery no longer provides power), they could send neither requests for trip routes nor requests for emergency assistance using that device.

  Absent, Inaccessible, or Unreadable Data. If the map or routing databases that are used to prepare a trip plan for a traveler are inaccessible, the resulting trip plans would be incomplete and the traveler would not be forewarned of the traffic or weather conditions affecting his or her trip.

  Absent or Unexecutable Software. If the PIAS software in the traveler's PDA or personal computer is inoperable or obsolete (e.g., some subsystems using a newer version of the application software than the traveler), the traveler may not be able to obtain traveler information.

Loss of Wireline Communications. If wireline communications were lost, the traveler would not be able to transactions from home or office PCs. Any severely delayed transactions could cause public distrust in the system. Additionally, as more travelers become accustomed to an on-line trip-routing feature, delays and disruptions could cause problems in various service reservation systems. Travelers who have attempted to book trips could find their travel plans delayed or rescheduled. If confirmations were not returned, travelers might find that their reservations are not valid.

Loss of Wide-Area Wireless Communications. Wide-area wireless communications loss would delay or deny the traveler's ability to generate an emergency notification. If travelers are unable to send an emergency alert, then an emergency response will be delayed until notification occurs by alternate means. If a travelers send emergency alerts and do not receive acknowledgments, then they could saturate the EM with notices. If highway patrols use the same technology to generate emergency notifications, those messages would also be delayed or blocked.

- **Impact of Disclosure**

The PIAS is subject to several threats of disclosure. First, the traveler's proposed or final itinerary could be subject to snooping. Unauthorized users who obtain the traveler's itinerary could plan the following attacks:

- Rob the traveler's house while the traveler is away
- Rob the traveler en route
- Stalk the traveler with other criminal intent

Another, less harmful attack could occur if the traveler's standard routes to and from work were collected and sold to local vendors. These vendors could then solicit the traveler. This could become the basis of telemarketing, which many people consider intrusive and disruptive.

Credit card information is also transmitted by the PIAS If a snooper could obtain this information, they could make unauthorized purchases on the traveler's credit card. Tables A-9a and A-9b indicate the PIAS data subject to the threat of unauthorized disclosure.

- **Impact of Manipulation**

Damaged or altered trip information could have serious impacts on traffic congestion. For example, if a traveler requests a route around an accident and is instead directed into the accident, the traveler's vehicle would at the least be delayed, and at worst, could become a part of the accident.

In a slightly different scenario, the traveler could be given a route with incomplete instructions (perhaps due to a request error) and the traveler could arrive in a dangerous environment or lose their way. Tables A-9a and A-9b show the PIAS data threatened by unauthorized manipulation.

- **Impact of Masquerading**

  The data flow assessment results indicate the threats of masquerading in PIAS For example, if user or vehicle identification information is stored in the traveler's PC or PDA, and the device is stolen, the thief could masquerade as another traveler.

- **Impact of Replay**

  The impact of successful replay attacks of traveler request and payment messages is shown in tables A-9a and A-9b.

- **Impact of Repudiation**

  Since the PIAS deals with payment requests and confiiations, the traveler could make a payment and then later deny that it had been made (see tables A-9a and A-9b).

4.5.2 Remote Traveler Support Subsystem

The Remote Traveler Support Subsystem (RTS) is a traveler subsystem that travelers use to access travel information at transit stations, transit stops, other fixed sites along travel routes, and at major trip-generation locations such as stadiums, concert halls, hotels, office complexes, amusement parks, and theaters. The RTS uses wireline communications exclusively in its interactions with other ITS subsystems.

Access points to the RTS's travel information may take several forms, from kiosks to simple displays providing schedule information and notices of imminent arrivals. At major trip generation sites, additional information and services may be provided to help the traveler select the best travel modes and routes. These include traffic condition alerts, fare-card vending, yellow pages, transit schedules, etc. When the traveler supplies additional information, the system can respond with more customized routing advice.

Additionally, this subsystem supports public safety monitoring using surveillance equipment such as CCTV cameras and emergency notification within these public areas. Fare card maintenance, and other features which enhance traveler convenience may also be provided at the discretion of the deploying agency.

Figure 4-22 illustrates associated ITS subsystems and terminators and provides exemplary data flows. Tables A-13a and A-13b contain the analyses for all RTS data flows.

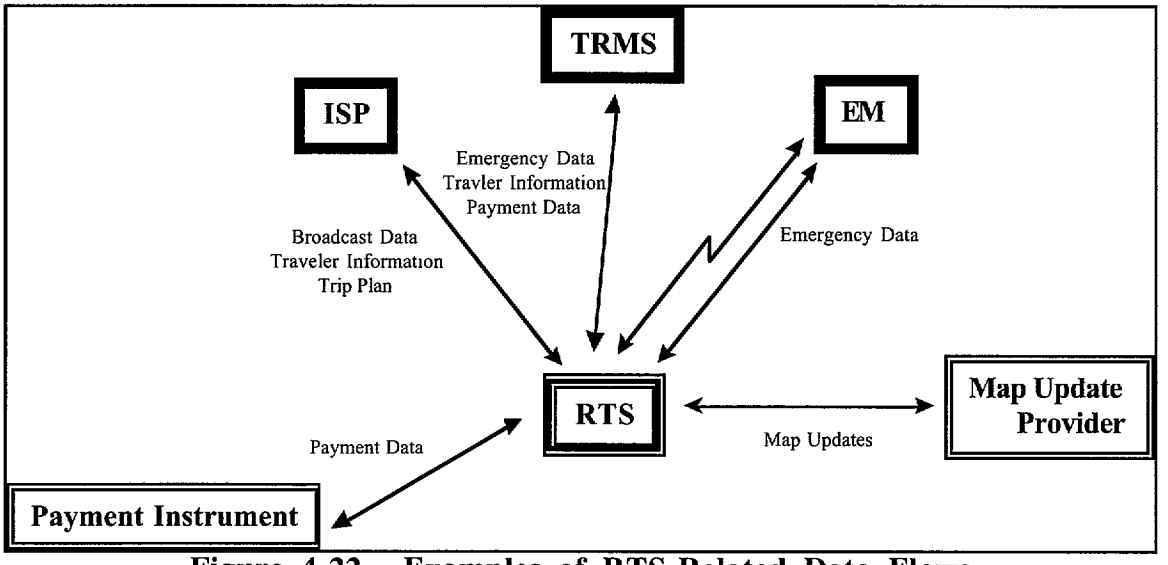


Figure 4-22. Examples of RTS-Related Data Flows

- **Impact of Denial of Service**

  RTS operations can be delayed, prevented, or mishandled in several ways.

  Absent or Inoperable RTS Devices. The information kiosk could be inoperable due to vandalism, natural disaster, etc. Without the kiosk, travelers would not be able to request any of the RTS services such as traffic condition alerts. Without the latest alerts regarding highway conditions and detours, travelers' safety could be endangered and their trips unnecessarily prolonged.

  Absent, Inaccessible, or Unreadable Data. If transit schedule information at an RTS access point is absent, travelers would need to use other less convenient and less accurate methods to obtain the information. If the data are obsolete, travelers would be misinformed about the re-scheduled mass-transit services (e.g., last bus to the airport).

  Absent or Unexecutable Software. If the RTS emergency notification software is inoperable, then travelers would not be able to report local emergency conditions. Other methods, such as a public telephone (if available), would need to be used instead.

  Loss of Wireline Communications. If the RTS were not able to communicate with the other ITS subsystems, most of its functionality would be lost. Only static, locally-stored information would be available to the traveler.

- **Impact of Disclosure**

  The RTS is vulnerable to threats of disclosure, particularly since this subsystem often uses personal financial information. As discussed earlier in regard to the PIAS, an attacker could obtain credit information and make unauthorized purchases. In addition, a traveler's location could be considered sensitive information under certain circumstances.

  Alternatively, an intruder could plant Trojan Horse code in the RTS computer system to record items of interest such as user names, addresses, and credit information. That information would be sufficient to make unauthorized purchases.

  Tables A-13a and A-13b reflect the RTS data flows subject to unauthorized disclosure.

- **Impact of Manipulation**

  The most critical function of the RTS is emergency notification and acknowledgment. If emergency messages were lost or garbled, emergency response would be severely hampered. As a more detailed example, when a traveler files an emergency report, the traveler's image is captured for later use in finding the traveler. If this-image were distorted, either by accident or on purpose, the traveler might not be identified.

  As another example, if credit information were incorrectly captured or garbled in transmission, payments could not be processed. Services would be rendered, but no payment would be received. Manipulation could also be used to alter the amount of a payment during a roadside request for service, or to change the receiving account information.

  Tables A-13a ad A-13b reflect these findings and indicate the RTS data flows subject to the threat of unauthorized manipulation.

- **Impact of Masquerading**

  Masquerading could be used to submit phony emergency reports or to generate phony acknowledgments to emergency reports. Since the RTS captures the image of the person making the emergency report, a masquerading attack could be enhanced by altering the captured image: bogus emergency messages could be transmitted and the sender's identity obscured. The data flow assessment reflects the significance of masquerade threats to RTS.

- **Impact of Replay**

  Replay could be used to mimic a response from the Emergency Management subsystem (EM) to the traveler. Another replay attack would be to send one or more duplicate payment requests or responses (see tables A-13a and A- 13b).

- **Impact of Repudiation**

  As noted in tables A-l 3a and A- 13b, travelers could deny requesting and receiving chargeable service.

4.6 SUBSYSTEM SECURITY SERVICES

This section discusses the security services that are relevant to each ITS subsystem. Since the subsystems have been grouped by similar functionality and location per the National ITS Architecture, the security services are addressed using the same approach.

4.6.1 Center Subsystems

Center subsystems (i.e., CVAS, EM, EMMS, FMS, ISP, PS, TAS, TMS, and TRMS) typically provide functions associated with public/private administrative, management, and planning agencies. They can be viewed as the "nerve centers" of ITS. Since center subsystems support capabilities such as business transactions, traffic control and management, and emergency coordination, only authorized users should be allowed to access subsystem computers, networks, and the facilities that house those computing resources.

Center subsystem users may involve operators or other workers employed by the public/private agency; help desk personnel who may on occasion require access to operational data (e.g., instructions for controlling traffic via roadway messages); and system and application programmers who will access program code as well as operational data. Each of these types of users will require various types of access to subsystem data and programs to perform their jobs properly. However, prior to gaining access to the computer system, all users must identify themselves to the subsystem. Typically, users identify themselves using their unique, pre-assigned user IDs. This user ID is then authenticated using a static password. This form of authentication is considered "weak" since passwords are easily guessed, often posted next to the computer terminal/workstation, shared between users, and are susceptible to replay attacks. However, depending upon the current security policy, the data sensitivity , and the function criticality, weak authentication may suffice. "Stronger" authentication may include encrypted passwords, one-time passwords, challenge-response schemes, public key cryptographic mechanisms, or biometrics (see appendix E). Such types of strong authentication should be used at least for remote access to the center subsystems with Internet, private network, and/or dial-up capabilities.

As stated in section 3.4.1, authentication provides the basis for additional security services, namely, access control and auditing. Users should be provided with the proper level of access to system files, processes, etc. required to perform their jobs -- and no more. The principle of "least privilege" should be the default in center subsystems. Those users with access to all system capabilities could not only place the ITS center subsystems at risk, but also the travelers dependent on those subsystems. Placing restrictions on user access via *access control* techniques helps control and limit in real-time the amount of damage that could be incurred. For example, a disgruntled system programmer -- if not limited with regard to system capabilities associated with his/her user ID -- could access traffic management functions and modify roadway messages or traffic signals, or less significantly, display disrespectful messages on variable message signs.

Auditing, on the other hand, is a passive security service that provides information in retrospect. Audits or logs capture user activity and can provide administrators and legal

authorities with evidence of computer system activity. Auditing requires regular review, and depending on the number of activities and users audited, auditing can require significant processing resources. Several products offer reduction capabilities to assist in processing audit data.

Often, organizations refrain from using complicated and expensive security measures and enforce strict security policies. These policies indicate that all system activity is subject to auditing and that activity performed outside the normal job description is grounds for dismissal.

In addition to business applications such as maintaining tax records and payment capabilities, several of the center subsystems perform critical functions (e.g., emergency response coordination, traffic management). Because such functions are critical to public safety, subsystem *availability* and data *integrity* are particularly important. Without back-up capabilities for both systems and communications, emergency requests could go unanswered and subsequently jeopardize public safety. Additionally, databases used for assisting emergency personnel must be accurately maintained else appropriate emergency response could be delayed.

Data integrity is also important for financial and business applications such as toll assessments. Corrupted toll accounts or commercial vehicle registration databases could result in incorrect billing and lead to consumer distrust in ITS. However, without *non-repudiation* services, toll and tax billing records could be refuted by individual travelers and commercial freight companies.

Personal data (e.g., traveler identity, credit identity, current location, and travel plans) and sensitive organization data (e.g., companies' credit identities, commercial vehicle route plans, and inspection records) that the center subsystems store and process all require *confidentiality* protections against unauthorized disclosure.

Since center subsystems will perform traditional information system functions, they too should utilize *system security management* practices. Good system security management includes: an organization information security policy; clearly delineated roles and responsibilities (separation or division of function/duties); system configuration management; training; back-up/recovery, and management of user accounts (system administrators need notification when employees leave, retire, or are terminated).

Other important system security management practices include:

- Controlling physical access to the subsystem facility: potential hackers may attempt to gain entry to the facility. Once inside, these individuals may cause significant damage (e.g., steal or damage ITS equipment, attempt to gain system access). Locks, keyless entry systems, and security guards represent some of the methods for securing a subsystem facility.

- Alternating subsystem activities so that potential hackers or unauthorized individuals are not able to obtain information or observe operational procedures: if outsiders or insiders were

to gain knowledge regarding subsystem update schedules, they could then have an advantage in electronically or physically attacking the subsystem.

- Screening employees in sensitive positions: personal and credit checks conducted by state, local, or private human resources departments as part of the interview process may be sufficient for identifying potential wayward or disloyal employees. Another option involves running state and local record checks for potential employees.

4.6.2 Roadside Subsystems

Roadside subsystems are positioned near the roadway to interface with travelers, vehicles, and the roadside environment. These subsystems perform parking management, toll/fee collection, and roadside-to-vehicle communications functions, and they consist of sensors, signals, programmable signs, and communications equipment.

Roadside subsystems (i.e., RS, PMS, CVCS, and TCS) process, store, and transmit a wide variety of data. Vehicular and multimodal traffic and signal control information passes through these subsystems -- indicating the necessity for data *integrity*. Modification of safety-related data while in transmission and/or in storage could place public safety at risk.

Toll and parking data involve financial transactions and may include personal location. These types of data require that integrity, *non-repudiation,* and *confidentiality* protections be considered. Similar to the center subsystems, incorrect toll or parking bills could result in the loss of revenue or refutable customer charges. Privacy is a major issue for ITS and requires that protections be applied appropriately and according to public law.

Due to the safety data (e.g., commercial vehicle inspection information), financial data (e.g., toll tag data), and personal data (e.g., incident or violation data) processed by these subsystems, users need to *authenticate* (see section 4.6.1 above) themselves prior to gaining subsystem access. Due to the weaknesses in traditional passwords, remote access to the roadside subsystems requires “strong” authentication techniques. “Stronger” authentication may include encrypted passwords, one-time passwords, challenge-response schemes, public key cryptographic mechanisms, or biometrics (see appendix E). Such types of authentication should be used at least for remote access (e.g., for maintenance purposes) to the subsystems from the Internet, private networks, and/or dial-up. As discussed for center subsystems, *access control, auditing,* and *availability* should be considered.

If the particular roadside subsystem is staffed, the same *system security management* protections used at a center subsystem may apply to a roadside subsystem.

4.6.3 Vehicle Subsystems

As the name implies, vehicle subsystems (i.e., VS, EVS, CVS, and TRVS) are located in vehicles, and are of four types: privately owned, transit, commercial, and emergency. Along with this broad range of vehicle types is an associated broad range of functional capability and data types. Many are similar to those already identified in the center and roadside subsystem discussions.

To gain access to a vehicle subsystem, user *authentication* may not be required. However, authentication may be needed for other capabilities provided by the vehicle subsystem such as chargeable or payment related transactions (i.e., financial) or emergency response coordination. *Access control* may be required only for transit systems to ensure that only authorized operators access the on-board system. Additionally, the on-board system may store and access traveler identities or credit identities. This data should be protected from disclosure (i.e., from any traveler using the system). Likewise, the *confidentiality* and *integrity* of such data are important for continued public/consumer trust.

The capability to provide *non-repudiation* services to travelers in both privately owned and transit vehicles is important for all chargeable and payment transactions.

While important to the vehicle subsystem, subsystem *availability* is of primary concern to emergency and commercial vehicles. Although, all vehicles can operate without the onboard system, they may do so at the risk of public safety.

Several components of *system security management* are important for vehicle subsystems. Specifically, the need to ensure that all vehicle subsystems are maintained and configured properly and that upgrades and repairs are performed correctly. For example, some form of *auditing* may be required to document repairs and system configuration changes. Tamper-proof or resistant features should be utilized to prevent vandals from modifying an on-board system. Likewise, mechanisms to alert travelers that their vehicle subsystem has been modified should also be utilized.

4.6.4 Traveler Subsystems

Traveler subsystems (i.e., RTS and PIAS) provide various types of traveler information and traveler support ranging from multimodal reservation services to emergency/security requests for assistance. This information can be obtained from kiosks located in major public areas as well as from pedestrians and other travelers using portable and personal computers.

Like vehicle subsystems, the necessity for *authentication* will depend upon the service requested. For transit maps or schedules, authentication normally would not be required since a fee would not be charged. However, fee-for-service transactions (e.g., trip and routing plans) may require authentication regardless of whether the request originated from a kiosk or a personally owned system. Due to the portability of palm-top, laptop computers, and personal digital assistants (PDAs), authentication (e.g., a Personal Identification Number (PIN)) may be necessary to protect the personal information stored in the device. Furthermore, personal information (e.g., credit identity, travel plans) may require additional protections such as encryption to ensure *confidentiality.*

Integrity is important for the financial transactions that the traveler subsystem processes and for the data provided at the traveler subsystem. Additionally, *non-repudiation* services must also be supported.

Access control may be necessary for certain admittance to the RTS (e.g., kiosk maintenance). Likewise, *auditing* of RTS maintenance, updates, and activity records may be necessary. Neither access control nor auditing is necessary for personal computers used to access PIAS services. *The availability* of the RTS is important primarily for emergency coordination at public locations. However, availability is also important for continued customer satisfaction and support of ITS.

System security management applies to both the PIAS and the RTS.

SECTION 5

CONCLUSIONS AND RECOMMENDATIONS

The ITS program is the application of information technologies (computing, sensing, and communications) to surface transportation. Because of a reliance on these technologies, ITS will become increasingly dependent on information security. By understanding how to achieve and maintain secure systems, the ITS community can develop comprehensive information security practices and appropriate security policies for ITS programs. Subsequently, they can put these into practice. The following summarize Mitretek's conclusions and recommendations to help accomplish these goals.

Information Security Awareness and Policy Development

1. *The surface transportation community is largely unaware of the significance of information security. Secure ITS will require an enhanced awareness of information security issues and the continued development **of** information security policy. State and local ITS implementors will need to be more cognizant **of** information security, and the industry as a whole will need to pursue the development and implementation **of** information security policy.*

   ITS information security awareness and policy development should include the following activities:

   - Developing an ITS information security program that provides guidance to those who will oversee the acquisition, installation, operation, and maintenance of ITS-based systems.

     High-level overviews could provide both management and field personnel with strategic information for implementing and maintaining necessary information security needs.

   - Clarifying ITS information security policy and its applicability (if any) at national, state, and local levels.

     Apart from the ITS industry's *Fair Information and Privacy Principles*, little effort has been expended to address information security within ITS. Additional policy issues must be resolved in order to develop and maintain secure ITS. Because many information infrastructure components are owned and operated by the private sector, it is essential that the government and the private sector work together to develop a strategy for protecting these components and for ensuring their continued operation. Policy makers should encourage participation at various government levels as well as within the private sector and should disseminate potential policy for public review.

   - Coordinating with the President's Commission on Critical Infrastructure Protection and its Information Protection Task Force (IPTF), the National Security Telecommunications Advisory Committee (NSTAC) Information Infrastructure Group (IIG), the National Science and Technology Committee (NSTC), and the International Institute for Surface Transportation Policy Studies (IISTPS).

The IPTF is focused on assessing the security of critical infrastructures (including transportation); addressing the legal and policy issues regarding the protection of these infrastructures; and recommending a comprehensive national policy and implementation strategy for protecting these critical infrastructures. Relatedly, the IIG is involved with identifying the potential impacts of new technologies (e.g., ITS) on national security and emergency preparedness (NS/EP) telecommunications. Activities from the NSTC are currently focused on investigating information security within different modal transportation systems (including ITS). The IISTPS has begun to address some aspects of security (e.g., physical or procedural) on current transportation systems around the world. Collaboration among these groups' security efforts could expedite both security awareness and security policy development within the surface transportation community.

ITS Security Analysis

The following conclusions and recommendations are derived from Mitretek's security analysis comprising assessments of the ITS subsystems, the ITS data flows, and the ITS communications infrastructures. The three assessments represent a high-level, initial foundation that, when combined with appropriate oversight activities and policy development, can serve as an effective guide towards protecting ITS from potential security threats. Detailed observations from the subsystem, the data flow, and the communications infrastructure assessments are provided in sections 4.2 to 4.5, section A.3, and section B.3, respectively.

1. *Due to the scope of the National ITS Architecture documents, information security requirements were not thoroughly considered. Currently, there is neither a Security Architecture nor a Security Policy for ITS that, at minimum, articulates high-level ITS security objectives.*

   - Support the information security awareness and policy development activities noted above. Resulting security requirements should be adopted consistently throughout ITS (e.g., subsystems, data flows, and supporting communications infrastructures).

2. *Since ITS encompasses a wide range of information (e.g., HAZMAT, traffic control, safety, financial, and personal privacy), it is also susceptible to various attacks. As noted in sections 4.2 through 4.5 and in sections B.2.1 through B.2.5, significant threats may involve actions such as the following:*

   - Hacker penetration of computers and networks
   - Accidental "insider" manipulation of data and system configurations
   - Disgruntled "insider" manipulation of data and system configurations
   - Terrorist attacks against or involving transportation systems
   - Interception of wireless transmissions

   Either intentional or accidental incidents that disrupt or compromise ITS could lead to significant public safety and emergency response effectiveness concerns, corruption of financial transactions and records, violation of citizen privacy, and a loss of ITS credibility.

- ITS system designs should include measures to protect against a wide range of security threats. Security services (e.g., authentication, access control, audit, etc.) and the infrastructures to support such services must be integrated into the overall system design to provide adequate security. Due to the rapid evolution of information technologies, no security solutions will be permanent, but it is essential to develop a foundation on which further enhancements to ITS security can be developed.

3. *ITS executes two general types of processes:*

   Mission-Critical Processes *-- Functions such as traffic control and emergency response must operate continuously and the data exchanges involved cannot be delayed.*
   Delay-Tolerable Processes *-- Functions such as special event coordination information for use in strategic traffic planning can be rescheduled if processing or communications services are unavailable.*

   - As exemplified in sections 4.2 through 4.5, most ITS subsystems execute both mission-critical and delay-tolerable processes in performing their intended functions. Therefore, the following conditions must be satisfied:

     - The software, hardware, data, and communications technologies involved must be available and operable to support the mission-critical processes.

     - Appropriate security services must operate to ensure such processes' correct operation and performance.

     - The proper system security management practices must be in place to ensure that unavailable systems are promptly made available again.

4. *Effective, efficient, and secure ITS operations require properly trained personnel to manage and operate ITS subsystems. The use of proper security services (e.g., authentication, access control, auditing, etc.) to combat both internal and external threats require significant planning, design, and interoperability considerations. Employee training and awareness should be considered as supplements to, not substitutes for, automated security techniques.*

   - Management should address both intentional and accidental "insider" and "outsider" threats by means of proper authentication, access control, and auditing mechanisms. Provide employee training to supplement these automated mechanisms. Consider using background checks for ITS personnel in critical positions.

5. *ITS relies on the collaborative operation **of** many individual subsystems. These subsystems, in turn, depend on communications technologies that are expected to operate without interruption, error, or delay. The denial-of-service impacts discussed in sections 4.2 through 4.5 effectively illustrate the potential consequences **of** such dependencies when backup facilities are not provided.*

   - Develop contingency plans for backup, recovery, and degraded performance of ITS operations. Consider the use of both redundant systems and geographically and electronically diverse communications. Develop plans for ITS subsystem backup, recovery, "off-nominal"/crisis response, and down-time avoidance.

6. *The security assessments reveal that ITS uses four types **of** data, each **of** which needs to be adequately protected against unauthorized disclosure, manipulation, and in some cases, replay.*

   ***Mission-Related Data** -- Traffic management data, **for** example, are used to control traffic signals and variable message signs; the emergency management facilities use real-time traffic and vehicle-location information to respond to emergencies. This type **of** data has a critical sensitivity to manipulation.*

   ***Personal and Private Information** -- Many ITS subsystem functions require the identities **of** vehicle drivers by their names, Social Security Numbers, credit-card IDs, and current locations. This type **of** data has a critical sensitivity to unauthorized disclosure.*

   ***Control Information** -- Communications technologies require specific transactions to configure the proper connections between ITS subsystems. Additionally, traveler information software employs configuration options to display information in private or commercial vehicles. This type **of** data has a critical sensitivity to manipulation and replay.*

   ***Summary and Statistical Data** -- Many ITS subsystems provide summaries **of** their operations **for** use by traffic planners in forecasting traffic and road conditions. The aggregated data is often more important to such planners than detailed or specific information This type **of** data has a critical sensitivity to disclosure (business data) and replay.*

   - Identify appropriate data types to allow the proper protection of information and to subsequently provide safe and secure ITS operations. Include the use of standard formats, metrics, and levels of protection for ITS data flows.

7. *The hardware and software comprising ITS subsystems should be interoperable. Interoperability is enhanced by not only the use **of** standard communication protocols, message sets, etc., but also by the use **of** standard security mechanisms (e.g., data encryption techniques). While open to flexibility, system designs (including any supporting communications infrastructures) should consider appropriate standards to aid interoperable, and therefore, more effective, more efficient, and more secure ITS operations.*

   - Adopt existing standards (or if necessary establish new standards) to allow for subsystem interoperability and secure ITS operations. Consider the standards for infrastructures that may be needed to support these subsystems (e.g., the Public Key Infrastructure required for managing public encryption keys).

Continuation of ITS Information Security Activities

1. *By identifying the range **of** potential threats (i.e., the threat categories) **for** the ITS subsystems, their supporting transportation infrastructure, and the information exchanged among these systems, the National ITS Architecture security analysis has established a basis **for more** complete and specific ITS information security needs. Some aspects of regional or local system designs/implementations will differ, but each should be able to use these assessment results **for** identifying initial needs and for continuing more comprehensive ITS security efforts*

Future ITS information security activities should include the following:

- Verifying the security assessments described and presented in this document. Reviewing the processes and results of the ITS subsystems assessment, the ITS communications infrastructure assessment, and the ITS data flow assessment would not on only contribute to security awareness (along with participation in oversight activities), but it would also provide a basis for further and more detail security efforts.

- Conducting an information security assessment of a system that is currently implementing (or will be implementing) parts of the National ITS Architecture; or perhaps one that does not follow the Architecture.

  Paper analyses provide numerous benefits including the ability to make necessary corrections early in the design phase. However, to maximize the benefits for those who will later build to an architecture (e.g., the National ITS Architecture), the analysis of an existing system would provide significant and realistic feedback.

.

REFERENCES

Text References

[CSI, 1993] Computer Security Institute, 1993, *Practical Methods for Information Systems Risk Analysis,* Washington, D.C., Computer Security Institute

[CSI, 1994] Computer Security Institute, 1994, *CSI Manager's Guide to Computer Security Awareness,* San Francisco, CA, Computer Security Institute

[Dam, Appendix I, 1996] Dam, Kenneth and Lin, Herbert, 1996, *National Research Council - Cryptography's Role in Securing the Information Society, Appendix I: Industry-Specific Dimensions **of** Security,* Washington, D.C., National Academy Press

[Dam, Appendix J, 1996] Dam, Kenneth and Lin, Herbert, 1996, *National Research Council -Cryptography's Role in Securing the Information Society, Appendix J: Examples **of** Risks Posed by Unprotected Information,* Washington, D.C., National Academy Press

[Garg, 1996] Garg, Vijay K. and Wilkes, Joseph E., 1996, *Wireless and Personal Communications Systems,* Upper Saddle River, NJ, PTR Prentice Hall

[National ITS Architecture, 1997] Joint Architecture Team, Loral Federal Systems, Rockwell International, January 1997, "ITS Architecture: Executive Summary".

[The Reliable Services for General Users Subgroup, 1995] The Reliable Services for General Users Subgroup, April 1995, "NII Reliability and the General User: Issues and Recommendations, A Report to the Reliability and Vulnerability Working Group of the Information Infrastructure Task Force"

Web/Internet References

[CSI, 1997] "CSI: 1997 Computer Crime and Security *Survey", Computer Security Issues & Trends.* http://www.gocsi.com/iss_t.htm#Computer Crime (16 March 1997).

Periodical References

[American Banker, 1997] Anason, Dean, April 1997, "Banks' Clear and Present Danger: Internal Glitch", *The American Banker,* Washington, p.4.

Washington Post, 1997] *The Washington Post,* April 26, 1997, "Couple fined for intercepting Gingrich call", Washington, D.C., p.a2.

BIBLIOGRAPHY

Text

Computer Security Institute, *1993, Practical Methods for Information Systems Risk Analysis,* Washington, D.C., Computer Security Institute

Computer Security Institute, 1994, *CSI Manager's Guide to Computer Security Awareness,* San Francisco, CA, Computer Security Institute

Dam, Kenneth and Lin, Herbert, 1996, *National Research Council - Cryptography's Role in Securing the Information Society, Appendix I: Industry-Specific Dimensions **of** Security,* Washington, D.C., National Academy Press

Dam, Kenneth and Lin, Herbert, 1996, *National Research Council -Cryptography's Role in Securing the Information Society, Appendix J: Examples **of** Risks Posed by Unprotected Information,* Washington, D.C., National Academy Press

Ford, Warfick, 1994, *Computer Communications Security,* Englewood Cliffs, NJ, PTR Prentice Hall

Garg, Vijay K. and Wilkes, Joseph E., 1996, *Wireless and Personal Communications Systems,* Upper Saddle River, NJ, PTR Prentice Hall

Pahlaven, Kaveh and Levesque, Allen H., 1995, *Wireless Information Networks, New* York, NY, John Wiley & Sons, Inc.

Stallings, William, 1991, *Data and Computer Communications,* Third Edition, New York, NY, Macmillan Publishing Company

Stallings, William, 1997, *Data and Computer Communications,* Fifth Edition, Upper Saddle River, NJ, PTR Prentice Hall

Texas Department of Information Resources, 1994, *Information and Resources Security and Risk Management,* Austin, TX, Texas Department of Information Resources

Periodical

Anason, Dean, April 1997, "Banks' Clear and Present Danger: Internal Glitch", *The American Banker,* Washington, p.4.

Bernstein David S., May/June 1996, "1996 Infosecurity News/Yankee Group Survey", *Infosecurity News,* Volume 7, Number 3, p.19.

Infosecurity News, November/December 1996, "Special Issue - Buyers Guide 1996".

Keating, Sean, October 1996, "Security over wireless - can you defend against airborne attacks?', *Wireless **for** the Corporate User,* p.22.

Wireless Week, November 18, 1996, "IS-41 Testing May Be Imminent", p30.

Keveney, Bill, April 1993, "Vulgar highway messages an outside job, policy say", *The Hartford Courant,* p.c 13.

Washington Post, April 26, 1997, "Couple fined for intercepting Gingrich call", p.a2.

National ITS Architecture

Joint Architecture Team, Loral Federal Systems, Rockwell International, January 1997, "ITS Architecture: Executive Summary".

Joint Architecture Team, Loral Federal Systems, Rockwell International, January 1997, "ITS Architecture: Physical Architecture".

Joint Architecture Team, Loral Federal Systems, Rockwell International, January 1997, "ITS Architecture: Logical Architecture Volume 1".

Joint Architecture Team, Loral Federal Systems, Rockwell International, January 1997, "ITS Architecture: Communications Document".

Web/Internet

Agre, Philip E., "Technology and Privacy in Intelligent Transportation Systems", *Conference on Computers, Freedom, and Privacy.* http://weber.ucsd.edu/-pagre/agre.html (11 Nov 1996).

"AT&T Certifies Cylink for Frame Relay Security", *Press Releases.* http://www.cylink.com/whatsnew/pressrel/att.htm (9 Dec 1996).

Brown, Dan, "Techniques for Privacy and Authentication in Personal Communication Systems", *PCS Privacy and Authentication.* http://www.cs.berkeley.edu/-gribble/cs269/summaries/priv_pcs.html (3 Dee 1996).

"CERT[SM]", http://www.cert.org (8 Nov 1996).

"Communications Standards Review", *Stay Informed About Technical Communications Standards That Affect Your Business.* http://www.csrstds.com/stdsover.html (12 Dec 1996).

"CSI: 1997 Computer Crime and Security Survey", *Computer Security Issues & Trends.* http://www. gocsi.com/iss_t.htm#Computer Crime (16 March 1997).

"Encryption Policy Resource Page", http://www.crypto.com (4 Oct 1996).

"Federal Networking Council Home Page", http://www.fnc.gov/FNC-home.html (11 Oct 1996).

"GSA: Office of Information Security", http://www.gsa.gov/irms/ki/ois.htm (8 Nov 1996).

"ITS Architecture Browsing Site", http://www.rockwell.com/-jblarson/homepage.htmI Oct 1996).

Kolb, Michael, "Automatic Vehicle Identification", Electronic ***Toll Collection.*** http://village.ios.com/-mkolb/avi.html (16 Dec 1996).

"National Institute of Standards and Technology: Computer Security Resource Clearinghouse", http://csrc.ncsl.nist.gov/nissc (30 Sep 1996).

"Office of Management and Budget", http://www2.whitehouse.gov/WH/EOP/OMB/html/ombhome.htm (24 Oct 1996).

"Senate Pro-CODE (S. 1726) Hearings 7/25/9", http://www.crypto.com/hearing-cybercast ***(23*** Jul 1996).

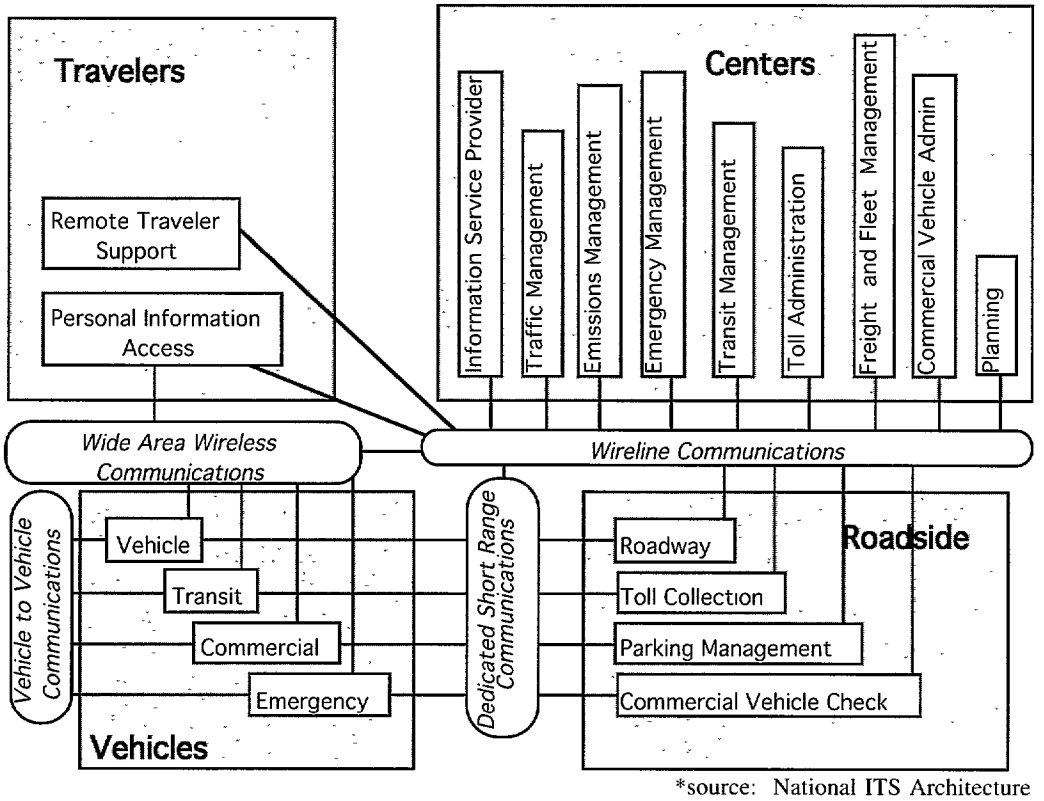
APPENDIX A

ITS DATA FLOW SECURITY ASSESSMENT

This appendix discusses the approach taken to assess and subsequently identify security threat categories and security services for all of the ITS data flows. It does not address how to implement the recommended services (i.e., selecting the specific mechanism(s) by which the security service will be provided) since identifying the specific security mechanisms would restrict system design flexibility. However, a comprehensive description of several common mechanisms is provided in appendix E, Information Security Mechanisms. Additionally, appendix F, Implementing Information Security Services, provides specific examples of implementing security services within ITS.

A.1 APPROACH AND METHODOLOGY

This information security assessment involved a detailed review of the ITS physical data flows. Generally, physical data flows represent an exchange of information between subsystems. Constituent logical data flows more precisely represent that same exchange between processes (i.e., functions) of those subsystems. Descriptions of the ITS physical data flows are found in the National ITS Physical Architecture document while logical data flows are located in the National ITS Logical Architecture document. Figure A-1, National ITS Architecture Subsystems Interconnect Diagram, illustrates high-level ITS subsystem relations and provides reference for each of the ITS physical data flow requirements.



*source: National ITS Architecture

Figure A-1. National ITS Architecture Subsystems Interconnect Diagram

Recalling the objectives of information security and the scope of this task, the ITS data flow assessment included:

- Reviewing the content (i.e., description) of the physical data flows as presented between associated source and destination end-systems (i.e., subsystems/terminators)
- Reviewing the content of all constituent logical data flows as well as their source and destination processes
- Considering collectively the content, intended function, and constraints of each complete data flow
- Considering the proposed transmission method and deciding what vulnerabilities and/or protections (if any) an appropriate communications system may inherently possess
- Identifying potential threat categories applicable to the collective data flow
- Identifying appropriate security service(s) to thwart any threat belonging to the noted threat categories (Recall that specific security mechanisms were not identified.)

To complete the context for this particular approach, the assessment was performed in accordance with the following considerations:

- Threat categories were identified and security services were recommended for the physical data flow (i.e., regarding the complete data flow structure) and not for individual constituent logical data flows or data entities. The logical data flows allow for variation in the functionality provided by individual physical data flows. Some variations may be more susceptible to threats than others, and the types of security services to counter those threats may differ. For the purposes of this assessment, all potential threat categories were identified. Subsequently, all potential security services were imposed.
- Threat categories were identified and security services were recommended based on the assumed correct operations of equipment, software, and human interaction. For example, threats to the data flows were examined with the assumption that the subsystem from which the data flow originated was properly secured (note: subsystem security issues are address in Section 4, ITS Subsystem Security Assessment).
- Transactions between collocated ITS subsystems (e.g., possibly a TMS and an EM) are more vulnerable to “inside” attack and may require different security services. However, collocated subsystems are specific to particular implementations -- not necessarily an architecture -- and therefore were not considered during this assessment.
- Physical, personnel, and operational security were not assessed since these components of system security are not directly applicable to data flows.
- Theoretically, all data flows are subject to denial of service attacks, yet the security service to counter these types of threats (i.e., this threat category) are commonly implemented by the application software and/or redundant hardware at the subsystem level. Therefore, all data flows are considered to be subject to denial of service, yet no security services to thwart denial of service threats (e.g., availability) are identified in Tables A-l through A-19.

A.2 ITS DATA FLOW ASSESSMENT

In this assessment, the complete data flow structure from the physical data flow through each level of logical data flow to the primitive elements were analyzed. Tables A-l through A-19 present the results of the ITS data flow assessment. Within each table, each physical data flow (e.g., "payment request") is associated with a source, a destination, an interconnect classification, and one or more threat categories and recommended security services.

The hierarchical nature of the data flow structure suggests that low-level constituent logical data flows or individual primitive elements may subject the entire data flow to various threats. Alternatively, some physical data flow descriptions -- at the highest level of the data flow structure -- suggest exposure to certain threats regardless of the information revealed in the constituent logical data flows. Tables A- 1 through A- 19 do not include the over 3,000 constituent logical data flows.

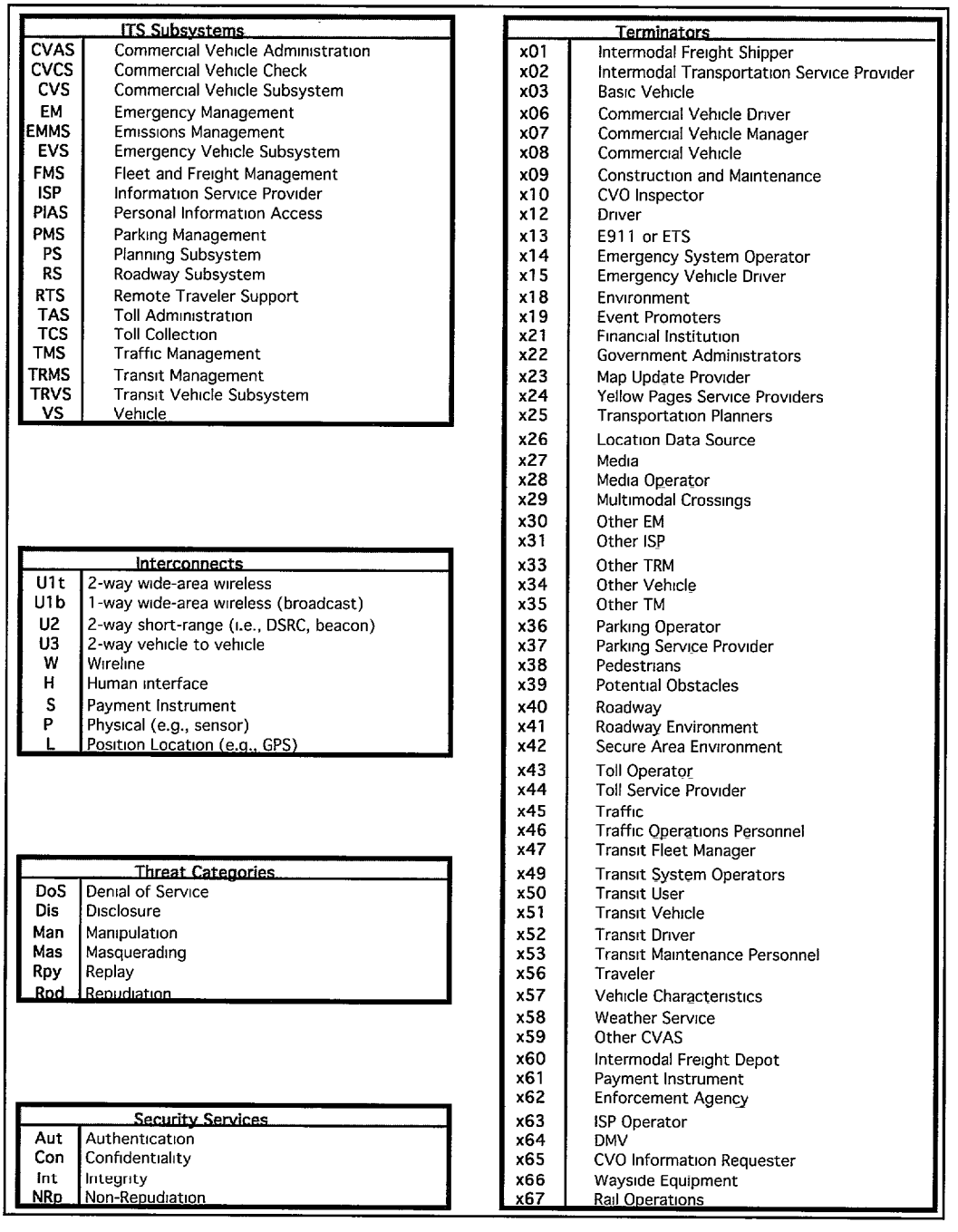
When reviewing the tables, the reader should note that a physical data flow name is unique only when paired with a source and destination. Therefore, different physical data flows with the same name can appear within the table; a "traveler information" data flow, for example, occurs between the ISP and the PIAS as well as between the ISP and the RTS. Although some assessments may seem inappropriate based on the name of the physical data flow, other factors such as data content or transmission medium (as noted in section A.3) contribute to the appropriate identification of threat categories and recommendation of security services.

Additionally, as discussed in section A. 1, all data flows are subject to denial-of-service attacks, yet the security service that could counter these types of threats are most commonly implemented by the application software and/or hardware at the subsystem level. Therefore, while the tables reflect the denial-of-service threat category, the security services to counter denial-of-service threats (e.g., availability) are not represented. Similarly, other security services (e.g., access control, auditing, system security management, and system configuration) that apply at the subsystem level and not at the data flow level have been excluded from the tables. Figure A-2, ITS Threat Category and Service Mapping, illustrates the relations between threat categories and applicable security services, and helps explain why certain threat categories and services are included in tables A- 1 through A- 19.

Security Services / Security Threats	Authentication	Confidentiality	Integrity	Non-Repudiation	Access Control	Auditing	Availability	System Security Management
Denial of Service					x		x	x
Disclosure		x			x			x
Manipulation			x		x	x		x
Masquerading	x							
Replay	x							
Repudiation				x				

Figure A-2. ITS Threat Category and Security Service Mapping

The keys provided in figure A-3 identify the specific elements of tables A-1 through A-19. Source and destination end-systems are either ITS subsystems such as the Traffic Management Subsystem (TMS), or terminators such as a state Department of Motor Vehicles (DMV). Interconnect classifications (e.g., Wireline (W)) identify the type of connection between end-systems for that particular data flow. Finally, the security threat categories and security services are identified by three-letter acronyms (e.g., "DoS" for denial of service, "Aut" for authentication). To simplify future reference, the tables are presented in alphabetical order by ITS subsystem.



ITS Subsystems	
CVAS	Commercial Vehicle Administration
CVCS	Commercial Vehicle Check
CVS	Commercial Vehicle Subsystem
EM	Emergency Management
EMMS	Emissions Management
EVS	Emergency Vehicle Subsystem
FMS	Fleet and Freight Management
ISP	Information Service Provider
PIAS	Personal Information Access
PMS	Parking Management
PS	Planning Subsystem
RS	Roadway Subsystem
RTS	Remote Traveler Support
TAS	Toll Administration
TCS	Toll Collection
TMS	Traffic Management
TRMS	Transit Management
TRVS	Transit Vehicle Subsystem
VS	Vehicle

Interconnects	
U1t	2-way wide-area wireless
U1b	1-way wide-area wireless (broadcast)
U2	2-way short-range (i.e., DSRC, beacon)
U3	2-way vehicle to vehicle
W	Wireline
H	Human interface
S	Payment Instrument
P	Physical (e.g., sensor)
L	Position Location (e.g., GPS)

Threat Categories	
DoS	Denial of Service
Dis	Disclosure
Man	Manipulation
Mas	Masquerading
Rpy	Replay
Rpd	Repudiation

Security Services	
Aut	Authentication
Con	Confidentiality
Int	Integrity
NRp	Non-Repudiation

Terminators	
x01	Intermodal Freight Shipper
x02	Intermodal Transportation Service Provider
x03	Basic Vehicle
x06	Commercial Vehicle Driver
x07	Commercial Vehicle Manager
x08	Commercial Vehicle
x09	Construction and Maintenance
x10	CVO Inspector
x12	Driver
x13	E911 or ETS
x14	Emergency System Operator
x15	Emergency Vehicle Driver
x18	Environment
x19	Event Promoters
x21	Financial Institution
x22	Government Administrators
x23	Map Update Provider
x24	Yellow Pages Service Providers
x25	Transportation Planners
x26	Location Data Source
x27	Media
x28	Media Operator
x29	Multimodal Crossings
x30	Other EM
x31	Other ISP
x33	Other TRM
x34	Other Vehicle
x35	Other TM
x36	Parking Operator
x37	Parking Service Provider
x38	Pedestrians
x39	Potential Obstacles
x40	Roadway
x41	Roadway Environment
x42	Secure Area Environment
x43	Toll Operator
x44	Toll Service Provider
x45	Traffic
x46	Traffic Operations Personnel
x47	Transit Fleet Manager
x49	Transit System Operators
x50	Transit User
x51	Transit Vehicle
x52	Transit Driver
x53	Transit Maintenance Personnel
x56	Traveler
x57	Vehicle Characteristics
x58	Weather Service
x59	Other CVAS
x60	Intermodal Freight Depot
x61	Payment Instrument
x62	Enforcement Agency
x63	ISP Operator
x64	DMV
x65	CVO Information Requester
x66	Wayside Equipment
x67	Rail Operations

Figure A-3. Keys for ITS Data Flow Security Assessment Tables

Table A-1a. ITS Data Flow Security Assessment: From CVAS

Source	Physical Data Flow	Destination	Inter-connect	THREAT CATEGORIES						SECURITY SERVICES			
				DoS	Dis	Man	Mas	Rpy	Rpd	Aut	Con	Int	NRp
cvas	credential information	cvcs	w	x	x	~	x			x	x		
cvas	CVO database update	cvcs	w	x	x	x	x			x	x	x	
cvas	international border crossing data	cvcs	w	x	x	~	x			x	x		
cvas	safety information	cvcs	w	x	x	x	x			x	x	x	
cvas	activity reports	fms	w	x	x	x	x			x	x	x	
cvas	compliance review report	fms	w	x	x	x	x			x	x	x	
cvas	electronic credentials	fms	w,u1t	x	x	x	x	x	x	x	x	x	x
cvas	operational data	ps	w	x		~	x			x			
cvas	payment request	x21	w	x		~	x	x	X	x			x
cvas	tax-credentials-fees request	x22	w	x	x	~	x		x	x	x		x
cvas	credentials and safety information request	x59	w	x	x	~	x		x	x	x		x
cvas	CVAS information exchange	x59	w	x		~	x			x			
cvas	request for information on violators	x62	w	x		~	x			x			
cvas	violation notification	x62	w	x	x	~	x			x	x		
cvas	license request	x64	w	x		~	x			x			
cvas	credentials and safety information response	x65	w	x	x	~	x			x	x		

Table A-1b. ITS Data Flow Security Assessment: To CVAS

Source	Physical Data Flow	Destination	Inter-connect	THREAT CATEGORIES						SECURITY SERVICES			
				DoS	Dis	Man	Mas	Rpy	Rpd	Aut	Con	Int	NRp
cvcs	citation and accident data	cvas	w	x	x	x	x			x	x	x	
cvcs	credentials information request	cvas	w	x	x	~	x			x	x		
cvcs	international border crossing data	cvas	w	x	x	~	x			x	x		
cvcs	roadside log update	cvas	w	x	x	x	x			x	x	x	
cvcs	safety information	cvas	w	x	x	~	x			x	x		
fms	credential application	cvas	w	x	x	~	x			x	x		
fms	information request	cvas	w	x	x	~	x			x	x		
fms	tax filing, audit data	cvas	w	x	x	x	x	x	x	x	x	x	x
x21	transaction status	cvas	w	x		~	x	x	x	x			x
x22	regulations	cvas	w	x	x	~	x			x	x		
x59	credentials and safety information response	cvas	w	x	x	~	x		x	x	x		x
x59	CVAS information exchange	cvas	w	x		~	x			x			
x62	information on violators	cvas	w	x	x	~	x			x	x		
x64	registration	cvas	w	x	x	~	x			x	x		
x65	credentials and safety information request	cvas	w	x		~	x			x			

Table A-2a. ITS Data Flow Security Assessment: From CVCS

Source	Physical Data Flow	Destination	Inter-connect	THREAT CATEGORIES						SECURITY SERVICES			
				DoS	Dis	Man	Mas	Rpy	Rpd	Aut	Con	Int	NRp
cvcs	citation and accident data	cvas	w	x	x	x	x			x	x	x	
cvcs	credentials information request	cvas	w	x	x	~	x			x	x		
cvcs	international border crossing data update	cvas	w	x	x	~	x			x	x		
cvcs	roadside log update	cvas	w	x	x	x	x			x	x	x	
cvcs	safety information request	cvas	w	x	x	~	x			x	x		
cvcs	border clearance event record	cvs	u2	x	x	~	x	x		x	x		
cvcs	border clearance request	cvs	u2	x		~	x	x		x			
cvcs	clearance event record	cvs	u2	x	x	~	x	x		x	x		
cvcs	lock tag data request	cvs	u2	x		~	x	x		x			
cvcs	on-board safety request	cvs	u2	x	x	~	x	x		x	x		
cvcs	pass/pull-in	cvs	u2	x	x	x	x	x		x	x	x	
cvcs	safety inspection record	cvs	u2	x	x	x	x	x		x	x	x	
cvcs	screening request	cvs	u2	x		~	x	x		x			
cvcs	CVO Pull in Message	x06	H	x									
cvcs	CVO inspector information	x10	H	x									

Table A-2b. ITS Data Flow Security Assessment: To CVCS

Source	Physical Data Flow	Destination	Inter-connect	THREAT CATEGORIES						SECURITY SERVICES			
				DoS	Dis	Man	Mas	Rpy	Rpd	Aut	Con	Int	NRp
cvas	credentials information	cvcs	w	x	x	~	x			x	x		
cvas	CVO database update	cvcs	w	x	x	x	x			x	x	x	
cvas	international border crossing data	cvcs	w	x	x	~	x			x	x		
cvas	safety information	cvcs	w	x	x	x	x			x	x	x	
cvs	border clearance data	cvcs	u2	x	x	x	x	x		x	x	x	
cvs	lock tag data	cvcs	u2	x	x	x	x	x		x	x	x	
cvs	on board safety data	cvcs	u2	x	x	x	x	x		x	x	x	
cvs	screening data	cvcs	u2	x	x	x	x	x		x	x	x	
x08	CVO weight and presence	cvcs	P	x									
x10	CVC override mode	cvcs	H	x			x			x			
x10	CVO inspector input	cvcs	H	x			x			x			

Table A-3a. ITS Data Flow Security Assessment: From CVS

Source	Physical Data Flow	Destination	Inter-connect	THREAT CATEGORIES						SECURITY SERVICES			
				DoS	Dis	Man	Mas	Rpy	Rpd	Aut	Con	Int	NRp
cvs	border clearance data	cvcs	u2	x	x	x	x	x		x	x	x	
cvs	lock tag data	cvcs	u2	x	x	x	x	x		x	x	x	
cvs	on board safety data	cvcs	u2	x	x	x	x	x		x	x	x	
cvs	screening data	cvcs	u2	x	x	x	x	x		x	x	x	
cvs	driver and vehicle information	fms	u1t	x	x	x	x	x	x	x	x	x	x
cvs	on board vehicle data	fms	u1t, u2	x	x	x	x	x		x	x	x	
cvs	processed cargo data	vs	w	x		~							
cvs	alerts, messages	x06	H	x									
cvs	CVO Pull in Message	x06	H	x									
cvs	log information	x06	H	x									
cvs	lock tag data request	x08	w	x		~							

Table A-3b. ITS Data Flow Security Assessment: To CVS

Source	Physical Data Flow	Destination	Inter-connect	THREAT CATEGORIES						SECURITY SERVICES			
				DoS	Dis	Man	Mas	Rpy	Rpd	Aut	Con	Int	NRp
cvcs	border clearance event record	cvs	u2	x	x	~	x	x		x	x		
cvcs	border clearance request	cvs	u2	x		~	x	x		x			
cvcs	clearance event record	cvs	u2	x	x	~	x	x		x	x		
cvcs	lock tag data request	cvs	u2	x		~	x	x		x			
cvcs	on-board safety request	cvs	u2	x	x	~	x	x		x	x		
cvcs	pass/pull-in	cvs	u2	x	x	x	x	x		x	x	x	
cvcs	safety inspection record	cvs	u2	x	x	x	x	x		x	x	x	
cvcs	screening request	cvs	u2	x		~	x	x		x			
fms	fleet to driver update	cvs	u1t	x	x	x	x	x	x	x	x	x	x
vs	CVO driver initialization	cvs	H	x			x			x			
x08	vehicle measures	cvs	w	x		~							

Table A-4a. ITS Data Flow Security Assessment: From EM

Source	Physical Data Flow	Destination	Inter-connect	THREAT CATEGORIES						SECURITY SERVICES			
				DoS	Dis	Man	Mas	Rpy	Rpd	Aut	Con	Int	NRp
em	assigned route	evs	u1t	x		x	x			x		x	
em	emergency dispatch requests	evs	u1t	x	x	x	x			x	x	x	
em	Hazmat information	evs	u1t	x		x	x			x		x	
em	Hazmat information request	fms	w	x		~	x			x			
em	emergency vehicle route request	isp	w	x	x	x	x			x	x	x	
em	incident information	isp	w	x		x	x			x		x	
em	emergency acknowledge	pias	w,u1t	x		x	x		x	x		x	x
em	operational data	ps	w	x	x	~	x			x	x		
em	emergency acknowledge	rts	w,u1t	x		x	x		x	x		x	x
em	emergency vehicle greenwave request	tms	w	x		x	x			x		x	
em	incident information	tms	w	x		x	x			x		x	
em	incident response status	tms	w	x		x	x			x		x	
em	transit emergency coordination data	trms	w	x		x	x			x		x	
em	emergency acknowledge	vs	u1t	x		x	x		x	x		x	x
em	emergency status	x13	w	x		x	x		x	x		x	x
em	emergency dispatch status	x14	H	x									
em	map update request	x23	w	x		~	x			x			
em	emergency coordination	x30	w	x		x	x			x		x	

Table A-4b. ITS Data Flow Security Assessment: To EM

Source	Physical Data Flow	Destination	Inter-connect	THREAT CATEGORIES						SECURITY SERVICES			
				DoS	Dis	Man	Mas	Rpy	Rpd	Aut	Con	Int	NRp
evs	emergency vehicle driver inputs	em	u1t	x		x	x			x		x	
evs	emergency vehicle driver status update	em	u1t	x		x	x			x		x	
evs	emergency vehicle tracking data	em	u1t	x		x	x			x		x	
fms	Hazmat information	em	w	x	x	x	x			x	x	x	
isp	emergency vehicle route	em	w	x	x	x	x			x	x	x	
isp	incident information request	em	w	x		x	x			x		x	
pias	emergency notification	em	u1t	x	x	x	x			x	x	x	
rts	emergency notification	em	w,u1t	x	x	x	x			x	x	x	
tms	incident information request	em	w	x		x	x			x		x	
tms	incident notification	em	w	x		x	x			x		x	
trms	security alarms	em	w	x		x	x			x		x	
vs	emergency notification	em	u1t	x	x	x	x			x	x	x	
x13	incident information	em	w	x		x	x			x		x	
x14	emergency dispatch request	em	H	x			x			x			
x23	map updates	em	w	x		x	x			x		x	
x30	emergency coordination	em	w	x		x	x			x		x	

Table A-5a. ITS Data Flow Security Assessment From EMMS

Source	Physical Data Flow	Destination	Inter-connect	THREAT CATEGORIES						SECURITY SERVICES			
				DoS	Dis	Man	Mas	Rpy	Rpd	Aut	Con	Int	NRp
emms	operational data	ps	w	x		~	x			x			
emms	vehicle pollution criteria	rs	w	x		~	x			x			
emms	widearea statistical pollution information	tms	w	x		~	x			x			
emms	map update request	x23	w	x		~	x			x			
emms	pollution data display	x46	H	x									

Table A-5b. ITS Data Flow Security Assessment: To EMMS

Source	Physical Data Flow	Destination	Inter-connect	THREAT CATEGORIES						SECURITY SERVICES			
				DoS	Dis	Man	Mas	Rpy	Rpd	Aut	Con	Int	NRp
rs	pollution data	emms	w	x		~	x			x			
tms	pollution state data request	emms	w	x		~	x			x			
x18	pollution data	emms	P	x		~	x			x			
x23	map updates	emms	w	x		~	x			x			
x46	pollution data parameters	emms	H	x			x			x			

Table A-6a. ITS Data Flow Security Assessment: From EVS

Source	Physical Data Flow	Destination	Inter-connect	THREAT CATEGORIES						SECURITY SERVICES			
				DoS	Dis	Man	Mas	Rpy	Rpd	Aut	Con	Int	NRp
evs	emergency vehicle driver inputs	em	u1t	x		x	x			x		x	
evs	emergency vehicle driver status update	em	u1t	x		x	x			x		x	
evs	emergency vehicle tracking data	em	u1t	x		x	x			x		x	
evs	emergency vehicle preemption request	rs	u2	x		~	x	x		x			
evs	emergency dispatch order	x15	H	x									

Table A-6b. ITS Data Flow Security Assessment: To EVS

Source	Physical Data Flow	Destination	Inter-connect	THREAT CATEGORIES						SECURITY SERVICES			
				DoS	Dis	Man	Mas	Rpy	Rpd	Aut	Con	Int	NRp
em	assigned route	evs	u1t	x		x	x			x		x	
em	emergency dispatch requests	evs	u1t	x	x	x	x			x	x	x	
em	Hazmat information	evs	u1t	x		x	x			x		x	
vs	vehicle location	evs	w	x		~							
x15	EV driver inputs	evs	H	x			x			x			

Table A-7a. ITS Data Flow Security Assessment: From FMS

Source	Physical Data Flow	Destination	Inter-connect	THREAT CATEGORIES						SECURITY SERVICES			
				DoS	Dis	Man	Mas	Rpy	Rpd	Aut	Con	Int	NRp
fms	credential application	cvas	w	x	x	~	x			x	x		
fms	information request	cvas	w	x	x	~	x			x	x		
fms	tax filing, audit data	cvas	w	x	x	x	x	x	x	x	x	x	x
fms	fleet to driver update	cvs	u1t	x	x	x	x	x	x	x	x	x	x
fms	Hazmat information	em	w	x	x	x	x			x	x	x	
fms	route request	isp	w	x	x	~	x			x	x		
fms	intermod CVO coord	x01	w	x		~	x			x			
fms	fleet status	x07	H	x									
fms	intermod CVO coord	x60	w	x		~	x			x			
fms	request for payment	x61	s	x		~	x	x	x	x		x	x

Table A-7b. ITS Data Flow Security Assessment: To FMS

Source	Physical Data Flow	Destination	Inter-connect	THREAT CATEGORIES						SECURITY SERVICES			
				DoS	Dis	Man	Mas	Rpy	Rpd	Aut	Con	Int	NRp
cvas	activity reports	fms	w	x	x	x	x			x	x	x	
cvas	compliance review report	fms	w	x	x	x	x			x	x	x	
cvas	electronic credentials	fms	w,u1t	x	x	x	x	x	x	x	x	x	x
cvs	driver and vehicle information	fms	u1t	x	x	x	x	x	x	x	x	x	x
cvs	on board vehicle data	fms	u1t,u2	x	x	x	x	x		x	x	x	
em	Hazmat information request	fms	w	x		~	x			x			
isp	route plan	fms	w	x	x	~	x			x	x		
x01	intermod CVO coord	fms	w	x		~	x			x			
x07	fleet manager inquiry	fms	H	x			x			x			
x60	intermod CVO coord	fms	w	x		~	x			x			
x61	payment	fms	s	x		x	x	x	x	x		x	x

Table A-8a. ITS Data Flow Security Assessment: From ISP

Source	Physical Data Flow	Destination	Inter-connect	THREAT CATEGORIES						SECURITY SERVICES			
				DoS	Dis	Man	Mas	Rpy	Rpd	Aut	Con	Int	NRp
isp	emergency vehicle route	em	w	x	x	x	x			x	x	x	
isp	incident information request	em	w	x		x	x			x		x	
isp	route plan	fms	w	x	x	~	x			x	x		
isp	broadcast information	pias	w,u1b	x	x	~	x			x	x		
isp	traveler information	pias	w,u1t	x	x	x	x		x	x	x	x	x
isp	trip plan	pias	w,u1t	x	x	~	x			x	x		
isp	parking lot data request	pms	w	x	x	x	x	x	x	x	x	x	x
isp	parking reservations request	pms	w	x	x	~	x			x	x		
isp	road network use	ps	w	x		~	x			x			
isp	broadcast information	rts	w,u1b	x		~	x			x			
isp	traveler information	rts	w,u1t	x	x	x	x		x	x	x	x	x
isp	trip plan	rts	w	x	x	~	x			x	x		
isp	toll data request	tas	w	x	x	x	x	x	x	x	x	x	x
isp	incident notification	tms	w	x		x	x			x		x	
isp	logged route plan	tms	w	x	x	x	x			x	x	x	
isp	request for traffic information	tms	w	x		~	x			x			
isp	road network use	tms	w	x	x	~	x			x	x		
isp	demand responsive transit request	trms	w	x	x	~	x			x	x		
isp	selected routes	trms	w	x	x	x	x	x	x	x	x	x	x
isp	transit information request	trms	w	x	x	x	x	x	x	x	x	x	x
isp	broadcast information	vs	u1b	x		~	x			x			
isp	traveler information	vs	u1t,u1b	x	x	x	x		x	x	x	x	x
isp	trip plan	vs	u1t	x	x	~	x			x	x		

Table A-8a (Continued). ITS Data Flow Security Assessment: From ISP

Source	Physical Data Flow	Destination	Inter-connect	THREAT CATEGORIES						SECURITY SERVICES			
				DoS	Dis	Man	Mas	Rpy	Rpd	Aut	Con	Int	NRp
isp	intermodal information	x02	w	x		~	x			x			
isp	payment request	x21	w	x		~	x	x	x	x			x
isp	map update request	x23	w	x		~	x			x			
isp	provider registration confirm	x24	w	x		~	x		x	x			x
isp	travel service request	x24	w	x		~	x	x	x	x			x
isp	incident information	x27	w	x		~	x			x			
isp	traffic information	x27	w	x		~	x			x			
isp	incident information	x28	w	x		~	x			x			
isp	traffic information	x28	w	x		~	x			x			
isp	ISP coord	x31	w	x		~	x			x			
isp	ISP route planning parameters	x63	H	x									

Table A-8b. ITS Data Flow Security Assessment: To ISP

Source	Physical Data Flow	Destination	Inter-connect	THREAT CATEGORIES						SECURITY SERVICES			
				DoS	Dis	Man	Mas	Rpy	Rpd	Aut	Con	Int	NRp
em	emergency vehicle route request	isp	w	x	x	x	x			x	x	x	
em	incident information	isp	w	x		x	x			x		x	
fms	route request	isp	w	x	x	~	x			x	x		
pias	traveler information request	isp	w,u1t	x	x	x	x	x	x	x	x	x	x
pias	trip confirmation	isp	w,u1t	x	x	x	x			x	x	x	
pias	trip request	isp	w,u1t	x	x	~	x			x	x		
pias	yellow pages request	isp	w,u1t	x	x	~	x			x	x		
pms	parking availability	isp	w	x	x	~	x			x	x		
pms	parking lot reservation confirmation	isp	w	x	x	x	x	x	x	x	x	x	x
rts	traveler information request	isp	w	x	x	x	x	x	x	x	x	x	x
rts	traveler selection	isp	w	x	x	~	x			x	x		
rts	trip request	isp	w	x	x	~	x			x	x		
rts	yellow pages request	isp	w	x		~	x			x			
tas	probe data	isp	w	x		~	x			x			
tas	toll data	isp	w	x	x	x	x	x	x	x	x	x	x
tms	traffic information	isp	w	x		~	x			x			
trms	demand responsive transit plan	isp	w	x	x	~	x			x	x		
trms	transit and fare schedules	isp	w	x	x	x	x			x	x	x	
trms	transit request confirmation	isp	w	x	x	x	x	x	x	x	x	x	x
vs	traveler information request	isp	u1t	x	x	x	x	x	x	x	x	x	x
vs	trip confirmation	isp	u1t	x		~	x			x			
vs	trip request	isp	u1t	x	x	~	x			x	x		
vs	vehicle probe data	isp	u1t	x	x	~	x			x	x		
vs	yellow pages request	isp	u1t	x	x	~	x			x	x		

Table A-8b (Continued). ITS Data Flow Security Assessment: To ISP

Source	Physical Data Flow	Destination	Inter-connect	THREAT CATEGORIES						SECURITY SERVICES			
				DoS	Dis	Man	Mas	Rpy	Rpd	Aut	Con	Int	NRp
x02	intermodal information	isp	w	x		~	x		x	x			x
x21	transaction status	isp	w	x		~	x	x	x	x			x
x23	map updates	isp	w	x		~	x			x			
x24	provider registration	isp	w	x	x	x	x			x	x	x	
x24	travel service info	isp	w	x		~	x	x	x	x			x
x27	external reports	isp	w	x		~	x			x			
x28	incident notification	isp	w	x		x	x			x		x	
x31	ISP coord	isp	w	x		~	x			x			
x58	weather information	isp	w	x		~	x			x			
x63	route planning parameters	isp	H	x			x			x			

Table A-9a. ITS Data Flow Security Assessment: From PIAS

Source	Physical Data Flow	Destination	Inter-connect	THREAT CATEGORIES						SECURITY SERVICES			
				DoS	Dis	Man	Mas	Rpy	Rpd	Aut	Con	Int	NRp
pias	emergency notification	em	u1t	x	x	x	x			x	x	x	
pias	traveler information request	isp	w,u1t	x	x	x	x	x	x	x	x	x	x
pias	trip confirmation	isp	w,u1t	x	x	x	x			x	x	x	
pias	trip request	isp	w,u1t	x	x	~	x			x	x		
pias	yellow pages request	isp	w,u1t	x	x	~	x			x	x		
pias	demand responsive transit request	trms	u1t	x	x	~	x			x	x		
pias	map update request	x23	w,u1t	x	x	x	x			x	x	x	
pias	traveler interface updates	x56	H	x									
pias	request for payment	x61	S	x		~	x	x	x	x			x

Table A-9b. ITS Data Flow Security Assessment: To PIAS

Source	'Physical Data Flow	Destination	Inter-connect	THREAT CATEGORIES						SECURITY SERVICES			
				DoS	Dis	Man	Mas	Rpy	Rpd	Aut	Con	Int	NRp
em	emergency acknowledge	pias	w,u1t	x		x	x		x	x		x	x
isp	broadcast information	pias	w,u1b	x	x	~	x			x	x		
isp	traveler information	pias	w,u1t	x	x	x	x		x	x	x	x	x
isp	trip plan	pias	w,u1t	x	x	~	x			x	x		
trms	demand responsive transit route	pias	w,u1t	x	x	~	x			x	x		
x23	map updates	pias	w,u1t	x		~	x			x			
x26	position fix	pias	L	x		x	x			x		x	
x56	traveler information request	pias	H	x			x			x			
x61	payment	pias	S	x		x	x	x	x	x		x	x

Table A-10a. ITS Data Flow Security Assessme: From PMS

Source	Physical Data Flow	Destination	Inter-connect	THREAT CATEGORIES						SECURITY SERVICES			
				DoS	Dis	Man	Mas	Rpy	Rpd	Aut	Con	Int	NRp
pms	parking availability	isp	w	x	x	~	x			x	x		
pms	parking lot reservation confirmation	isp	w	x	x	x	x	x	x	x	x	x	x
pms	operational data	ps	w	x		~	x			x			
pms	demand management price change response	tms	w	x		~	x			x			
pms	parking availability	tms	w	x		~	x			x			
pms	transit parking coordination	trms	w	x		~	x			x			
pms	request tag data	vs_	u2	x	x	x	x	x	x	x	x	x	x
pms	tag update	vs_	u2	x	x	x	x	x	x	x	x	x	x
pms	transaction status	x12	H	x									
pms	payment request	x21	w	x	x	x	x	x	x	x	x	x	x
pms	parking status	x36	H	x									
pms	parking availability	x37	w	x	x	x	x	x	x	x	x	x	x
pms	violation notification	x62	w	x	x	~	x			x	x		
pms	license request	x64	w	x		~	x			x			

Table A-10b. ITS Data Flow Security Assessment: To PMS

Source	Physical Data Flow	Destination	Inter-connect	THREAT CATEGORIES						SECURITY SERVICES			
				DoS	Dis	Man	Mas	Rpy	Rpd	Aut	Con	Int	NRp
isp	parking lot data request	pms	w	x	x	x	x	x	x	x	x	x	x
isp	parking reservations request	pms	w	x	x	~	x			x	x		
tms	demand management price change request	pms	w	x		~	x			x			
tms	parking instructions	pms	w	x		~	x			x			
trms	parking lot transit response	pms	w	x		~	x			x			
vs	tag data	pms	u2	x	x	x	x	x	x	x	x	x	x
x03	vehicle characteristics	pms	P	x									
x21	transaction status	pms	w	x	x	x	x	x	x	x	x	x	x
x36	parking instructions	pms	H	x			x			x			
x37	request for performance data	pms	w	x		~	x	x	x	x			x
x57	vehicle image	pms	P	x									
x64	vehicle characteristics	pms	w	x	x	~	x			x	x		

Table A-lla. ITS Data Flow Security Assessment: From PS

Source	Physical Data Flow	Destination	Inter-connect	THREAT CATEGORIES						SECURITY SERVICES			
				DoS	Dis	Man	Mas	Rpy	Rpd	Aut	Con	Int	NRp
ps	planning data	tms	w	x		~	x			x			
ps	map update request	x23	w	x		~	x			x			
ps	planning data	x25	w	x		~	x			x			

Table A-llb. ITS Data Flow Security Assessment: To PS

Source	Physical Data Flow	Destination	Inter-connect	THREAT CATEGORIES						SECURITY SERVICES			
				DoS	Dis	Man	Mas	Rpy	Rpd	Aut	Con	Int	NRp
cvas	operational data	ps	w	x		~	x			x			
em	operational data	ps	w	x	x	~	x			x	x		
emms	operational data	ps	w	x		~	x			x			
isp	road network use	ps	w	x		~	x			x			
pms	operational data	ps	w	x		~	x			x			
tas	operational data	ps	w	x		~	x			x			
tms	operational data	ps	w	x		~	x			x			
trms	operational data	ps	w	x		~	x			x			
x23	map updates	ps	w	x		~	x			x			
x25	planning data	ps	w	x		~	x			x			

Table A-12a. ITS Data Flow Security Assessment: From RS

Source	Physical Data Flow	Destination	Inter-connect	THREAT CATEGORIES						SECURITY SERVICES			
				DoS	Dis	Man	Mas	Rpy	Rpd	Aut	Con	Int	NRp
rs	pollution data	emms	w	x		~	x			x			
rs	AHS status	tms	w	x		~	x			x			
rs	fault reports	tms	w	x		~	x			x			
rs	freeway control status	tms	w	x		~	x			x			
rs	HOV data	tms	w	x		~	x			x			
rs	hri status	tms	w	x		x	x			x		x	
rs	incident data	tms	w	x	x	~	x			x	x		
rs	intersection blockage notification	tms	w	x		x	x			x		x	
rs	local traffic flow	tms	w	x		~	x			x			
rs	request for right of Way	tms	w	x		~	x			x			
rs	signal control status	tms	w	x		~	x			x			
rs	signal priority request	tms	w	x		~	x			x			
rs	vehicle probe data	tms	w	x	x	~	x			x	x		
rs	AHS control data	vs	u2	x		x	x	x		x		x	
rs	intersection status	vs	u2	x		x	x	x		x		x	
rs	request tag data	vs	u2	x		~	x	x	x	x			x
rs	vehicle signage data	vs	u2	x		~	x	x		x			
rs	driver information	x12	H	x									
rs	grant right of way and/or stop traffic	x29	w	x		x	x			x		x	
rs	crossing permission	x38	H	x									
rs	hri status	x66	w	x		x	x			x		x	
rs	intersection blockage notification	x66	w	x		x	x			x		x	

Table A-12b. ITS Data Flow Security Assessment: To RS

Source	Physical Data Flow	Destination	Inter-connect	THREAT CATEGORIES						SECURITY SERVICES			
				DoS	Dis	Man	Mas	Rpy	Rpd	Aut	Con	Int	NRp
emms	vehicle pollution criteria	rs	w	x		~	x			x			
evs	emergency vehicle preemption request	rs	u2	x		~	x	x		x			
tms	AHS control information	rs	w	x		x	x			x		x	
tms	freeway control data	rs	w	x		x	x			x		x	
tms	hri control data	rs	w	x		x	x			x		x	
tms	hri request	rs	w	x		~	x			x			
tms	signage data	rs	w	x		~	x			x			
tms	signal control data	rs	w	x		x	x			x		x	
tms	surveillance control	rs	w	x		~	x			x			
trvs	local signal priority request	rs	u2	x		~	x	x		x			
vs	ahs vehicle data	rs	u2	x		x	x			x		x	
vs	vehicle probe data	rs	u2	x	x	x	x			x	x	x	
x03	vehicle characteristics	rs	P	x									
x18	pollution data	rs	P	x									
x29	request for right of Way	rs	w	x		x	x			x		x	
x29	right of way preemption request	rs	w	x		x	x			x		x	
x38	crossing call	rs	H	x									
x41	weather conditions	rs	P	x									
x45	vehicle count	rs	P	x									
x66	arriving train information	rs	w	x		x	x			x		x	
x66	track status	rs	w	x		x	x			x		x	

Table A-13a. ITS Data Flow Security Assessment: From RTS

Source	Physical Data Flow	Destination	Inter-connect	THREAT CATEGORIES						SECURITY SERVICES			
				DoS	Dis	Man	Mas	Rpy	Rpd	Aut	Con	Int	NRp
rts	emergency notification	em	w,u1t	x	x	x	x			x	x	x	
rts	traveler information request	isp	w	x	x	x	x	x	x	x	x	x	x
rts	traveler selection	isp	w	x	x	~	x			x	x		
rts	trip request	isp	w	x	x	~	x			x	x		
rts	yellow pages request	isp	w	x		~	x			x			
rts	emergency notification	trms	w	x	x	x	x			x	x	x	
rts	transit request	trms	w	x	x	x	x	x	x	x	x	x	x
rts	traveler information request	trms	w	x	x	x	x	x	x	x	x	x	x
rts	map update request	x23	w	x		~	x			x			
rts	traveler information	x50	H	x									
rts	traveler interface updates	x56	H	x									
rts	request for payment	x61	s	x		~	x	x	x	x			x

Table A-13b. ITS Data Flow Security Assessment: To RTS

Source	Physical Data Flow	Destination	Inter-connect	THREAT CATEGORIES						SECURITY SERVICES			
				DoS	Dis	Man	Mas	Rpy	Rpd	Aut	Con	Int	NRp
em	emergency acknowledge	rts	w,u1t	x		x	x		x	x		x	x
isp	broadcast information	rts	w,u1b	x		~	x			x			
isp	traveler information	rts	w,u1t	x	x	x	x		x	x	x	x	x
isp	trip plan	rts	w	x	x	~	x			x	x		
trms	emergency acknowledge	rts	w	x		x	x			x		x	
trms	transit and fare schedules	rts	w	x	x	~	x		x	x	x		x
trms	traveler information	rts	w	x	x	x	x	x	x	x	x	x	x
x23	map updates	rts	w	x		~	x			x			
x50	traveler information request	rts	H	x									
x56	traveler information request	rts	H	x									
x61	payment	rts	s	x		x	x	x	x	x		x	x

Table A-14a. ITS Data Flow Security Assessment: From TAS

Source	Physical Data Flow	Destination	Inter-connect	THREAT CATEGORIES						SECURITY SERVICES			
				DoS	Dis	Man	Mas	Rpy	Rpd	Aut	Con	Int	NRp
tas	probe data	isp	w	x		~	x			x			
tas	toll data	isp	w	x	x	x	x	x	x	x	x	x	x
tas	operational data	ps	w	x		~	x			x			
tas	toll instructions	tcs	w	x	x	x	x	x	x	x	x	x	x
tas	demand management price change response	tms	w	x		~	x			x			
tas	probe data	tms	w	x		~	x			x			
tas	payment request	x21	w	x	x	x	x	x	x	x	x	x	x
tas	toll transaction reports	x43	H	x									
tas	toll revenues and summary reports	x44	w (? H)	x	x	x	x			x	x	x	
tas	violation notification	x62	w	x	x	~	x			x	x		
tas	license request	x64	w	x		~	x			x			

Table A-14b. ITS Data Flow Security Assessment: To TAS

Source	Physical Data Flow	Destination	Inter-connect	THREAT CATEGORIES						SECURITY SERVICES			
				DoS	Dis	Man	Mas	Rpy	Rpd	Aut	Con	Int	NRp
isp	toll data request	tas	w	x	x	x	x	x	x	x	x	x	x
tcs	Toll Transactions	tas	w	x	x	x	x	x	x	x	x	x	x
tms	demand management price change request	tas	w	x		~	x			x			
x21	transaction status	tas	w	x	x	x	x	x	x	x	x	x	x
x43	toll operator requests	tas	H	x			x			x			
x44	toll fees	tas	H	x			x			x			
x64	registration	tas	w	x	x	~	x			x	x		

Table A-15a. ITS Data Flow Security Assessment: From TCS

Source	Physical Data Flow	Destination	Inter-connect	THREAT CATEGORIES						SECURITY SERVICES			
				DoS	Dis	Man	Mas	Rpy	Rpd	Aut	Con	Int	NRp
tcs	Toll Transactions	tas	w	x	x	x	x	x	x	x	x	x	x
tcs	request tag data	vs	u2	x		~	x	x	x	x			x
tcs	tag update	vs	u2	x	x	x	x	x	x	x	x	x	x
tcs	transaction status	x12	H	x									

Table A-15b. ITS Data Flow Security Assessment: To TCS

Source	Physical Data Flow	Destination	Inter-connect	THREAT CATEGORIES						SECURITY SERVICES			
				DoS	Dis	Man	Mas	Rpy	Rpd	Aut	Con	Int	NRp
tas	toll instructions	tcs	w	X	X	x	x	x	x	x	x	x	x
vs	tag data	tcs	u 2	X	X	x	x	x	x	x	x	x	x
x03	vehicle characteristic	tcs	p	X									
x57	vehicle image	tcs	P	X									

Table A-16a. ITS Data Flow Security Assessment: From TMS

Source	Physical Data Flow	Destination	Inter-connect	THREAT CATEGORIES						SECURITY SERVICES			
				DoS	Dis	Man	Mas	Rpy	Rpd	Aut	Con	Int	NRp
tms	incident information request	em	w	x		x	x			x		x	
tms	incident notification	em	w	x		x	x			x		x	
tms	pollution state data request	emms	w	x		~	x			x			
tms	traffic information	isp	w	x		~	x			x			
tms	demand management price change request	pms	w	x		~	x			x			
tms	parking instructions	pms	w	x		~	x			x			
tms	operational data	ps	w	x		~	x			x			
tms	AHS control information	rs	w	x		x	x			x		x	
tms	freeway control data	rs	w	x		x	x			x		x	
tms	hri control data	rs	w	x		x	x			x		x	
tms	hri request	rs	w	x		~	x			x			
tms	signage data	rs	w	x		~	x			x			
tms	signal control data	rs	w	x		x	x			x		x	
tms	surveillance control	rs	w	x		~	x			x			
tms	demand management price change request	tas	w	x		~	x			x			
tms	demand management price change request	trms	w	x		~	x			x			
tms	signal priority status	trms	w	x		~	x			x			
tms	traffic information	trms	w	x		~	x			x			
tms	work schedule	x09	H	x									
tms	event confirmation	x19	w	x		~	x		x	x			x
tms	map update request	x23	w	x		~	x			x			
tms	TMC coord.	x35	w	x	x	x	x			x	x	x	
tms	traffic operations data	x46	H	x									
tms	violation notification	x62	w	x	x	~	x			x	x		
tms	license request	x64	w	x		~	x			x			
tms	hri advisories	x67	w	x		x	x			x		x	

Table A-16b. ITS Data Flow Security Assessment: To TMS

Source	Physical Data Flow	Destination	Inter-connect	THREAT CATEGORIES						SECURITY SERVICES			
				DoS	Dis	Man	Mas	Rpy	Rpd	Aut	Con	Int	NRp
em	emergency vehicle greenwave request	tms	w	x		x	x			x		x	
em	incident information	tms	w	x		x	x			x		x	
em	incident response status	tms	w	x		x	x			x		x	
emms	widearea statistical pollution information	tms	w	x		~	x			x			
isp	incident notification	tms	w	x		x	x			x		x	
isp	logged route plan	tms	w	x	x	x	x			x	x	x	
isp	request for traffic information	tms	w	x		~	x			x			
isp	road network use	tms	w	x	x	~	x			x	x		
pms	demand management price change response	tms	w	x		~	x			x			
pms	parking availability	tms	w	x		~	x			x			
ps	planning data	tms	w	x		~	x			x			
rs	AHS status	tms	w	x		~	x			x			
rs	fault reports	tms	w	x		~	x			x			
rs	freeway control status	tms	w	x		~	x			x			
rs	HOV data	tms	w	x		~	x			x			
rs	hri status	tms	w	x		x	x			x		x	
rs	incident data	tms	w	x	x	~	x			x	x		
rs	intersection blockage notification	tms	w	x		x	x			x		x	
rs	local traffic flow	tms	w	x		~	x			x			
rs	request for right of Way	tms	w	x		~	x			x			
rs	signal control status	tms	w	x		~	x			x			
rs	signal priority request	tms	w	x		~	x			x			
rs	vehicle probe data	tms	w	x	x	~	x			x	x		
tas	demand management price change response	tms	w	x		~	x			x			
tas	probe data	tms	w	x		~	x			x			
trms	demand management price change response	tms	w	x		~	x			x			
trms	request for transit signal priority	tms	w	x		~	x			x			
trms	transit system data	tms	w	x		~	x			x			

Table A-16b (Continued). ITS Data Flow Security Assessment: To TMS

Source	Physical Data Flow	Destination	Inter-connect	THREAT CATEGORIES						SECURITY SERVICES			
				DoS	Dis	Man	Mas	Rpy	Rpd	Aut	Con	Int	NRp
x09	work zone status	tms	H	x			x			x			
x19	event plans	tms	w	x		~	x			x			
x23	map updates	tms	w	x		~	x			x			
x35	TMC coord.	tms	w	x	x	x	x			x	x	x	
x46	traffic control	tms	H	x			x			x			
x58	weather information	tms	w	x		~	x			x			
x64	registration	tms	w	x	x	~	x			x	x		
x67	railroad advisories	tms	w	x		x	x			x		x	
x67	railroad schedules	tms	w	x		~	x			x			

Table A-17a. ITS Data Flow Security Assessment: From TRMS

Source	Physical Data Flow	Destination	Inter-connect	THREAT, CATEGORIES						SECURITY SERVICES			
				DoS	Dis	Man				Aut	Con	Int	NRp
trms	security alarms	em	w	x		x	x			x		x	
trms	demand responsive transit plan	isp	w	x	x	x	x			x	x		
trms	transit and fare schedules	isp	w	x	x	x	x			x	x	x	
trms	transit request confirmation	isp	w	x	x	x	x	x	x	x	x	x	x
trms	demand responsive transit route	pias	w,u1t	x	x	~	x			x	x		
trms	parking lot transit response	pms	w	x		~	x			x			
trms	operational data	ps	w	x		~	x			x			
trms	emergency acknowledge	rts	w	x		x	x			x		x	
trms	transit and fare schedules	rts	w	x	x	~	x		x	x	x		x
trms	traveler information	rts	w	x	x	x	x	x	x	x	x	x	x
trms	demand management price change response	tms	w	x		~	x			x			
trms	request for transit signal priority	tms	w	x		~	x			x			
trms	transit system data	tms	w	x		~	x			x			
trms	bad tag list	trvs	u1t	x	x	x	x			x	x	x	
trms	driver instructions	trvs	u1t	x	x	~	x			x	x		
trms	emergency acknowledge	trvs	u1t	x		x	x			x		x	
trms	request for vehicle measures	trvs	u1t,u2	x		~	x			x			
trms	schedules, fare info request	trvs	u1t	x	x	x	x	x	x	x	x	x	x
trms	traveler information	trvs	u1t	x	x	x	x		x	x	x	x	x

Table A-17a (Continued). ITS Data Flow Security Assessment: From TRMS

Source	Physical Data Flow	Destination	Inter-connect	THREAT CATEGORIES						SECURITY SERVICES			
				DoS	Dis	Man	Mas	Rpy	Rpd	Aut	Con	Int	NRp
trms	intermodal information	x02	w	x		~	x			x			
trms	payment request	x21	w	x	x	x	x	x	x	x	x	x	x
trms	map update request	x23	w	x		~	x			x			
trms	TRMS coord	x33	w	x		~	x			x			
trms	camera control	x42	w	x		x	x			x		x	
trms	emergency acknowledge	x42	w	x		x	x			x		x	
trms	actual schedule and fare info	x47	H	x									
trms	transit operator display	x49	H	x									
trms	route assignment	x52	H	x									
trms	work schedule	x53	H	x									
trms	violation notification	x62	w	x	x	~	x			x	x		

Table A-17b. ITS Data Flow Security Assessment: To TRMS

Source	Physical Data Flow	Destination	Inter-connect	THREAT CATEGORIES						SECURITY SERVICES			
				DoS	Dis	Man	Mas	Rpy	Rpd	Aut	Con	Int	NRp
em	transit emergency coordination data	trms	w	x		x	x			x		x	
isp	demand responsive transit request	trms	w	x	x	~	x			x	x		
isp	selected routes	trms	w	x	x	x	x	x	x	x	x	x	x
isp	transit information request	trms	w	x	x	x	x	x	x	x	x	x	x
pias	demand responsive transit request	trms	u1t	x	x	~	x			x	x		
pms	transit parking coordination	trms	w	x		~	x			x			
rts	emergency notification	trms	w	x	x	x	x			x	x	x	
rts	transit request	trms	w	x	x	x	x	x	x	x	x	x	x
rts	traveler information request	trms	w	x	x	x	x	x	x	x	x	x	x
tms	demand management price change request	trms	w	x		~	x			x			
tms	signal priority status	trms	w	x		~	x			x			
tms	traffic information	trms	w	x		~	x			x			
trvs	emergency notification	trms	u1t	x	x	x	x			x	x	x	
trvs	fare and payment status	trms	u1t,u2	x	x	x	x	x	x	x	x	x	x
trvs	request for bad tag list	trms	u1t,u2	x		~	x			x			
trvs	transit vehicle conditions	trms	u1t,u2	x	x	~	x			x	x		
trvs	transit vehicle passenger and use data	trms	u1t,u2	x		~	x			x			
trvs	traveler information request	trms	u1t	x	x	x	x	x	x	x	x	x	x
trvs	vehicle probe data	trms	u1t	x		~	x			x			
x02	intermodal information	trms	w	x		~	x			x			
x21	transaction status	trms	w	x	x	x	x	x	x	x	x	x	x
x23	map updates	trms	w	x		~	x			x			
x33	TRMS coord	trms	w	x		~	x			x			
x42	physical activities	trms	P	x		x	x			x		x	
x47	schedule Guidelines	trms	H	x			x			x			
x49	transit operator fare schedules	trms	H	x			x			x			
x53	maint Status	trms	H	x			x			x			

Table A-18a. ITS Data Flow Security Assessment: From TRVS

Source	Physical Data Flow	Destination	Inter-connect	THREAT CATEGORIES						SECURITY SERVICES			
				DoS	Dis	Man	Mas	Rpy	Rpd	Aut	Con	Int	NRp
trvs	local signal priority request	rs	u2	x		~	x	x		x			
trvs	emergency notification	trms	u1t	x	x	x	x			x	x	x	
trvs	fare and payment status	trms	u1t,u2	x	x	x	x	x	x	x	x	x	x
trvs	request for bad tag list	trms	u1t,u2	x		~	x			x			
trvs	transit vehicle conditions	trms	u1t,u2	x	x	~	x			x	x		
trvs	transit vehicle passenger and use data	trms	u1t,u2	x		~	x			x			
trvs	traveler information request	trms	u1t	x	x	x	x	x	x	x	x	x	x
trvs	vehicle probe data	trms	u1t	x		~	x			x			
trvs	traveler advisory request	vs	w	x		~							
trvs	transit user fare status	x50	H	x									
trvs	transit user outputs	x50	H	x									
trvs	transit driver display	x52	H	x									
trvs	request for payment	x61	s	x		~	x	x	x	x			x

Table A-18b. ITS Data Flow Security Assessment: To TRVS

Source	Physical Data Flow	Destination	Inter-connect	THREAT CATEGORIES						SECURITY SERVICES			
				DoS	Dis	Man	Mas	Rpy	Rpd	Aut	Con	Int	NRp
trms	bad tag list	trvs	u1t	x	x	x	x			x	x	x	
trms	driver instructions	trvs	u1t	x	x	~	x			x	x		
trms	emergency acknowledge	trvs	u1t	x		x	x			x		x	
trms	request for vehicle measures	trvs	u1t,u2	x		~	x			x			
trms	schedules, fare info request	trvs	u1t	x	x	x	x	x	x	x	x	x	x
trms	traveler information	trvs	u1t	x	x	x	x		x	x	x	x	x
vs	vehicle location	trvs	w	x		~							
x50	emergency notification	trvs	H	x									
x50	transit user inputs	trvs	H	x									
x51	vehicle measures	trvs	w	x		~							
x52	transit driver inputs	trvs	H	x			x			x			
x61	payment	trvs	s	x		x	x	x	x	x		x	x

Table A-19a. ITS Data Flow Security Assessment: From VS

Source	Physical Data Flow	Destination	Inter-connect	THREAT CATEGORIES						SECURITY SERVICES			
				DoS	Dis	Man	Mas	Rpy	Rpd	Aut	Con	Int	NRp
vs	cargo data request	cvs	w	x		~							
vs	emergency notification	em	u1t	x	x	x	x			x	x	x	
vs	vehicle location	evs	w	x		~							
vs	traveler information request	isp	u1t	x	x	x	x	x	x	x	x	x	x
vs	trip confirmation	isp	u1t	x		~	x			x			
vs	trip request	isp	u1t	x	x	~	x			x	x		
vs	vehicle probe data	isp	u1t	x	x	~	x			x	x		
vs	yellow pages request	isp	u1t	x	x	~	x			x	x		
vs	tag data	pms	u2	x	x	x	x	x	x	x	x	x	x
vs	ahs vehicle data	rs	u2	x		x	x			x		x	
vs	vehicle probe data	rs	u2	x	x	x	x			x	x	x	
vs	tag data	tcs	u2	x	x	x	x	x	x	x	x	x	x
vs	vehicle location	trvs	w	x		~							
vs	vehicle control	x03	w	x		~							
vs	driver updates	x12	H	x									
vs	transaction status	x12	H	x									
vs	map update request	x23	u1t	x		~	x			x			
vs	vehicle to vehicle coordination	x34	u3	x		x	x	x		x		x	
vs	request for payment	x61	s	x		~	x	x	x	x			x

Table A-19b. ITS Data Flow Security Assessment: To VS

Source	Physical Data Flow	Destination	Inter-connect	THREAT CATEGORIES						SECURITY SERVICES			
				DoS	Dis	Man	Mas	Rpy	Rpd	Aut	Con	Int	NRp
cvs	processed cargo data	vs	w	x		~							
em	emergency acknowledge	vs	u1t	x		x	x		x	x		x	x
isp	broadcast information	vs	u1b	x		~	x			x			
isp	traveler information	vs	u1t,u1b	x	x	x	x		x	x	x	x	x
isp	trip plan	vs	u1t	x	x	~	x			x	x		
pms	request tag data	vs	u2	x	x	x	x	x	x	x	x	x	x
pms	tag update	vs	u2	x	x	x	x	x	x	x	x	x	x
rs	AHS control data	vs	u2	x		x	x	x		x		x	
rs	intersection status	vs	u2	x		x	x	x		x		x	
rs	request tag data	vs	u2	x		~	x	x	x	x			x
rs	vehicle signage data	vs	u2	x		~	x	x		x			
tcs	request tag data	vs	u2	x		~	x	x	x	x			x
tcs	tag update	vs	u2	x	x	x	x	x	x	x	x	x	x
trvs	traveler advisory request	vs	w	x		~							
x03	vehicle measures	vs	w	x		~							
x12	driver inputs	vs	H	x			x			x			
x12	request for service	vs	H	x			?			?			
x23	map updates	vs	w	x		~	x			x			
x26	position fix	vs	L	x		x	x			x		x	
x34	vehicle to vehicle coordination	vs	u3	x		x	x	x		x		x	
x39	physical presence	vs	P	x									
x40	roadway conditions	vs	P	x									
x41	weather conditions	vs	P	x									
x61	payment	vs	s	x		x	x	x	x	x		x	x

A.3 DATA FLOW ASSESSMENT OBSERVATIONS

The ITS data flow assessment observations are derived not only from the results displayed in tables A-l through A-19 but also from the assessment process itself. Observations have been segregated into general, threat category, security service, and high-level statistical observations.

A.3.1 General Observations

More often than not, the physical data flow name and description do not provide sufficient detail to determine applicable threats. As noted, this data flow assessment involved a review of the complete data flow structure (i.e., from the physical data flow, through each level of logical data flow, to the primitive elements). The hierarchical nature of the data flow structure suggests individual data elements at the lowest level may subject the data flow to various threats. Alternatively, some physical data flow descriptions (the highest level of the data flow structure) suggest exposure to certain threats regardless of the information revealed in the constituent logical data flows.

When performing the assessment, the data flow could not be accurately assessed by the name of the physical data flow alone. Often the physical data flow names are counter-intuitive or more or less descriptive than anticipated. Although the National ITS Architecture attempts to reuse as much information as possible, the physical data flow names and structures did not lend themselves to the same reuse with regard to security threats and services. More precisely, physical data flows of the same name may not be subject to the same threat categories and, therefore, may require a different set of security services. One must review all of the constituent logical data flows, the source and destination subsystems, and the interconnect (i.e., interface type) to determine appropriate threat categories and associated security services.

A.3.1.1 Considerations for the Constituent Logical Data Flows

The physical data flow “broadcast information” from the Information Service Provider (ISP) to the Remote Traveler Subsystem (RTS) (e.g., a kiosk) uses either a wireline or two-way wide-area wireless communications (i.e., interconnect method) and contains no personal or private organizational information; hence, disclosure was not considered a threat to this data flow (refer to section A.3.2 regarding “Disclosure”).

The physical data flow “broadcast information” (same name) from Information Service Provider (ISP) to Personal Information Access Subsystem (PIAS) (e.g., a traveler’s palmtop computer) also uses either a wireline or two-way wide-area wireless interconnect. However, this data flow comprises significant personal information and is therefore subject to the threat of disclosure.

A.3.1.2 Considerations for the Source and Destination Subsystems

Data flows with the same name but with different end-systems may be vulnerable to different threats due to the physical location of the subsystems and/or the type of end-system involved -- for example, a critical subsystem like the Emergency Management subsystem (EM).

The first instance (i.e., physical location of the subsystems) is illustrated by the Vehicle Subsystem (VS) to Commercial Vehicle Subsystem (CVS) interconnect. These two subsystems are not only collocated (which is by no means reason to disregard any threat), but most often are mounted in the same rack and hard-wire connected. Considering the

physical location and configuration, data flows between these subsystems are often less vulnerable to particular threats.

The second instance (i.e., the type of end-system involved) is illustrated by a physical data flow named "map updates" that is provided from the Map Update terminator (X23) to several ITS subsystems. Most instances of this data flow are considered non-real-time or non-critical, except the one provided to the Emergency Management subsystem (EM). The emergency management map information is frequently a real-time update required for routing emergency vehicles. Due to the application of this data flow, it is more vulnerable to manipulation than other "map update" data flows, and an additional level of integrity is required to ensure the information is provided in an accurate and timely manner.

A.3.1.3 Considerations for the Interconnect

Although some data flows have the same name, they occasionally have different interconnects. For example, "vehicle probe data" is the name of a short-range wireless (U2) interconnect between the Vehicle Subsystem (VS) and the roadside subsystem (RS). It is also the name of a two-way wide-area wireless interconnect between the Transit Vehicle Subsystem (TRVS) and the Transit Management Subsystem (TRMS) as well as a wireline interconnect between the Roadway Subsystem (RS) and the Traffic Management Subsystem (TMS). These three identically-named data flows are not only different in content, but they are also more or less vulnerable to particular threats due to the transmission media or interface type (e.g., independent of message content, wireless interfaces are more susceptible to replay than wireline interfaces).

Throughout the National ITS Architecture and associated with every subsystem there are instances of four uncommon interconnects (i.e., interface types): physical (P), human (H), payment instrument (S), and position location (L). These interconnects were considered in this assessment as follows:

- **"P" or "Physical" Interconnects:** the "P" or "physical" interconnects are interfaces that sense a physical characteristic or cause an action that is not represented using standard communications technology (e.g., observing an obstacle in the roadway). This interconnect is illustrated by the "physical presence" data flow between the Potential Obstacles terminator (X39) and the Vehicle Subsystem (VS). This flow indicates the detection of obstacles that may include animals, vehicles, or rocks in roadway. There were no threat categories identified and, hence, no recommended security services, for the data flows of this interconnect type.

- **"H" or "Human" Interconnects:** the "H" or "human" interconnects are interfaces between a human user, operator, or driver and a subsystem. This interconnect is illustrated by the "CVO driver initialization" and the "log information" data flows between the Commercial Vehicle Driver terminator (X06) and the Commercial Vehicle Subsystem (CVS). The former data flow consists of driver instructions to the commercial vehicle, and the latter data flow consists of information to be entered into the driver log. For the "II" or "human" interconnects, applicable threat categories (primarily masquerading) are identified if the information flow was human-to-subsystem (exceptions included systems that allow public access (e.g., kiosks)). However, if the subsystem is providing

information to the human, no data flow threat categories are identified and, hence, no security services are recommended.

- **"S" or "Payment Instrument" Interconnects:** "S" or "payment instrument" interconnects are interfaces between either a smart-card or a non-smart-card (e.g., magnetic swipe card) carried by the traveler and an object that accepts this information such as a reader at a kiosk or in a vehicle. This interconnect is illustrated by the "request for payment" and "payment" data flows between the Payment Instrument terminator and the Remote Traveler Subsystem (RTS) (e.g., kiosk).

  Depending on the type of information exchanged, the flows of interconnect type "S" or "payment instrument" may be vulnerable to any of the particular threat categories except disclosure. Disclosure is not identified as a viable threat in this case because the data flow is the actual reading of/writing to the smart card by the reader. The threat of disclosure in these particular transactions is negligible. However, due to the financial sensitivity of smart card transactions, manipulation, masquerading, replay, and repudiation threats are viewed as viable threats. Hence, authentication, integrity, and non-repudiation security services are required to protect these transactions.

- **"L" or Position Location Interconnects:** "L" or "position location" interconnects are interfaces between position location equipment and the source for indicating the position location (e.g., Global Positioning Satellite (GPS), Frequency Modulation (FM) Subcarrier, Dead Reckoning, etc.). This interconnect is illustrated by the "position fix" data flow from the Location Data Source terminator (X26) to the Vehicle Subsystem (VS). This data flow provides information (e.g., latitude, longitude) about a vehicle's position.
  Most often these types of data flows would be subject to masquerading and manipulation and, hence, would require some form of authentication and additional integrity.

A.3.2 Security Threat Category Observations

The following observations were made regarding the six categories of threats.

A.3.2.1 Denial of Service

As noted previously, all data flows are subject to denial-of-service attacks, yet the security service to counter these types of threats is most commonly implemented at the subsystem level. For this reason, all data flows are identified as subject to denial of service, yet no security services to thwart denial-of-service threats (e.g., availability) are identified in tables A- 1 through A- 19.

A.3.2.2 Disclosure

The threat of disclosure (and subsequently the confidentiality security service) was recognized for any data flow (including those at the lowest level of the data flow structure) comprising personal and/or private organizational information. All such information is considered confidential, and confidentiality services are recommended as appropriate.

Data flows between ITS subsystems or terminators not specifically containing such personal or private organizational information are not considered to be threatened by disclosure. For example, the physical data flow “incident information” from the Emergency Management subsystem (EM) to the Traffic Management Subsystem (TMS) provides notification of an incident and expected severity, location, and nature of the incident, yet contains no personal and/or private organizational information. Similarly, the data flow “vehicle probe data” from the Transit Vehicle Subsystem (TRVS) to the Transit Management Subsystem (TRMS) provides transit vehicle data indicating link time and location, yet also contains no personal and/or private organizational information.

However, in these particular instances, the Emergency Management, Transit Management, or Traffic Management facility supervisors may (for various reasons) request/require that these types of data flows be protected against disclosure and remain confidential. This is an implementation-dependent decision, and it is therefore reiterated that the identified threat categories represent the most probable threats to a particular data flow. Likewise, the recommended services represent a core set of service protections.

A.3.2.3 Manipulation

Manipulation is identified for only those data flows that are considered particularly vulnerable to major (often intentional) manipulative threats (e.g., vandalism, fraud) that could result in significant losses. This is opposed to most of the remaining data flows that are subject to minor (often accidental) threats (e.g., electrical surges, etc.) and may often be handled by the inherent functions of the underlying communications protocol (e.g., forward error correction (FEC)). Note that those data flows marked with an “X” in the “manipulation” column of tables A-l through A- 19 indicate a major threat of manipulation (e.g., the vandalism) while those marked with a "~" identify only a minor threat of manipulation (e.g., the electric surges, etc.).

The data flows most vulnerable to major threats of manipulation involved financial-, emergency-, incident-, or safety-related data. This categorization includes those data flows that directly impact vehicular traffic (e.g., influence drivers in the form of signals/messages) at roadway intersections or highway-rail intersections (HRI).

Integrity is viewed as additional integrity beyond that provided inherently by most communications protocols and is recommended only for those data flows identified as being subject to major threats of manipulation. Again, facility managers/supervisors may consider the need to protect particular data flows (i.e., those not identified as subject to manipulation in this assessment).

A.3.2.4 Masquerade

An unauthorized user (e.g., a hacker) armed with the proper set of tools could potentially masquerade as a number of legitimate ITS subsystems and/or terminators. For most of the data flows, identifying the source is necessary to ensure that the messages received were transmitted by an authentic subsystem/terminator. Results of this assessment indicate that 84 percent of the data flows are subject to masquerading and, thus, require some form of source authentication.

Those data flows not subject to masquerading most often involve wireline interconnects within the same vehicle (usually hardwired, possibly a small LAN); “H” or “human” interconnects for which information is provided from a subsystem to a human; and "P" or “physical” interconnects for which the actual item/sensor involved would have to be physically removed and replaced (to do so without detection is considered unlikely).

A.3.2.5 Replay

Only those data flows particularly vulnerable to replay were identified. Although, theoretically, one could capture and "replay" any message, clearly some data flows are more vulnerable to replay than others. This vulnerability is based on not only message content, but also the communications medium (e.g., wireline vs. wireless). For example, "road network use" is a wireline (W) data flow from the Information Service Provider (ISP) to the Planning Subsystem (PS), and it contains information for planning non-vehicle portions of traveler routes (e.g., cycling, walking, etc.). This data flow is not nearly as vulnerable to replay as the "tag data" data flow from the Vehicle Subsystem (VS) to the Toll Collection Subsystem (TCS). In this instance, "tag data" is provided over a short-range two-way wireless (U2) interface and contains a unique identification for the payment for services (toll tag data from on-board the vehicle, etc.). Intuitively, there are more motives and easier methods for replaying the wireless "tag data" data flow than the wireline "road network use" data flow. "Tag data" is more vulnerable to replay not only due to the message content, but also to the communications medium. In this assessment, "tag data" is considered to be vulnerable to replay.

A.3.2.6 Repudiation

This assessment identified only those data flows most vulnerable to threats of repudiation. For example, the "transaction status" data flow from the Financial Institution terminator (X2 1) to the Information Service Provider (ISP) provides confirmation of payments for electronic map updates and other services. The provision of service and/or payment confirmations (i.e., financial transactions) are obviously subject to repudiation.

Other data flows consisting of what may be considered to be common operational data are not considered susceptible to repudiation. However, facility supervisors may (for various reasons) request/require that these types of data flows be protected against repudiation as well. For example, the "signal priority status" data flow between the Traffic Management Subsystem (TMS) and the Transit Management Subsystem (TRMS) provides the status (e.g., enabled or disabled) of signal priority request functions at the roadside. Although the repudiation of such information seems unlikely and irrelevant, the Traffic Management facility supervisor may believe that the information is critical to protecting Traffic Management operations, say, from a legal or administrative position. Therefore, the data flow is considered to be subject to repudiation.

A.3.3 Security Service Observations

The ITS data flow security assessment not only identifies appropriate threat categories, but also recommends an appropriate combination of security services. General relationships are also illustrated by figure A-2.

This data flow assessment does not identify how to implement security services. Recall that security services are implemented by security mechanisms. These security mechanisms are the software, hardware, and/or procedures needed to enforce a particular security service. Each security service can be implemented by various mechanisms; furthermore, some security mechanisms can support more than one security service. The correct implementation or selection of mechanisms depends on specific system design and related environmental variables. Identifying specific security mechanisms to implement the assessed services would restrict system design flexibility.

Appendix E provides an extensive review of several security mechanisms and the associated standards that can be used for implementing the different security services (associations are illustrated in table E- 1). This information will help the reader understand which mechanisms can be used to implement particular security services and how these mechanisms function. Appendix F illustrates the implementation of information security services for various ITS data flows.

A.3.4 Statistical Observations

The following high-level statistical observations were based on the 374 physical data flows (comprising over 3000 constituent logical data flows) reviewed in this assessment.

- Eighty-four percent (84%) of the data flows are found to be subject to threats of masquerading and 19%, subject to threats of replay. Subsequently, 84% of the data flows (encompassing the 19% subject to replay) require some form of authentication. The high number of data flows subject to masquerading and hence requiring authentication reflects the importance of this service in a distributed system. It also illustrates the fact that authentication provides a basis for the other security services.

- Thirty-two percent (32%) of the data flows are found to be subject to disclosure (within the considerations of disclosure for this assessment) and, therefore, 32% require confidentiality. Considering the many traveler information services within the ITS, it is not surprising that nearly one-third of the data flows contain private or confidential information.

- Eighty-two percent (82%) of the data flows are found to be subject to threats of manipulation. Thirty-four percent (34%) are considered vulnerable to major threats of manipulation (e.g., fraud) and, therefore, require some form of supplemental integrity (integrity beyond that inherently provided by typical communications protocols). The remaining 48% are considered vulnerable to minor threats of manipulation (e.g., electrical surge). The data flows requiring additional integrity are primarily the result of emergency-, incident-, safety-, and financial-related transactions within the ITS.

- Seventeen percent (17%) of the data flows are found to be subject to repudiation (within the considerations of repudiation for this assessment) and, therefore, 32% require non-repudiation. Repudiation is primarily found to impact those data flows involving the provision or confirmation of services and/or payments.

APPENDIX B

COMMUNICATIONS INFRASTRUCTURE ASSESSMENT

This section describes the assessment of impacts to ITS given a communications denial of service. First, the approach and methodology are described; then, the findings of the communications infrastructure assessment; and finally, major observations regarding the impacts to ITS.

B.l APPROACH AND METHODOLOGY

A high level assessment of the following communications technologies utilized for ITS operations (i.e., data, voice, and video) was conducted:

- Wireline
- Two-way wide-area wireless
- One-way wide-area wireless
- Dedicated short-range communications (DSRC)
- Vehicle-to-vehicle

The intent of the assessment was to identify the impacts to ITS in the event of a major communications denial of service. Types of communications denial of service include, but are not limited to:

- Major outage
- Degraded service, degraded performance, or interruptions
- Service unavailable to some or all users, applications, regions, or devices

The purpose of this section is to emphasize the importance of the communications infrastructure and to identify the threats to it. The underlying communications infrastructure supports messages (comprising ITS data flows) which in turn support the operations of the ITS subsystems. This section summarizes the impacts ITS should one of the underlying communications technologies become unavailable (e.g., a power blackout taking down all wireline communications in a metropolitan area). Additionally, the focus is on threats and not on vulnerabilities since we are assessing an architecture and not a specific implementation.

In assessing the communications denial of service impacts to ITS, the specific threats were analyzed and potential communications impairments were identified. Additionally, information from the subsystem and the data flow assessments was used to determine major impacts. Relevant threat scenarios were extracted from these assessments to reiterate the impact to ITS and the users of ITS based services.

B.2 LOSS OF ITS COMMUNICATION SERVICES

As the transportation infrastructure becomes automated, so does the increased interaction with other existing infrastructures such as those in banking and commercial enterprise.

Like these existing infrastructures, ITS relies heavily on many of the communications technologies that make up the nation's collection of intertwined automated telecommunications networks and computer systems. ITS depends on such collections of communications technologies for overall performance and functionality.

For each of the five communications technologies utilized by ITS, the following sections contain:

- A description of its characteristics as defined in the National ITS Architecture
- An identification of specific threats to its availability
- A descriptions of its denial of service impacts to ITS

The examples presented illustrate a range of impairments from the more detrimental (e.g., time-critical, life threatening) to the mundane (e.g., delay of statistical data).

B.2.1 Wireline

- Description: there are numerous wireline technologies to provide for fixed-to-fixed communications requirements. For example, leased or owned twisted wire pairs, coaxial cable, or fiber optics can be used for some transmissions. In other applications, it may be more advantageous to use terrestrial microwave links or cellular radio networks to provide communications. Although the above are wireless communications technologies, they are used to provide fixed-to-fixed communications, and consequently the architecture recognizes them as wireline communications media. Wireline transmissions include data, voice, and video.

  Wireline network options include the use of private networks, public shared networks, or a mixture of the two. Private network technologies assessed by the architecture team include Ethernet, Fiber Distributed Data Interface (FDDI), Synchronous Optical NETwork (SONET), and Asynchronous Transfer Mode (ATM). Public shared network technologies assessed include leased analog lines, leased digital lines, frame relay, Integrated Services Digital Network (ISDN), metropolitan ethernet, Internet, and Switched Multimegabit Data Service (SMDS). [National ITS Architecture, 1997]

- Exemplary threats to wireline communications:

  - Any act of nature that could damage or destroy the actual physical lines, power plants, and/or microwave radios and antennas (Note: major telecommunications companies have some level of backup capabilities and can reroute traffic as needed, etc.)
  - Construction near roadside equipment, other ITS subsystem, or buried wireline cable could sever wireline connections (Note: recommend use of a sophisticated network management system to detect and locate problem.)
  - Fluctuations in the power source may cause time-outs and retransmission, either of which could introduce additional delays
  - Unreliable power supply due to employee strikes or summertime brownouts may introduce unreliable service
  - A number of intentional threats such as a terrorist or disgruntled employee who gains physical access to the switching station and modifies route controllers (Note: physical procedures and controls are currently in place at major switching stations with the intent to preclude or minimize such an occurrence.)

- Accidental network saturation during a natural disaster when citizens will be making telephone calls to family members potentially congesting any available bandwidth and impeding emergency related transmissions (Note: according to [The Reliable Services for General Users Subgroup, 1995] the Public Switched Network (PSN) is extremely reliable at a rate greater than 99.98%.)

- Exemplary impacts of wireline communications loss: the impact to ITS due to unavailable wireline communications is significant given that fifteen (15) of the nineteen (19) ITS subsystems use wireline to communicate with other ITS subsystems and terminators. Two subsystems are completely dependent on wireline communications. Additionally, all center subsystems are linked via wireline connections.

  The importance of ITS wireline transmissions, the dependence upon supporting wireline technologies, and the impact if/should this infrastructure be partially or wholly compromised is exemplified in the wireline communications between the Roadway Subsystem (RS) and the Traffic Management Subsystem (TMS) [note: TMS depends exclusively on wireline communications]. Without wireline connectivity or with intermittent, unreliable connections, the RS would be unable to exchange several forms of time-sensitive information. Specifically, traffic control, highway rail intersection (HRI), signal control, intersection collision avoidance, and right-of-way messages would be affected, thereby potentially placing travelers in unsafe conditions. Enhancing the severity of potential incidents, emergency requests depending partially or wholly on wireline communications might not be transmitted leaving travelers without timely medical assistance. Also, HAZMAT recovery crews depend on wireline connections to the Fleet and Freight Management Subsystem (FMS) for hazardous material information. Such information may not be available for an appropriate and timely response.

  Wireline losses would also impact the surface transportation of goods. Commercial carriers transporting food or medical supplies to remote areas of the country could be delayed if continual delays are incurred at commercial vehicle checkstations that have lost wireline connectivity.

  While the above scenarios illustrate more significant impacts to ITS, a partial or complete wireline outage could also cause various minimal impacts to ITS as well. For example, the Planing Subsystem (PS), using wireline connections exclusively, provides historical operational data for traffic simulation and prediction functions. Transportation planning and traffic management entities could possibly tolerate delays for this application. As long as delays are within an acceptable range, toll and parking financial transactions can also tolerate wireline losses. However, lengthy delays in processing could impact cash flow, bookkeeping, and accounting processes.

B-2.2 Two-Way Wide-Area Wireless

- Description: wide-area wireless communications are suited for services and applications where information is disseminated to users who are not located near the source of transmission and who require seamless coverage. Wireless communications are concerned primarily with data transmissions.

Several two-way wide-area wireless technologies were assessed by the National ITS Architecture team. They included Global System for Mobile Communications (GSM), Special Mobile Radio (SMR), Enhanced Special Mobile Radio (ESMR), Personal Communications System (PCS), ARDIS, RAM, Geotek, 220 MHz, Metricom, Tether-less Access Ltd. (TAL), two-way paging, and Cellular Digital Packet Data (CDPD). [National ITS Architecture, 1997]

Given the limited geographic coverage of existing two-way wide area wireless technologies, emerging satellite communications technologies were also considered. Systems assessed included ORBCOMM, STARSYS, VITASAT, MSAT, Constellation, GLOBALSTAR, IRIDIUM, TELEDESIC, Ellipso, Odyssey, Skycell, VSAT, and OmniTRACS.

- Exemplary threats to two-way wide-area wireless communications:

  - Any of the above wireline examples due to the reliance on wireline services to connect calls between the two infrastructures
  - Any act of nature that could physically damage or destroy the communications towers, base stations, antennas, and repeaters (note: most likely, wireless service providers will provide some type of back-up service for those intermittent power fluctuations, system hiccups, etc.)
  - A number of intentional threats to the host computers accessed via two-way wide-area wireless (e.g., a hacker could gain access to a host computer system and modify system configurations, data, and system software thereby disrupting and/or denying service originating or passed through this system)
  - Accidental modifications to host computers due to operator or user error
  - Accidental or intentional saturation of the airwaves resulting in cross-talk, or unintelligible conversations (note: saturation of the finite bandwidth available for cellular calls could result in denial of emergency assistance during peak hours
  - Threats of disclosure (note: cellular scanners -- although legal for cellular phone repair, yet illegal for intercepting calls [Garg, 1996] -- are in use today. This is evident in the recent news coverage of House Speaker Newt Gingrich's cellular call intercepted by a Florida couple [Washington Post, 1997]
  - Limited coverage and service based on geographic region, frequency allocations, and roaming agreements
  - Dependence upon costly satellite communications technologies
  - Adverse geographic location (e.g., mountains, valleys, high buildings)
  - Incompatible devices and protocols among various cell phone manufactures
  - Theft of services (i.e., cloning of cellular phones)
  - Jamming

- Exemplary impacts of two-way wide-area wireless communications loss: as with wireline, the impact to ITS due to unavailable two-way wide-area wireless communications is significant since eleven (11) of the nineteen (19) ITS subsystems use two-way wide-area wireless to communicate with other ITS subsystems and terminators.

  ITS two-way wide-area wireless transmissions include, but are not limited to: traveler information, trip plans, transit driver instructions, transit fare transactions, payment information, commercial driver dispatches and routing instructions, commercial vehicle enrollment and payment information, commercial vehicle safety data, emergency requests and acknowledgments, and HAZMAT information.

The Emergency Management subsystem (EM) uses two-way wide-area wireless extensively to communicate with emergency vehicles as well as with travelers on foot or in their automobiles. These types of transmissions exemplify the dependence upon this supporting communications technology for prompt emergency response. With total loss or even partial wireless connectivity, emergency crews would not be able to provide timely emergency assistance, coordinate responses with appropriate agencies, or provide route planning for responding emergency crews. The impacts could be severe if the incident involved multiple cars, commercial vehicles transporting hazardous material, or motorcades transporting high-level Government officials. Portions of the emergency response coordination involve the exchange of commercial vehicle HAZMAT information to ensure proper, safe, and timely cleanup/removal.

Two-way wide-area wireless transmissions from the FMS to Commercial Vehicle Subsystem (CVS) include vehicle safety data. Should this communication degrade or become completely unavailable, unsafe commercial vehicles may be permitted to travel on highways and potentially endanger travelers. Without wireless communications, commercial vehicle weigh-in-motion (WIM) facilities may have to revert to manual mode to ensure that only vehicles passing the safety inspection are permitted on the roadways. Not only could this manual process delay the transport of goods, but it could introduce significant traffic congestion.

While the above scenarios describe time-critical and possibly life-threatening situations, the loss of two-way wide-area wireless could include tolerable delays that impact traveler convenience. Information such as transit and traveler information (e.g., map updates, trip plans) may be delayed or unavailable to travelers. Again. such circumstances would impact consumer trust in ITS, but most often, they would not generate any of the more severe impacts.

B.2.3 One-Way Wide-Area Wireless

- Description: one-way, broadcast communications technologies examined included AM subcarrier, FM subcarrier, and Highway Advisory Radio (HAR). FM subcarrier systems assessed included The Mitre Corporation's Subcarrier Traffic Information Channel (STIC), NHK's Data Radio Channel (DARC), SEIKO's High Speed FM Subcarrier Data System (HSDS), RBDS, ALERT, and Modulation Sciences, Inc.'s SCA. One-way wide-area wireless communications are concerned mostly with data transmissions. [National ITS Architecture, 1997]

- Exemplary threats to one-way wide-area wireless communications:

  - Any act of nature that could physically damage or destroy the communications towers, base stations, antennas, and repeaters
  - A number of intentional threats to the host computers accessed via one-way wide-area wireless
  - Accidental modifications to host computers due to operator or user error (e.g., repair or configuration)
  - Accidental or intentional saturation of the airwaves resulting in cross-talk, or unintelligible conversations
  - Adverse geographic location (e.g., mountains, valleys, high buildings)
  - Incompatible devices and protocols among various manufactures
  - Hardware failure
  - Other threats of disclosure and masquerading

- Exemplary impacts of one-way wide-area wireless communications loss: based on the National ITS Architecture, few data flows rely on a broadcast or one-way wide-area wireless communications medium. The type of information transmitted via this infrastructure includes traveler and traffic information (e.g., common link travel times, advisories, transit schedule exceptions, traveler routing, yellow pages information). Much of this information is not severely time-critical and only a small number of data flows utilize this particular medium. Therefore, the threat impacts to ITS are not as significant as those for the communications technologies discussed above.

  Impacts to ITS based on loss of one-way wide-area wireless are primarily delays or inconveniences to travelers. However, while most impacts are not life threatening or jeopardizing national security, these losses could result in a negative public perception of ITS. Likewise, commercial vendors and service providers may lose confidence in ITS and withdraw from their public sector relations. Lengthy outages would disrupt traffic and route planning and cause a loss of consumer confidence in the system. The loss of wide-area wireless communications, even temporarily, could cause traffic disruptions, particularly after travelers have become accustomed to using their onboard devices for weather, advisory, and routing information.

  Some of these transmissions while not time-critical may contain financial-related information (e.g., confirmation of payment). With these types of transactions, a communications delay can be tolerated within an acceptable time frame.

B.2.4 Dedicated Short-Range Communications (DSRC)

- Description: short range wireless is concerned with information transfer that is of a localized interest. The architecture team assessed radio frequency (RF) and Infrared (IR) short range wireless beacon/tag communications for the DSRC requirement. DSRC is concerned primarily with data transmissions. [National ITS Architecture, 1997]

- Exemplary threats to dedicated short-range communications (DSRC):

  - Any act of nature that could physically damage or destroy the roadside beacons or equipment housed in a roadside subsystem
    A number of intentional threats to the host computers
  - Accidental modifications to host computers due to operator or user error (e.g., repair or configuration)
  - Roadside or en route jamming
    Incompatible protocols among various manufactures
    Hardware failure
  - Incompatibility between roadside equipment and vehicle devices
    Other threats of disclosure, masquerading, or replay

- Exemplary impacts of dedicated short-range communications (DSRC) loss: data between the roadside subsystems and the onboard vehicle systems are transmitted extensively using this communications technology. DSRC transmissions include vehicle safety data, tag data, parking fee payments, commercial vehicle credentials, and intersection collision avoidance data. Many of these transmissions are time-critical.

Impacts to ITS based on loss of DSRC are greater for safety related transmissions. The loss of commercial vehicle safety inspection data could jeopardize the traveling public allowing unsafe trucks on the highways; the loss of signal preemption capability could impede timely emergency response, and the loss of intersection collision avoidance data from the roadside to passing vehicles could result in automotive accidents.

Similar to two-way wide-area wireless, without DSRC capabilities, commercial vehicle weigh-in-motion (WIM) facilities or roadside checkstations may have to revert to manual inspections to ensure that only safe vehicles are permitted on the roadways. Not only would this manual process delay the transport of goods, but it would also cause congestion on connecting highways and arterial roadways. Likewise, the lack of automated processes could introduce human error (e.g., mistyped entries) that result in similar adverse impacts.

Also important, yet slightly less significant, are the potential delays and unnecessary traffic jams due to loss of automated transmission of commercial vehicle enrollment credentials and tag data. Additionally, sporadic or continual loss of DRSC capabilities at toll collection subsystems could be detrimental to the revenue collection process and cause substantial accounting problems.

B.2.5 Vehicle-to-Vehicle

- Description: vehicle-to-vehicle (mobile-to-mobile) short range wireless communications are required to support the Automated Highway System (AHS), and most likely, intersection collision avoidance implementations. This technology area is still in the research phase. [National ITS Architecture, 1997]

- Exemplary threats to vehicle-to-vehicle communications:

  - Intentional and accidental misconfiguration of the onboard vehicle system
  - Roadside or en route jamming (e.g., some type of intentional threat or act of terrorism)
  - Faulty repair of the onboard vehicle system
  - Incompatible protocols and/or equipment/devices

- Exemplary impacts of vehicle-to-vehicle communications loss: this technology will be used for vehicles moving at high speeds on automated highways. Should this technology be unavailable to travelers intending on using these highways, travelers would possibly experience traffic delays and personal inconveniences. More importantly, should transmissions utilizing this technology become unreliable, the result could have severe personal and public safety impacts. Automobiles traveling in close proximity and at high speeds are dependent upon this technology as a reliable source for vehicle coordination and collision avoidance. Loss of vehicle-to-vehicle communications could result severe accidents and possible fatalities. Such harsh consequences could be compounded by the public questioning the application of this technology for ITS.

B.3 COMMUNICATIONS INFRASTRUCTURE ASSESSMENT OBSERVATIONS

General observations from the assessment include:

- Loss of communications impacts a variety of ITS functions including: emergency response, traffic management, transit management, traveler information, commercial vehicle operations, and financial transactions. Potential impacts should not be viewed as impediments to the deployment of ITS. Instead, they should drive the requirement for backup systems, alternate means for communications, etc.

- Although major telecommunications companies have backup capabilities and can reroute information traffic as needed, there are concerns for the other components of the infrastructure:

    - Have alternative communications media been considered?
    - Are other wireline and wireless backup capabilities adequate for ITS?
    - Have adequate network management systems to detect and locate problem been considered?

- Loss of communications causes regression to manual or non-automated methods. This introduces several considerations:

    - Will ITS information and systems become unreliable due to an increase in human error (e.g., from manual entry)?
    - Will the proper equipment be available?
    - Will employees/personnel/users be knowledgeable of manual procedures?
    - How long must legacy systems be maintained, and how can they be upgraded?

- Physical procedures and controls are currently in place at major PSN switching stations with the intent to preclude or minimize actual facility penetration. Similar procedures and controls should be considered for remote, logical access to ITS host computer systems?

- Proper transfers of data require interoperable (preferably standard) devices and protocols. Although numerous standards are in use today, the surface transportation community needs to continue support for general and ITS-specific standards development.

- Reliable communications services require collaborative efforts between public and private ITS developers and commercial communications providers.

Table B-l, ITS Subsystem Usage of Communication Media, identifies the type(s) of communications media utilized by each of the nineteen (19) ITS subsystems. Note, these are identified interconnects based on National ITS Architecture documents and do not reflect all possible (or probable) permutations.

Table B-l: ITS Subsystem Usage of Communications Media

	Wireline	Two-Way Wide-Area Wireless	One-Way Wide-Area Wireless	Dedicated Short-Range Comm	Vehicle to Vehicle
CVAS	x	x			
CVCS	x			x	
CVS		x		x	x
EM	x	x			
EMMS	x				
EVS		x		x	x
FMS	x	x			
ISP	x	x	x		
PIAS	x	x			
PMS	x			x	
PS	x				
RS	x			x	
RTS	x	x			
TAS	x				
TCS	x			x	
TMS	x				
TRMS	x	x			
TRVS		x	x	x	x
v s		x	x	x	x

APPENDIX C

INFORMATION SECURITY POLICY DOCUMENTS

The following documents contain information security policy for Federal systems as well as privacy policy and guidance for ITS systems:

- Office of Management and Budget Circular *No.* A- *130, Management of Federal Information Resources*, 8 February 1996 - establishes security policy for Federal automated information resources.
- Public Law 93-579, *The Privacy Act* of1974 - addresses protection of individual records or information maintained by a Federal agency.
- *Computer* Security *Act* of1987 - establishes security protection and privacy of sensitive information in Federal computer systems.
- ITS America's *Fair Information and Privacy Principles* - outlines the ITS industry's principles prepared in recognition of the importance of protecting individual privacy within ITS.
- *The Driver's Privacy Protection Act* of *1994* - protects the personal privacy and safety of licensed drivers, taking into account the legitimate needs of government and business.
- The *Anti-Hacker Bill* (signed October 11, 1996) - curbs computer crime and stiffens penalties for federal employees who violate individual privacy through access to government records.

APPENDIX D

EXAMPLES OF REAL-WORLD INFORMATION SYSTEMS ATTACKS

D.l DENIAL OF SERVICE

Denial of service pertains to any action or series of actions that prevent any part of a system from functioning as intended. Preventing a system or subsystem from functioning properly threatens system availability. Denial of service threats consist of intentional, accidental, or natural events, and they can take on many forms and can target particular parts of a system.

Traditional denial of service attacks involve the introduction of malicious code, such as a computer virus, that causes the system to perform unauthorized functions and/or become unavailable to authorized users. A computer virus is a program with the ability to reproduce by modifying other programs to include a copy of itself. Many viruses are benign, but in each case, a virus will cause at least some inconvenience and some loss of system access time. More destructive viruses may cause hardware and software destruction, lost system access time, and more significantly the loss of data. They may also move into multiple programs, data files or devices on a system and spread through multiple systems in a network. In 1988 there were less than a dozen computer viruses in existence. By 1992, there were nearly 1000 known virus strains in existence, including the infamous yet fizzled "Michelangelo". The U.S. Department of Justice indicated that the government expected to see an additional 600 viruses and mutant strains introduced during 1992; that's almost two per day [CSI, 1994]. Current rates of infection are difficult to determine objectively.

On the other hand, computer bacteria are programs that do not explicitly darnage any files. Their sole purpose is to reproduce. Typical bacteria programs are designed to do nothing more than reproduce themselves exponentially; consume all the processor capacity, memory or disk space; and eventually deny the user access to resources. This kind of programming attack (i.e., denial of service) is one of the oldest forms of programmed threat.

Recently in southern Finland, all trains were halted for approximately an hour because a paper clip fell into the keyboard of the railroad systems backup traffic control computer. The clip shorted-out some keyboard functions, causing the computer to continually submit system requests. The systems ran out of disk space and failed; subsequently, the main computer shut-down all trains. Such an incident constitutes denial of service due to an accidental threat of resource consumption.

D.2 DISCLOSURE

Disclosure is the acquisition of sensitive (e.g., personal, financial) information through unauthorized channels such as users, processes, or other systems. Disclosure threats consist of intentional or accidental events. Disclosure impacts the confidentiality of information and subsequently impacts privacy -- a fundamental personal or organizational expectation.

As the cost of data storage plummets, information technology trends will make it possible to inexpensively and efficiently assemble an individual data profile of extraordinary detail by cross-referencing multiple databases. Some applications of these profiles may initially appear to be benign. Farrell's Ice Cream Parlor sold the names of those claiming free

sundaes on their birthdays. The list was purchased by a marketing firm which in turn sold them to the Selective Service System, and some of the ice-cream eaters soon found draft registration warnings in their mail. More distressing, between 1989 to 1992, forty-five Los Angeles police officers were cited for using department computers to run background checks for personal reasons [Dam, Appendix J, 1996]. Given the likely predominance of data collection, these examples may be trivial to what lies ahead. Data collection will grow in at least five areas: medical history, government records, personal movements, transactions, and reading and viewing habits. Between them, these five areas cover most of modem life and represent a significant potential for disclosure.

D.3 MANIPULATION

Manipulation involves the modification of system information whether being processed, stored, or transmitted. It can include the removal or replacement of information or the resequencing of data to produce unauthorized effects. Manipulation threats consist of intentional, accidental, or natural events that jeopardize the integrity of a system.

In the 1996 FBI computer crime survey, the most frequent form of attack reported against medical and financial institutions was manipulation. Somewhat recently, insiders at the First National Bank of Chicago manipulated their own systems files and transferred approximately $70 million in bogus transactions out of client accounts [Dam, Appendix J, 1996].

D.4 MASQUERADING

Masquerading is the attempt by an unauthorized user or process to gain access to a system by posing as an authorized entity. If successful, the unauthorized entity could then obtain access to other information and processes that would normally be unobtainable. Masquerading threats consist of intentional or accidental events.

Forty-two percent (42%) of respondents to the 1996 FBI survey experienced some form of intrusion or other unauthorized use of computer systems within the year [CSI, 1996]. Electronic money transfers are among the most closely guarded activities in banking, yet in 1994, an international group of criminals penetrated Citicorp's computerized electronic transfer system using customers' user identifications and passwords to impersonate legitimate customers. The criminals moved about $12 million from legitimate customer accounts to their own accounts in banks around the world [Dam, Appendix I, 1996]. In 1987, a Dutch bank employee made two bogus electronic transfers to a Swiss account for over $15 million. Each transfer required the password of two different people for authorization; however, the employee knew someone else's password as well as his own [Dam, Appendix J, 1996]. In both of the previous instances, the impostors were able to easily disguise their identity (i.e., masquerade).

D.5 REPLAY

Replay is the re-transmission of valid messages under invalid circumstances to produce unauthorized effects. Depending upon the messages or actions reproduced, replay can have a severe impact on the integrity of a system. Replay threats consist of intentional or accidental events.

Every day the cellular phone industry loses between one and two million dollars as a result of "cloning" fraud. As described later in Appendix E, Information Security Mechanisms, this fraud occurs by first capturing specific unprotected user information from the airways.

Once obtained, the thieves can then reprogram a cellular phone (i.e., the clone) and successfully complete calls by replaying this information. The charges for these calls are then billed to the legitimate user's account.

D.6 REPUDIATION

Repudiation is the successful denial of an action. Repudiation allows either the sender or receiver to deny the action occurred. This typically affects the integrity of the system and applies to all types of electronic transactions. Repudiation threats consist of intentional or accidental events.

An example of a repudiation might involve a consumer denying that he or she made a credit card purchase via the telephone. This type of threat can occur whether or not the consumer was the legitimate card owner or someone who was using a stolen card. In either case, the credit card company absorbs any amount over the first $50 of the transaction. However, credit card issuers have recently made the statement that any service provider/bureau (e.g., travel agency) that does not adequately protect credit card numbers (authorized to be in their possession) will be held liable for any costs incurred due to the service provider's negligence. If credit card numbers were stolen from a service provider's database and charges were incurred on any of the accounts, the service provider -- not the issuing credit card company -- will be held accountable.

APPENDIX E

INFORMATION SECURITY MECHANISMS

This appendix describes a subset of available and applicable mechanisms (also referred to as techniques) and associated standards for implementing various security services (associations are illustrated in table E-l). These security mechanisms are the software, hardware, and/or procedures needed to enforce a particular security service. Each security service can be implemented by various mechanisms, and some security mechanisms can enforce more than one security service. Keep in mind that the correct implementation or selection of mechanisms depends on specific system design and related environmental variables.

The information presented in this appendix will help the reader understand which security mechanisms can be used to implement a particular security service and how those mechanisms function. The next four subsections (E. 1 - E.4) describe security mechanisms that support all the security services identified in the ITS Data Blow Security Assessment (see appendix B) and some of the services identified in the ITS Subsystem Security Assessment (see section 4). These services include confidentiality, authentication, integrity, and non-repudiation. The remaining subsections (E.5 - E.8) identify mechanisms that provide for the remainder of the security services applicable to ITS Subsystem Security Assessment (i.e., access control, accountability, availability, and systems security management).

CONFIDENTIALITY	
Security Mechanism	**Standard**
Encryption:	
Symmetric Key Cryptography	FIPS PUB *46-* 1, *Data Encryption Standard (DES),* Federal Information Processing Standards Publication 46- 1, 1988 FIPS PUB *74, Guidelines for Implementing and Using the NBS Data Encryption Standard,* Federal Information Processing Standards Publication 74, 198 1 ANSI *X3.92: American National Standard, Data Encryption Algorithm (DEA),* 1981
Public-Key Cryptography	RSA Laboratories' Public-Key Cryptography Standards (PKCS) - *(de,facto* standards)
Spread Spectrum	IEEE-802.1 1, Wireless Local Area Network (WLAN) TIA/EIA/IS-95-A, Mobile Station - Base Station Compatibility Standard for Dual-Mode Wideband Spread Spectrum Cellular System.
Shared Secret Data (wireless)	TIA Interim Standard-41C, "Cellular Radiotelecommunications Intersystem Operations."
Token-Based Authentication (wireless)	GSM Specification Series 3 .O l-3.88, "GSM PLMN Functions, Architectures, Numbering and Addressing, Procedures." Tl/P1/94-089, "PCS-2000, A Composite CDMA/TDMA Air Interface Compatibility Standard for Personal Communications in 1.8-2.2 GHz for Licensed and Unlicensed Applications," Committee Tl Approved Trial User Standard, T 1 -LB-459, November, 1994
Public-Key Authentication (wireless)	TBD (under development)

* Previously addressed in table

Table E-1: Security Services, Mechanisms, and Standards

AUTHENTICATION	
Security Mechanism	**Standard**
Passwords	FIPS PUB 112 - *Password* Usage, Federal Information Processing Standards Publication 112, 1985 ANSI *X9.26: American National Standard for Wholesale Financial Systems - Financial Institution Sign-On Authentication,* 1990
Personal Identification Numbers (PINS)	ISO *9564: Banking - Personal Identification Number Management and Security*
Tokens:	
One-time Passwords	RFC 1938, A One-Time Password System
Challenge-Response Schemes	TBD
Diskettes	TBD
Smart Cards	ISO/IEC 7816: *Identification Cards - Integrated Circuit(s) Cards with Contacts* ISO/IEC 10536: ISO *9992: Banking and Related Financial Services – Messages Exchanged with Integrated Circuit Cards* ISO 10202 *Financial Transaction Cards – Security Architecture of banking Systems Using Integrated Circuit Cards* (Draft)
PCMCIA Cards (i.e., PC cards)	PCMCIA *(de facto* standard)
Biometrics	No standard
Nonces:	
Sequence Numbers	TBD
Time-Stamps	TBD
Random Values	TBD

* Previously addressed in table

Table E-1 (cont'd): Security Services, Mechanisms, and Standards

AUTHENTICATION (cont'd)	
Security Mechanism	**Standard**
Seals	ISO/IEC *9797: Injormation Technology - Security Techniques - Data Integrity Mechanism Using a Cryptographic Check Function Employing a Block Cipher Algorithm* ISO 8730: *Banking - Requirements for Message Authentication (Wholesale)* ISO *873* l-l: *Banking-Approved Algorithms for Message Authent – Part I: Data Encryption Algorithm (DEA)* *ISO 873* l-2: *Banking-Approved Algorithms for Message Authent-Part 2: Message Authenticator Algorithm* ANSI X9.9: *American National Standard, Financial Institution Message Authentication (Wholesale),* 1986 *ISO 9807: Bunking und Related Financial Services – Requirements for Message Authentication (Retail)* ANSI *X9.19: American National Standard, Financial Institution Retail Message Authentication, 1986* FIPS PUB 113: U.S. Department of Commerce, *Computer Data Authentication,* 1985
Digital Signatures	ISO/IEC 9594-8: Information Technology – Open Systems Interconnection – The Directory – Authentication Framework (ITU-T Recommendation X.509) FIPS PUB 186 Digital Signature Standard (DSS), May 1994 ANSI X9.30: Public Key Cryptography using Irreversible Algorithms for the Financial Services Industry ANSl X9.3 1- 1: Public Key Crypt. using Reversible Algo. for the Financial Industry (RSA *de facto* standard) Hash Functions: FIPS PUB 180: U.S. Department of Commerce, Secure Hash Algorithm (SHA), Federal Information Processing Standards Publication 180, 1993 ISO/IEC 10118: Information Technology - Security techniques - Hash Functions for Digital Signatures ANSI X9.3 l-2: Public Key Cryptography using Reversible Algorithms for the Financial Industry (MDC2) The MD2 Message-Digest Algorithm, Request for Comments (RFC) 13 19 The MD4 Message-Digest Algorithm, Request for Comments (RFC) 1320 The MD5 Message-Digest Algorithm, Request for Comments (RFC) 132 1
MIN/ESN Authentication	TIA Interim Standard-4 1 C, "Cellular Radiotelecommunications Intersystem Operations."
Shared Secret Data (wireless)	*
Token-Based Authentication (wireless)	*
Public-Key Authentication (wireless)	*

* Previously addressed in table

Table E-l (cont'd): Security Services, Mechanisms, and Standards

Security Mechanism	Standard
INTEGRITY	
Error Detection	IEEE-802.10 LAN/MAN Security (SILS) CRC-CCITT (International Consultative Committee on Telegraphy and Telephony)
Seals	*
Digital Signatures	
NON-REPUDIATION	
Digital Signatures	*
ACCESS CONTROL	
Access Control Lists	No standard. Typically implemented by the receiving and/or sending subsystem at the application layer.
ACCOUNTABILITY	
Audit	No standard. Typically implemented by the receiving and/or sending subsystem at the application layer.
AVAILABILITY	
Redundant Systems, Transmission Medium, or Data	No standard. Typically implemented through various procedural and operational security procedures.
SYSTEM SECURITY MANAGEMENT	
	No standard. Typically implemented through various procedural and operational security procedures

* Previously addressed in table

Table E-1 (concluded): Security Services, Mechanisms, and Standards

E.l CONFIDENTIALITY SECURITY MECHANISMS

Given the highly visible concern for confidentiality within ITS, information such as traveler identity and any associated personal information and/or location data will require protection. So too will the many potential instances of financial-related transactions. The following mechanisms can help provide for the confidentiality of such ITS information. The first subsection describes encryption techniques and the remaining four subsections describe confidentiality techniques specific to wireless transmissions.

E.l.l Encryption

Encryption is the primary technique used to protect data from disclosure and subsequently provide data confidentiality. Based on the science of cryptography -- derived from the Greek word kryptos, meaning "hidden" -- encryption is the procedure of hiding data. A rigorous mathematical transformation is performed on the original or clear text data using a code (i.e., a key) such that the original data cannot be recovered without knowing that code. Depending upon the specific technique, encryption can also be used to provide data authentication, integrity, and non-repudiation. Given that cryptographic-based technology is used to support multiple security services, a brief overview of the subject is provided.

There are two basic types of cryptographic systems: symmetric (also called secret key) and public-key (also called asymmetric key). Symmetric cryptography uses the same key to encrypt and decrypt messages (see Figure E- 1, Symmetric Cryptography). The key must be transmitted securely out-of-band (i.e., not with the original data) to all systems with which transmissions will be conducted. Symmetric key provides a fast method for encrypting messages, yet the management and distribution of the keys require significant overhead. FIPS PUB 46 1, Data Encryption Standard (DES), is the most popular standard used for unclassified but sensitive data transmissions requiring confidentiality. NIST has initiated efforts to replace this standard with one that offers a higher level of security. In 1998 -- the next scheduled review of this standard -- the specified algorithm (i.e., the Data Encryption Algorithm) will be over twenty years old.

Public-key cryptography uses two separate yet related keys for encryption and decryption. The generation of the key pair is such that it is extremely difficult to obtain one key from the other. The use of two keys minimizes problems associated with symmetric key distribution; however, management of the public keys is required. The private key is closely-held by the sender and the public key is made available to other users with whom the sender would like to communicate.

Often in public-key cryptosystems two key pairs are generated: one for encryption and another for digital signatures. A description of the second pair for digital signature application may be found in Section E.2, Authentication. Note that public-key cryptography can provide the four primary security services identified in Section 3.

One implementation using public-key encryption techniques entails the sender encrypting a message with the receiver's public key. Then, the receiver decrypts the message with the receiver's private key. The success of this technique depends upon restricting access to the receiver's private key to only the receiver simply because only the receiver's private key will decrypt the message. Given that symmetric key encryption executes much faster than public-key, it is often used for encryption in a public-key based system. However, this presents the problem of securely transmitting the secret key which is required for decryption. The solution involves the sender

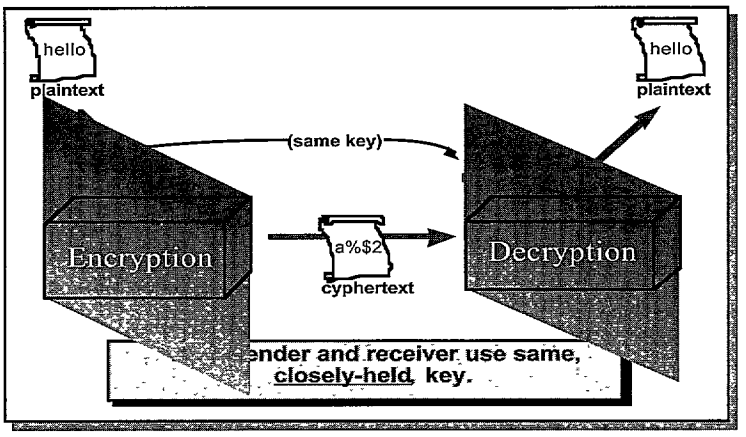


Figure E-1, Symmetric Cryptography

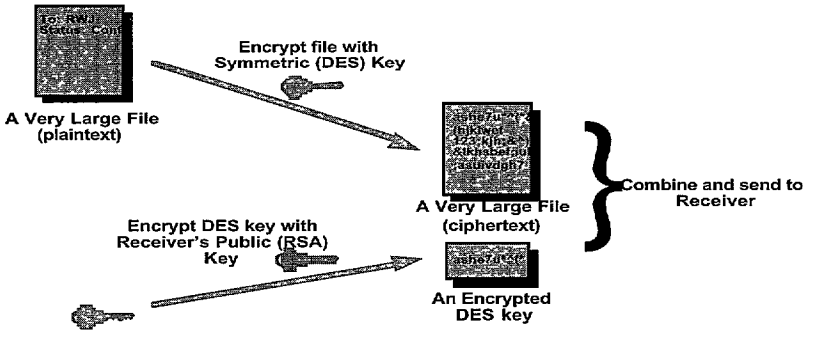


Figure E-2, Public-Key Cryptography

encrypting the symmetric key using the receiver's public key. Both the encrypted message and encrypted symmetric key are transmitted to the receiver (see Figure E-2, Public-Key Cryptography). The receiver then decrypts the encrypted symmetric key using the receiver private key. This process produces the symmetric key which is then used to decrypt the message. The majority of the encryption process is transparent to the user. Currently, the RSA cryptosystem, named after the three inventors, Rivest, Shamir, and Aldeman, is the de facto standard.

E.l.2 Spread Spectrum

Spread spectrum is another mechanism for providing data confidentiality -- particularly for wireless transmissions. Spread spectrum is a type of digital signal processing scheme in which the transmitted signal is spread across a much greater bandwidth than required to transmit the information. This type of communication makes intercepting transmissions very difficult and allows multiple users to simultaneously use a significant bandwidth.

Most modern spread spectrum systems use a stored-reference approach, whereby a spreading code is independently stored at the both the transmitter and receiver (older systems transmitted both the spreading code and the data signal, but this was very inefficient and allowed the spreading code to be easily intercepted). The primary advantage of the stored-reference approach is that a well designed spreading code cannot be predicted by monitoring the transmission. However, since this approach requires that same code be generated independently at more than one site, the code sequence cannot be truly random. It must be deterministic, even though it should appear random to unauthorized listeners. Such random-appearing deterministic signals are called pseudonoise (PN) or pseudorandom signals. How does the pseudorandom signal differ from a random one? A random signal cannot be predicted; its future variations can only be described in a statistical sense. However, a pseudorandom signal is not random at all; it is a deterministic and periodic signal that appears to have the statistical properties of sampled white noise. It appears to the listener to be truly random.

Direct sequencing (DS) and frequency hopping (FH) are the most commonly used methods for spread spectrum. Direct sequence (DS) is a method whereby a carrier signal is first modulated with a data signal, then the data-modulated signal is again modulated with a high speed (wide-band) pseudorandom spreading code signal. In the frequency hopping (FH) method, a data-modulated signal is frequency shifted over an extremely wide hopping bandwidth by a pseudorandomly controlled frequency synthesizer. Current technology permits frequency hopping bandwidths on the order of several Gigahertz, an order of magnitude larger than those allowed by direct sequencing. There are also hybrid combinations of these techniques (e.g., DS/FH, etc.); however, these are viewed as simple extensions of the individual methods.

E.1.3 Shared Secret Data (SSD)

With the increases in demand for cellular service and the frequency of cellular fraud came the development of more sophisticated cellular systems and security techniques. One of those techniques is an authentication scheme referred to as Shared Secret Data (SSD) . SSD not only provides a means for confidentiality but also a method to authenticate users. This technique may be used with systems employing time division multiple access (TDMA) and code division multiple access (CDMA) schemes as well as the Personal Access Communications System (PACS) and future versions of Advanced Mobile Phone System (AMPS). SSD uses symmetric-key cryptography to provide authentication and call privacy. All signaling, voice, and data are encrypted. A 64-bit "A-key" is entered in the mobile unit and the network database during service activation. In addition to the stored A-key, the telephone unit has an associated Electronic Serial Number (ESN) and 15-digit International Mobile Subscriber Identity (IMSI). The mobile unit and the network system, using the same algorithm, derive a secret key from this A-key. This secret key will be used for authenticating the mobile unit to the host system and to visitor hosts when roaming outside the service provider area. Typically, the system broadcasts a challenge, a random number which the mobile unit encrypts with the secret key. The mobile unit then transmits the encrypted random number back to the host. The system decrypts the transmission and

compares the random number against a list of possible random numbers to determine if the mobile unit is authorized. Visited systems will query the host system for the roaming mobile unit's secret key. The visited host then assigns the mobile unit a Temporary Mobile Subscriber Identity (TMSI) to allow for continued operation [Garg, 96].

E.1.4 Token-Based Authentication

Token-based authentication is somewhat of a misnomer in that confidentiality is supported in addition to the authentication service. Originally developed to provide authentication for wireless service providers, token-based authentication is based on encryption and subsequently serves as a useful technique for providing confidentiality. Like SSD, it provides encryption of signaling, voice, and data using a symmetric key cryptosystem. Under this technique, a removable smart-card interface referred to as a Subscriber Identity Module (SIM) provides mobile unit security. A symmetric key is stored in the home system and on the mobile unit's SIM. From this symmetric key, both the home system and the mobile unit derive a "triplet" of information (i.e., another key) that may be shared with visited systems. After verifying the triplet with that from the home system, the visited system can provide service to the mobile unit. This technique allows the mobile unit to authenticate itself to a visited system without revealing its symmetric key. Both Global System for Mobile Communications (GSM) and Omnipoint PCS-2000 support token-based authentication mechanisms [Garg, 96].

E.1.5 Public-Key Authentication

Like token-based authentication, public-key authentication was developed to provide authentication for wireless service providers. However, it is also a slight misnomer for the same reason as token-based authentication. As the name implies, this mechanism is based on public-key cryptography. The technique provides signaling, voice, and data encryption; however, system specifications are still under definition and development at this time. PACS, a low-powered system designed for slow moving mobile units, is the only system to currently implement this technique [Garg, 96]. The encryption functionality will be similar to that described in Section E. 1.1, Encryption.

E.2 AUTHENTICATION SECURITY MECHANISMS

The authentication security service supports the verification of an entity's identification prior to granting access to a system. As noted in earlier sections, authentication provides the foundation for other security services; thus, the importance of implementing an appropriate level of authentication. In the ITS environment there are numerous security mechanisms appropriate for implementing authentication. Many of these mechanisms are described below.

E.2.1 Passwords

Typically, a user identifies himself to a system by entering or submitting an assigned, unique userID. The system is then able to authenticate or verify the identity of the user by a password. The password, supposedly known only to the user, is compared to the one securely stored and associated with the userID. Passwords can offer a great deal of protection to a system if properly used. They must be easy to remember yet difficult to guess so as to properly safeguard from disclosure to unauthorized individuals. Additionally, passwords should have a limited life-time, minimum length, and periodic

change cycle to reduce the risk of being compromised. Since passwords are easily mis-managed, stronger authentication methods, as described in subsequent sections, have been developed.

E.2.2 Personal Identification Numbers (PINs)

Personal Identification Numbers (PINs) are used extensively in the banking and telecommunications industries. They authenticate users who identify themselves to the system with a company card (e.g., automatic teller machine (ATM) card) or with personal information -- perhaps information that could be inferred by others (e.g., an individual's phone number). PINs are traditionally determined by the service provider and cannot be easily changed by the user. However, banks and telecommunications companies are now allowing users to select their own PIN. PINs may be appropriate for particular ITS applications where users access Remote Traveler Subsystems (RTS) such as a kiosk or Personal Information Access Subsystems (PIAS) such as ones personal data assistant (PDA).

E.2.3 Mobile Identification Number (MIN)/Electronic Serial Number (ESN)

The Advanced Mobile Phone System (AMPS), the predominant U.S. analog cellular system standard, uses a Mobile Identification Number (MIN)/Electronic Serial Number (ESN) technique to provide authentication, The technique supports authentication of the cellular telephone unit itself, yet provides no confidentiality for the conversation or data transmission. The MIN and ESN are both unique to the cellular phone. The MIN, a 10 digit number, represents the phone number associated with the mobile unit. Tamper-proof modules are used for protecting the factory-coded ESN and render the unit inoperable if someone attempts to modify this number. When placing a call, the MIN and ESN are transmitted over the airlink to the cellular switching stations. A search of either one or both of the numbers against a list of "bad" MINs/ESNs will determine whether or not the system should connect the call. The Electronics Industry Association / Telecommunications Industry Association (EIA/TIA) Interim Standard (IS)-41 has provided an automated and updated searching process. Additionally, security of wireless calls is slightly enhanced if cellular service providers require users to enter a PIN with each call. As discussed in Section B.5, these numbers (including the PIN) are transmitted in the clear and may easily be stolen and used to clone cellular phones.

E.2.4 Tokens

Passwords and PINs can provide a stronger means of authentication when combined with other authentication techniques. Typically, the combination involves something the user knows (e.g., passwords, PINs) and something that the user possesses (e.g., tokens). Tokens are the software or hardware mechanism that provide the user with the second piece of authenticating information. Included within this group of mechanisms are one-time password generators, challenge-response schemes, diskettes, smart cards, and PCMCIA (Personal Computer Memory Card International Association) cards -- now commonly referred to as "PC cards". A brief description of each is provided below.

E.2.4.1 One-Time Passwords

As the name implies one-time passwords are similar to traditional passwords since they are used in conjunction with a userID, but they are limited to one-time use. The advantage of this technique is preventing the replay of a compromised password. Often, one-time passwords are used not only in conjunction with userIDs but also with passwords or

PINS. Commonly, a small hand-held device the size of a credit card (e.g., the SecureID card manufactured by Security Dynamics Technologies, Inc.) is synchronized with the target system's authentication scheme and displays a one-time password that periodically changes (e.g., every minute). To access the target system, the user enters an assigned userID and password or PIN followed by the one-time password currently displayed on the hand-held device. This method of authentication provides additional security since the user must possess knowledge of information (i.e., the userID and password) as well as the authentication token.

E.2.4.2 Challenge-Response Schemes

Mechanisms resembling one-time passwords are challenge-response schemes. These schemes use a similar synchronization device; however, additional user actions are required for authentication. When prompted by the target system, the user enters a userID and password, then enters a PIN into the hand-held device. After receiving the userID and password, the target authenticating system presents the user with a challenge (e.g., a number). The challenge is entered into the hand-held device by the user, and a response is calculated. This response is then entered into the target system by the user, and if the response is that expected by the target system, then the user is authenticated and granted access. Authorized users requesting remote access to ITS subsystems (e.g., to monitor roadway equipment) could use one-time password or challenge response-schemes for user authentication.

Both the one-time password and challenge-response schemes are cumbersome and allow for human error in data entry. As technology progresses, simpler, more user-friendly means for providing strong authentication are becoming available. One such method builds on the bar-code reader technology. Instead of entering a series of challenges and responses, a user can use a hand-held scanner to read and respond to challenges from the target system.

E.2.4.3 Tokens Requiring Cryptography

The following group of tokens (i.e., diskette, smart card, and PC card) require the use of cryptographic techniques. These tokens store information about the user and require a reader device. To support strong authentication, personal identifying information is stored on the token. To protect against theft, the user must enter a password or PIN before this information on the token can be accessed.

A standard 3.5" floppy *diskette* and associated disk drive can be used to store identifying information and support authentication as described above, but this is relatively restricted to personal computer applications. Authenticating *smart cards* (intelligent smart cards and memory smart cards) are approximately the size of a credit card and require a physical device for reading identifying information stored on the card. Intelligent smart cards include a microprocessor and have the capability to read, write, store, and process identifying information. Some may support additional encryption techniques. Memory smart cards typically store monetary value as an alternative to cash and are valid "payment instruments" as defined by the National ITS Architecture documents. Authentication PC *cards* are similar in size to smart cards yet are used with personal computers and require a special interface to the computer.

E.2.5 Biometrics

Other authentication mechanisms which provide a simpler, more user-friendly interface are referred to as biometrics. Biometric schemes utilize unique physical characteristics as the basis for authentication. Current biometric based mechanisms include fingerprint and retinal scanning, hand geometry, and voice pattern. A pattern is made of an user's biometric characteristic and stored within the system. To request access, the system scans the user characteristic and compares it with the stored pattern. If the patterns match, then system access is granted. This type of authentication mechanism provides a less cumbersome interface; one that may be preferred by emergency response personnel who are required to authenticate themselves to an ITS subsystem, yet do not have much time to do so.

E.2.6 Nonces

Nonces refer to non-repeating values that protect against the replaying of an entity's authenticating information. Included within this group of mechanisms are sequence numbers, time-stamps, and random values. All of these mechanisms entail some level of management or coordination between end-systems. One-time passwords and challenge-response schemes, while protecting against replay attacks, require the use of a token and remain within that category for the purposes of this paper.

E.2.6.1 Sequence Number

The sequence number mechanism is based on the end-systems using proper and previously agreed upon numbering schemes for particular transmissions. If a transmission contains the correct sequence number, (i.e., the one which the receiving system expects) then with some level of assurance, the receiver can presume that the sender is legitimate. This type of mechanism requires management of the sequence numbers which is commonly viewed as a disadvantage. Internal management is more controllable; hence, transmissions with "external" users such as commercial carriers and privately owned vehicles are most likely not good candidates for this type of authentication mechanism. One-way (i.e., broadcast) or DSRC transmissions from "internal" users (i.e., subsystems under the aegis of the same governing organization) are good candidates for sequence number authentication. For example, traffic signal control messages transmitted from an emergency vehicle to the roadside subsystem (i.e., the traffic signal) should provide source authentication prior to changing the signal. The transmission, for this example, would include an authentication code along with the control request.

E.2.6.2 Time-Stamp

Another authentication mechanism requiring some form of management is the time-stamp. Time-stamps require that the clocks of interfacing systems be synchronized and periodically monitored. Similar to the way sequence numbers function, time-stamps accompany a transmission and provide the receiving system with assurance of a legitimate source. Accordingly, candidates for time-stamp authentication include those using one-way or DSRC transmissions between "internal" subsystems.

E.2.6.3 Random Values

Random value mechanisms are most often a form of pseudorandom number generation. Like one-time passwords and challenge-response schemes, these mechanisms require an exchange of information or prior coordination between the end-systems. The sending

system includes with the data transmission a random value that the receiver can use to verify the authenticity of the source. Random value mechanisms can be applied to the same applications that would use sequence numbers or time-stamps; however, this technique does not require the same level of management. The distinction between using a random value mechanism and a spread spectrum technique is that in this case the random value is used to verify the authenticity of the sender, not to indicate the "pattern" of the coded transmission.

E.2.7 Seals

A seal (also referred to as a message authentication code (MAC)) provides dual security services: source authentication and data integrity. The financial community, the majority of whose transactions require such services, often use this mechanism. (Note: within the financial community, there is a trend toward digital signatures as a means for providing authentication and integrity -- See Section E.2.8). Based on symmetric-key cryptography, the sealing process involves the generation of a message authentication code or appendix. The appendix is a cryptographic (e.g., DES) representation of multiple elements. The multiple elements include the message itself and perhaps a time-stamp to ensure freshness and mitigate the risk of replay. The appendix is attached to the message prior to transmission. The receiving system, using the same symmetric key as the sender, computes a version of the appendix from the message received, then compares this appendix with the appendix sent in the transmission. If appendices match, then the receiver can assume with some level of assurance that the data has not been modified and originated with the alleged sender. As evident, sealing mechanisms do have an associated overhead for management of the symmetric keys. Figure E-3 illustrates the sealing mechanism process -- one that may be used for some ITS financial related transactions.

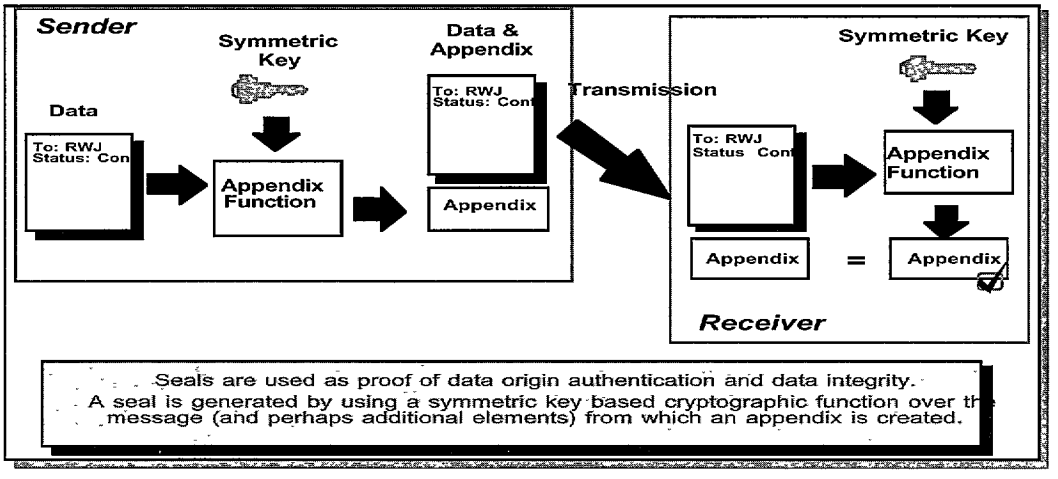


Figure E-3, Sealing Mechanism Process

E.2.8 Digital Signatures

A digital signature is the electronic equivalent of a hand-written signature and can be attached to various types of transactions. The primary purpose of a digital signature is to counter the threat of repudiation; however, a total of three security services are provided by this mechanism:

- Authentication – proof that the sender did in fact initiate a transaction
- Integrity – proof that the data was not modified
- Non-repudiation – proof such that the sender cannot later deny initiating a transaction
  Note: ITS data flows requiring some form of receipt or proof of transaction (e.g., payment requests) are typical candidates for digital signatures.

Digital signatures are generated in a way that provides all three security features. Therefore, the authors have elected to discuss how digital signatures support each of the noted security services here, as opposed to describing support for authentication, then integrity and non-repudiation in subsequent subsections. A reference back to this section is provided when digital signatures are mentioned as a mechanism to support integrity and non-repudiation.

Digital signatures are similar to seals; however, they are based on public-key cryptographic systems. Digital signatures may be generated in a manner as illustrated in Figure E-4. A message digest created by a hashing function represents a unique and irreversible depiction of the transmitted data. Typical algorithms for creating a digest include the Secure Hash Algorithm (SHA) and Message Digest 5 (MD-5). Once the digest has been created, the sender encrypts the digest with the sender's private key. Often referred to as "signing," this process produces a digital signature. The digital signature is then attached to the original data and transmitted to the receiver. Upon receiving the signed data, the receiver **decrypts** the message digest using the sender's public key. Using the same message digest algorithm as the sender, the receiver computes a version of the digest for bit-to-bit comparison. If the two digests are equivalent, then the receiver has proof that:

- the sender actually initiated the transaction (otherwise, the sender public key would not have decrypted the message digest);
- the message was not modified (otherwise, the two digests would not be equivalent);
- the sender cannot later deny sending the message (only the sender's private key could have been used to encrypt the message digest).

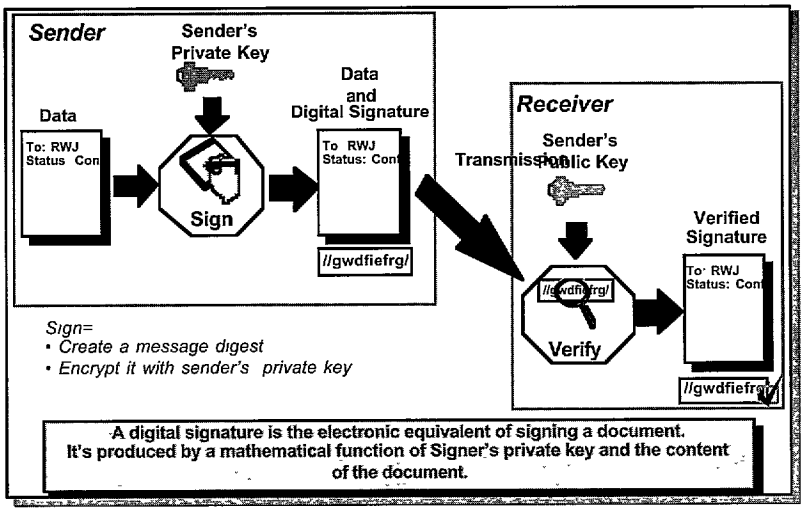


Figure E-4, Digital Signature Mechanism Process

E.2.9 SSD, Token-Based Authentication, and Public-Key Authentication

Shared secret data (SSD), token-based authentication, and public-key authentication were originally developed to provide authentication for wireless service providers. These mechanisms were also noted in previous sections for providing confidentiality. For a description of these mechanisms, refer to sections E.1.3 , E.1.4, and E.1.5 respectively.

E.3 INTEGRITY SECURITY MECHANISMS

The integrity security service supports the objective that data should not be altered during storage, transmission, and/or processing, unless the modification is specifically intended. Several mechanisms including error detection, seals, and digital signatures, protect against unintended data modification.

E.3.1 Error Detection

Error detection mechanisms include several methods for detecting errors in data transmission. Methods include, but are not limited to block codes, cyclic codes, convolutional codes, interleaving and concatenated codes, and digests generated from hash functions. Since these procedures are similar in functionality, for the purposes of this document, they have been grouped under error detection mechanisms.

In general, error detection mechanisms operate by performing a specified algorithm on the message data. The product of this operation is a value that is incorporated with the message. Upon receipt of the message, the receiving system performs the same operation, and if the calculated value is the same as that incorporated with the message, then the recipient can be assured that the message is identical to that transmitted by the sender. These procedures are the weakest of the available integrity techniques since the message

could be modified, the code recalculated, and the new code appended to the message. However, in a low threat environment these methods can provide a valued service.

E.3.2 Seals and Digital Signatures

Seals and digital signatures will provide a stronger level of data integrity than error detection mechanisms. If an authorized user wanted to modify the message and recalculate the integrity code, then they must have access to either the sender's private key or the symmetric key. For a description of seals and digital signatures, refer to sections E.2.7 and E.2.8 respectively.

E.4 NON-REPUDIATION SECURITY MECHANISMS

The primary purpose of non-repudiation is to prevent a sender from later denying having sent a transmission (i.e., non-repudiation of origin). A secondary purpose involves the receiver not being able to deny having received a transmission (i.e., non-repudiation of delivery). Typically, digital signature mechanisms cover both cases of non-repudiation. Section E.2.8 provides a description of how digital signatures are obtained, validated, and used to support non-repudiation of origin. Non-repudiation of delivery is supported by applying the same technique to a return message.

E.5 ACCESS CONTROL SECURITY MECHANISMS

After the authentication service has been performed and has properly validated a user or process, the access control security service restricts access to a system and its resources. The traditional mechanism for implementing access control is an access control list (ACL). ACLs are typically associated with a particular resource (e.g., files, databases, processes, etc.) and specify permissions that pre-defined users or processes may perform on these resources. ACLs are implemented in the application software and therefore not truly applicable at the data flow level. However, ACLs could be incorporated to provide access control on message creation as well as outgoing and incoming messages.

E.6 ACCOUNTABILITY SECURITY MECHANISMS

Accountability is the means of tracing system activities to a particular entity. Logging or audit trails are typical mechanisms used to support the accountability service. These mechanisms support a more passive role toward system security than most security mechanisms described above. Auditing is a detection rather than protection mechanism. Audit trails can be used to detect patterns of operation or abuse. Unfortunately, mechanisms for implementing accountability produce vast quantities of information. Fortunately, tools are available for managing audit information and for selectively controlling auditable events. Though not truly applicable at the data flow level, auditing of the processes that send and receive messages will help provide thorough system security.

E.7 AVAILABILITY SECURITY MECHANISMS

The availability service ensures that system resources are accessible and useable when required by authorized users and processes. Typically, physical and/or procedural control mechanisms provide the primary support for system availability. Examples include redundant systems, redundant transmission media, and redundant data. Systems enforcing strong authentication and access control minimize the chances of an unauthorized user modifying files and potentially denying valid users access to a needed service. While

availability mechanisms are implemented by various means, some provision is required to ensure the availability of processes controlling ITS messaging.

E.8 SYSTEM SECURITY MANAGEMENT SECURITY MECHANISMS

Security management is the means of providing adequate security controls throughout the system life-cycle, This includes the definition, implementation, and enforcement of security policies and procedures, roles and responsibilities, system configuration, operational security, personnel security, and physical security. These components should be well defined and reviewed periodically to ensure that they reflect the current security needs of the system. Effective system security management techniques consider all components and provide indirect support to other currently implemented security mechanisms. Specific to the ITS data flows, this includes those security mechanisms targeted towards message authentication, confidentiality, integrity, and non-repudiation.

It is system configuration that provides the means of ensuring all aspects of the system are configured to provide an effective, efficient, and secure operating environment. One aspect of system configuration involves the interfaces with other systems. The parameters which facilitate system interfaces on a network must be kept current and controlled. Interfaces should be established to minimize system exposure and subsequently reduce the risks for any associated systems. Another aspect of system configuration involves the integrity of the operating system. Keeping the operating system up to date with current releases and system patches is necessary to prevent exposure to changing vulnerabilities. It is also important to ensure proper configuration of system applications.

Other security mechanisms can function properly as long as the supporting software and hardware are working correctly. Erroneous or incomplete system configuration can lead to unauthorized users obtaining privileged access to system utilities and applications. Though not directly applicable to individual data flows, mechanisms providing adequate system configuration can protect the processes and functions that control ITS data flows.

APPENDIX F

IMPLEMENTING INFORMATION SECURITY SERVICES

Each of the following examples illustrates the process of identifying specific security services for ITS data flows. Additionally, the examples illustrate the implementation of these services (i.e., selecting an appropriate security mechanism to enforce the required security service).

The ITS data flows were assessed as described in Appendix A. 1, Approach and Methodology. The content of the physical data flow between associated source and destination end-systems was reviewed. Additionally, the content of all constituent logical data flows and their source and destination process(es) was analyzed. Considering the overall content and intended function of the specific data flow, the potential threats were identified, and the appropriate security services were recommended. Furthermore, based on the assessed services and a hypothetical yet appropriate communications system (part of the system design), appropriate security mechanism(s) were identified.

F.l WIRELINE

The "incident notification" wireline physical data flow passes notification of an incident on the roadway from the Traffic Management Subsystem (TMS) to the Emergency Management Subsystem (EM) (See Figure F-l). To support this wireline physical data flow requirement, the authors assume that the implementing entity will utilize a frame relay connection from a public service provider.

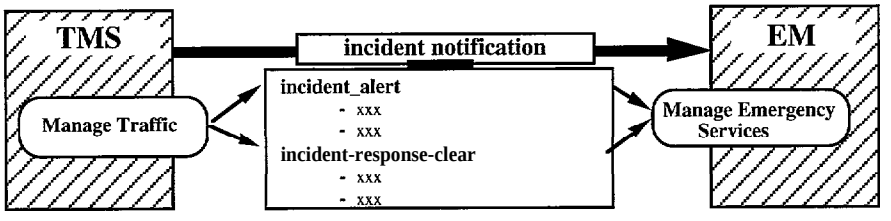


Figure F-l, Wireline Data Flow Requirement

This physical data flow may comprise both the "incident alert" and "incident response clear" first level logical data flows. The "incident alert" logical data flow is used to send details of an incident from the "Manage Traffic" function to the "Manage Emergency Services" function and contains information on incident location, start-time, duration, severity, type, etc. "Incident response clear" is sent from the "Manage Traffic" function to the "Manage Emergency Services" function and shows that the TMS has data indicating an incident has been cleared. This logical data flow contains information on both incident location and incident type.

Mitretek's complete review (physical and logical data flows, process specifications, communications system, intended functions, special constraints, etc.) indicates this data flow requirement is vulnerable to masquerading, manipulation, and denial of service. Although theoretically the message is also susceptible to disclosure, it contains no information considered to be personally or organizationally confidential. For this particular

requirement, the authentication and integrity services are required to ensure authorized source identification and accurate message content in an emergency related transaction.

Having identified the required security services, one may now select appropriate security mechanisms to implement these services. Since this requirement has the need for both authentication and integrity, a seal (i.e., message authentication code (MAC)) would be a likely candidate to implement the required services (see table E-l). As discussed in Section E.2.7. seals are based on symmetric key cryptographic systems and used primarily in the financial industry where there is now a trend toward public-key cryptographic systems. The management of keys within a public-key system is presumed to require less overhead than that for symmetric based systems, hence the trend toward this technique. Therefore, digital signatures, a public-key based cryptographic system, offer an alternative to seals. Digital signatures provide integrity and authentication as well as non-repudiation services, and they are offered with many new security products -- some are specifically designed to implement such services for frame relay networks.

F.2 TWO-WAY SHORT-RANGE WIRELESS

As described by the National ITS Architecture, an Emergency Vehicle Subsystem (EVS) will transmit an "emergency vehicle preemption request" physical data flow to a Roadway Subsystem (RS) (See Figure F-2). For the purposes of this example, the authors will assume the use of a DSRC system to provide for this requirement. The authors will also assume an existing communications capability (i.e., a National Transportation Communications for ITS Protocol (NTCIP)) to monitor and control Roadway Subsystem processes from a remote location (e.g., a TMS).

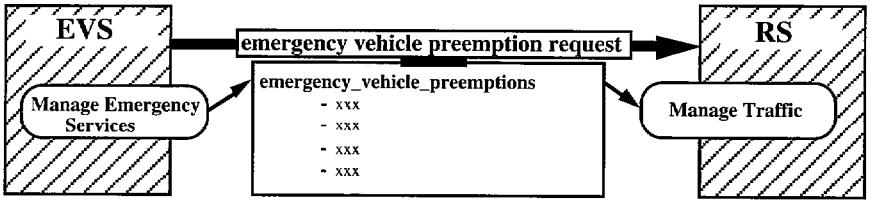


Figure F-2, Two-Way Short-Range Wireless Data Flow Requirement

The noted physical data flow consists of an "emergency vehicle preemptions" logical data flow from the "Manage Emergency Services" function to the "Manage Traffic" function. This logical data flow contains the data necessary for an individual emergency services vehicle to be given preemption (i.e., priority) by an indicator controller at a particular junction (e.g., roadway intersection), pedestrian crossing, ramp, or sign. The data is sent directly from the emergency vehicle to the next controller along its route and therefore is not subject to any centralized coordination.

After completely reviewing this data flow, masquerading and replay appear to present the primary threats. To prevent replay by unauthorized users, the preemption message transmitted from the emergency vehicle to the indicator control should provide source authentication. Therefore, for this particular requirement, the authentication security service is required.

As indicated by Table E- 1, there are several mechanisms to implement the authentication security service. However, because internal management of security mechanisms is more controllable, DSRC transmissions from "internal" users (i.e., subsystems under the

protection of the same governing organization) are good candidates for sequence number authentication (See E.2.6.1). As a requirement intended to facilitate the headway of an emergency vehicle, the authors safely assume that time is an important constraint. Therefore, with only a sequential authentication code tagged to the preemption request, the transmission from emergency vehicle to indicator controller would include minimal delay. If there is significant concern for a greater level of authentication, then as technology progresses, simpler means for providing strong authentication such as token-based schemes (e.g., fast scan bar-code readers) can be used.

F.3 TWO-WAY WIDE-AREA WIRELESS

The "trip request" wide-area wireless physical data flow is a request for special routing from a Personal Information Access Subsystem (PIAS) (e.g., a personal portable device/computer) to an Information Service Provider (ISP) subsystem (See Figure F-3). The authors will assume that this data flow is transmitted over a CDPD wide-area wireless network, and that a frame relay wireline connection is used to provide CDPD service to the ISP.

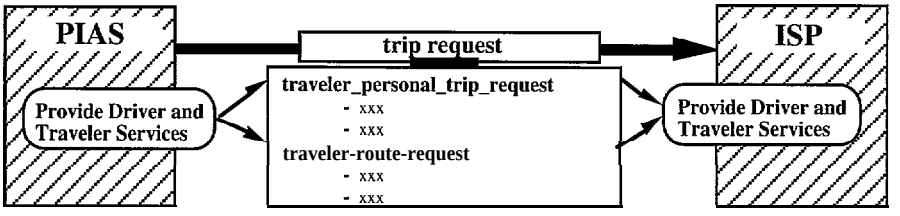


Figure F-3, Two-Way Wide-Area Wireless Data Flow Requirement

The "trip request" physical data flow contains the "traveler personal trip request" and "traveler route request" first level logical data flows. The "traveler personal trip request" logical data flow is used within the "Provide Driver and Traveler Services" functions and contains data about a traveler's trip request that has been entered from a personal portable device. One of several secondary logical data flows further identifies the parameters needed for an ISP to provide a trip or route. This data flow consists of information such as the traveler's origin, destination, departure time, desired arrival time, as well as personal preferences and constraints. The "traveler route request" logical data flow is used among the "Provide Driver and Traveler Services" functions and contains data from which the route requested by a traveler can be determined. This logical data flow may contain not only a traveler's identity, but also information regarding the traveler's intended origin, destination, and arrival time; preferred modes, routes, and transit options; acceptable travel times, and mode changes; and individual special needs.

Detailed review of the "trip request" physical data flow requirement reveals the significant amount of personal information exchanged. This data flow is particularly vulnerable to disclosure, and therefore requires the confidentiality security service. Along with confidentiality, this data flow also requires authentication to indicate that the message is a valid and legitimate request to the ISP.

Although the end-to-end physical data flow requirement is direct from PIAS to ISP, the communications link is divided into a wireless connection from PIAS to the cellular base station (i.e., the CDPD airlink) and a wireline connection from the base station to the ISP (i.e., the frame relay connection stated in the assumption above). From an understanding of the communications design, one would know that the CDPD airlink inherently supports

source authentication and data link confidentiality using secret-key encryption. Over the airlink, there would be no additional security services needed for this requirement. However, since the frame relay wireline connection provides no such inherent security, the end-to-end (i.e., PIAS to ISP) requirement would still need the authentication and confidentiality security services.

There are currently some new mechanisms (e.g., shared secret data (SSD)) for additional security over the "airlink" of other wide-area wireless communications networks. However, for a CDPD implementation, the necessary security service needs of the end-to-end requirement may be achieved by implementing authentication and confidentiality mechanisms. As noted earlier, some new products will provide for authentication and confidentiality over frame relay networks and subsequently satisfy these particular end-to-end security service needs.

GLOSSARY

Acronym

ACL	Access Control List
AMPS	Advanced Mobile Phone System
ANSI	American National Standards Institute
ASC	Accredited Standards Committee
ATM	Automatic Teller Machine
CDMA	Code-Division Multiple Access
CDPD	Cellular Digital Packet Data
CERT	Computer Emergency Response Team
CRC	Cyclic Redundancy Check
CSSPAB	Computer System Security and Privacy Board
CSI	Computer Security Institute
CTIA	Cellular Telecommunications Industry Association
CVAS	Commercial Vehicle Administration Subsystem
CVSC	Commercial Vehicle Check Subsystem
CVS	Commercial Vehicle Subsystem
CVO	Commercial Vehicle Operations
DEA	Data Encryption Algorithm
DES	Data Encryption Standard
DMV	Department of Motor Vehicle
DS	Direct Sequencing
DSRC	Dedicated Short-Range Communications
DSS	Digital Signature Standard
ED1	Electronic Data Interchange
EIA	Electronic Industry Association
EM	Emergency Management Subsystem
ESMR	Enhanced Specialized Mobile Radio
ESN	Electronic Serial Number
EVS	Emergency Vehicle Subsystem
FBI	Federal Bureau of Investigation
FH	Frequency Hopping
FHWA	Federal Highway Administration
FIPS	Federal Information Processing Standards
FM	Frequency Modulation
FMS	Freight and Fleet Management Subsystem
GHz	Giga Hertz
GSM	Global System for Mobile Communications

Acronym

IATF	Information Assurance Task Force
ID	Identification
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IITF	Information Infrastructure Task Force
IMSI	International Mobile Subscriber Identity
IS	Interim Standard
IS0	International Organization for Standardization
ISP	Information Service Provider
ISTEA	Intermodal Surface Transportation Efficiency Act
ITS	Intelligent Transportation System
ITU	International Telecommunication Union
LAN	Local Area Network
MAC	Message Authentication Code
MAN	Metropolitan Area Network
MD	Message Digest
MIN	Mobile Identification Number
NAB	National Association of Broadcasters
NACIC	National Countcrintclligcncc Ccntcr
NIST	National Institute of Standards of Technology
NRSC	National Radio Systems Committee
NSA	National Security Agency
NSTAC	National Security Telecommunications Advisory Committee
NSTC	National Science and Technology Council
NTCIP	National Transportation Communications for ITS Protocol
PACS	Personal Access Communications System
PC	Personal Computer
PCMCIA	Personal Computer Memory Card International Association
PCS	Personal Communications System
PDA	Personal Data Assistant
PIAS	Personal Information Access Subsystem
PIN	Personal Identification Number
PKCS	Public-Key Cryptography Standard
PLMN	Public Land Mobile Network
PMS	Parking Management Subsystem
PN	Pseudonoise
PSTN	Public Switched Telephone Network
PUB	Publication
RBDS	Radio Broadcast Data Standard
RFC	Request For Comment
RS	Roadway Subsystem
RSA	Rivest, Shamir, and Aldeman
RTS	Remote Traveler Subsystem

Acronym	
SHA	Secure Hash Algorithm
SILS	Standard for Interoperable LAN/MAN Security
SIM	Subscriber Identity Module
SPB	Security Policy Board
SSD	Shared Secret Data
TAS	Toll Administration Subsystem
TCS	Toll Collection Subsystem
TDMA	Time-Division Multiple Access
TIA	Telecommunications Industry Association
TMS	Traffic Management Subsystem
TMSI	Temporary Mobile Subscriber Identity
TRMS	Transit Management Subsystem
TRVS	Transit Vehicle Subsystem
USDOT	United States Department of Transportation
VMS	Variable Message Sign
VS	Vehicle Subsystem
WLAN	Wireless Local Area Network

Publication Number: FHWA-JPO-98-009
12/97(2.5M)EW