United States
Department of Justice

Applying Wireless Security Practices to Justice Information Sharing

BJA

This document was prepared under the leadership, guidance, and funding of the Bureau of Justice Assistance (BJA), Office of Justice Programs, U.S. Department of Justice, in collaboration with the U.S. Department of Justice's Global Justice Information Sharing Initiative. The opinions, findings, and conclusions or recommendations expressed in this document are those of the authors and do not necessarily represent the official position or policies of the U.S. Department of Justice.

April 2006

Table of Contents

Tables

Figures

Acknowledgements

Applying Wireless Security Practices to Justice Information Sharing was developed through a collaborative effort of the Security Working Group of the Global Justice Information Sharing Initiative (Global), Office of Justice Programs (OJP), U. S. Department of Justice (DOJ).

Global aids its member organizations and the people they serve through a series of important initiatives. These include the facilitation of Global Working Groups. The Global Security Working Group (GSWG) is one of four various Global Working Groups covering critical topics such as intelligence, privacy, and standards.

The GSWG focus is on the trusted and secure information exchange among justice agencies. Security of the entire information exchange enterprise is only as strong as the weakest link. The GSWG pursues security measures necessary for today's enhanced information sharing abilities.

This document is the product of Global and its membership of justice practitioners and industry professionals. Sincere appreciation and gratitude are extended to the Global Security Working Group and its members for volunteering their time to contribute to this project.

Mr. David Buchanan, retired—County of San Bernardino, San Bernardino, California

Mr. Jim Cabral—Integrated Justice Information Systems (IJIS) Institute, Seattle, Washington

Mr. David Clopton—U.S. Department of Justice, Washington, DC

Mr. Scott Fairholm—National Center for State Courts, Williamsburg, Virginia

Mr. Robert Hanson—Minnesota Supreme Court, St. Paul, Minnesota

Alan Harbitter, Ph.D.—IJIS Institute, Fairfax, Virginia

Mr. Joseph Hindman—Scottsdale Police Department, Scottsdale, Arizona

Mr. Tom Merkle—National Institute of Justice, Greenbelt, Maryland

Mr. Bill Phillips—Nlets–The International Justice and Public Safety Information Sharing Network, Phoenix, Arizona

Mr. John Powell—National Public Safety Telecommunications Council, Denver, Colorado

Ms. Christina Rogers—Statewide Investigative Networking System, Division of Criminal Justice Information Services, California Department of Justice, Sacramento, California

Mr. John Ruegg—Information Systems Advisory Board, Los Angeles County Board of Supervisors, Cerritos, California

Mr. Todd Shipley—SEARCH, The National Consortium for Justice Information and Statistics, Sacramento, California

Mr. Chris Traver—Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice, Washington, DC

Mr. Andrew Thiessen—Institute for Telecommunication Sciences, National Telecommunications and Information Administration, Boulder, Colorado

Ms. Richelle Uecker—Orange County, Superior Court of California, Santa Ana, California

Global Justice Information Sharing Initiative (Global)

Global Mission and Guiding Principles

The Global mission is to improve the administration of justice and protect the nation's public by promoting practices and technologies for the secure sharing of justice-related information. The vision is to lead the way by getting the right information to the right people at the right time.

The guiding principles of Global are to:

- Bring together representatives from the entire justice, public safety, and first responder communities—including private industry—to overcome the barriers to justice information sharing across agencies, disciplines, and levels of government.
- Promote the development and implementation of standards that facilitate seamless exchange of information among justice, public safety, and first responder communities.
- Provide information that supports sound business decisions for the planning, design, and procurement of cost-effective, interoperable information systems.
- Promote constitutional values and individual rights by ensuring the accuracy and security of justice information and the implementation of appropriate privacy safeguards.
- Acknowledge that while there is a strong national consensus that improved justice-related information sharing is critically important, there is a commensurate desire to protect individuals' privacy.
- Recommend concepts that leverage existing infrastructure, capabilities, and functionality.

The broad scope of the effort is fundamental, because public and practitioner safety is best secured when all players—from patrol officers to prosecutors and from court officials to corrections personnel—have access to timely and accurate information.

Global operates in accordance with Federal Advisory Committee Act (FACA) provisions and convenes twice a year in Washington, DC. Meetings are announced in the *Federal Register,* and the public are welcome as observers.

Global Structure: Membership and Leadership

The Global Advisory Committee (GAC) comprises key personnel from local, state, tribal, federal, and international justice and public safety entities, including agency executives and policymakers; automation planners and managers; information practitioners; and, most importantly, end users. This last group distinguishes the GAC as a committee whose members remain actively dedicated to information sharing, precisely because they continue to be producers, consumers, and administrators of crucial justice-related data.

Committee membership reflects the fundamental GAC tenet that the entire justice, public safety, and courts community must be involved in information exchange. Representatives from the following entities serve as members:

- Administrative Office of the U.S. Courts
- American Association of Motor Vehicle Administrators
- American Correctional Association
- American Probation and Parole Association
- Conference of State Court Administrators
- Criminal Justice Information Services Advisory Policy Board
- Executive Office for United States Attorneys
- Federal Bureau of Investigation—Criminal Justice Information Services Division
- International Association of Chiefs of Police
- International Association of Chiefs of Police—Division of State and Provincial Police
- International Association of Chiefs of Police—Indian Country Law Enforcement Section
- INTERPOL–USNCB
- Major Cities Chiefs Association
- Nlets—The International Justice and Public Safety Information Sharing Network
- National Association for Court Management
- National Association of Attorneys General
- National Association of State Chief Information Officers
- National Center for State Courts
- National Conference of State Legislatures
- National Congress of American Indians
- National Council of Juvenile and Family Court Judges
- National Criminal Justice Association
- National District Attorneys Association
- National Governors Association

- National Legal Aid & Defender Association
- National Sheriffs' Association
- SEARCH, The National Consortium for Justice Information and Statistics
- U.S. Department of Homeland Security
- U.S. Department of Justice—Justice Management Division
- U.S. Drug Enforcement Administration

GAC working groups comprise committee members and other subject-matter experts, expanding the GAC's knowledge and experience. These groups are formed around timely issues impacting justice information sharing and meet as often as necessary. The following working groups are engaged in targeted activities on behalf of the GAC:

- **Global Security Working Group**—The Global Security Working Group was formed in recognition that the security of the entire justice information exchange enterprise is only as strong as the weakest link. Of particular importance is the determination of effective security guidelines for legacy systems, as well as the new and enhanced networks and systems to which they are joined. The goal of this working group is to inform the justice and justice-related communities about acceptable integrated justice system security measures, encouraging them to adopt security guidelines that have been reviewed to ensure trusted partnerships and data integrity.

- **Global Privacy and Information Quality Working Group**—The Global Privacy and Information Quality Working Group was formed because of the growing need to address information privacy as impacted by advancing technological capabilities. Goals of this working group include assisting governments in ensuring that personal information will not be inappropriately disseminated or misused, ensuring that there are safeguards against the collection and use of inaccurate information—particularly when the information is disseminated in open environments such as Internet-based systems, and improving the reliability of criminal records in an integrated electronic system.

- **Global Intelligence Working Group**—The Global Intelligence Working Group was formed to examine and integrate into the GAC dialogue the particular challenges to intelligence sharing. This working group has developed a *National Criminal Intelligence Sharing Plan (Plan or NCISP)*—a formal intelligence sharing initiative that will securely link local, state, tribal, and federal law enforcement agencies, facilitating the exchange of critical intelligence information. This Plan contains model policies and standards and describes a nationwide network that will link all levels of law enforcement personnel, including officers on the street, intelligence analysts, unit commanders, and police executives. In October 2003, former U.S. Attorney General John Ashcroft approved the Plan.

- **Global Infrastructure/Standards Working Group**—The Global Infrastructure/Standards Working Group was formed because successful broadscale data exchange is greatly facilitated by (if not dependent on) the

development and adoption of standards that enable transparent integration of disparate systems. The goal of this working group is to define a Justice Reference Architecture that will assist government entities in establishing an operational environment that will enable them to share justice information within the guiding principles of the GAC. The framework will be designed to identify those critical components, programmatic and technical, necessary to develop and maintain a sound infrastructure.

Global Web Site—www.it.ojp.gov

The Web site provides information about Global and other important information technology initiatives. The Web site is in response to the need for additional information sharing resources throughout justice and public safety communities. This valuable online tool offers resources that support information sharing at all levels of government.

How to Use This Document

This wireless document is a companion resource to *Applying Security Practices to Justice Information Sharing* (document) or (Applying Security Practices). In most cases, the reference material in the Applying Security Practices document is relevant to the wireless perspective.

This wireless document contains expanded information containing wireless overviews and wireless guidelines for secure information sharing. Additional content specifically relevant to wireless environments has been used to expand upon the information that was previously written for security disciplines that span the important elements of an information security architecture. Only issues unique to wireless deployments have been addressed.

This document is not intended to suggest a standard security approach nor is it intended to provide an in-depth security solution for any particular system. It is also not intended to provide a detailed technical reference for system administrators.

Many of these suggested practices are low cost in that they require users to be educated about security practices and suggest awareness and evaluation of the security threat. Other practices require capital investment and continued maintenance to ensure their effectiveness. However, doing nothing can have unacceptable associated costs.

Recognizing the trend of law enforcement to utilize commercially available wireless hardware, networks, and services, the GSWG will continue to identify security policies required to safeguard information in those environments. The policies encompass (but are not limited to) areas such as access control, audit and accountability, certification, accreditation, security assessments, identification, authentication, physical and environmental protection, system and communications protection, and system and information integrity.

Current standard wireless technologies include (but are not limited to) IEEE 802.11 (Wi-Fi); IEEE 802.16 (WiMAX); IEEE 802.20 (Mobile Broadband Wireless Access); microwave, and satellite; IEEE 1451.5 (Wireless Sensor Standards); and third generation mobile standards, such as TIA CDMA2000 1x (1xRTT), 1xEV-DO (1x Evolution-Data Optimized), and 1xED-DV (Evolution-Data/Voice). Third generation mobile and wireless technologies are being researched for security and vulnerability.

Criminal Justice Information Services (CJIS)

The GSWG recommends that all justice and public safety wireless device users follow the currently proscribed policies in the *Criminal Justice Information Services (CJIS) Security Policy*.[1]

The *CJIS Security Policy* is considered to be Sensitive But Unclassified (SBU) material and can not be disclosed in this publication nor posted to a public Web site, and discretion shall be exercised in sharing the contents of the policy with individuals and entities who are not engaged in law enforcement or the administration of criminal justice.

All agencies required to adhere to the *CJIS Security Policy* should be aware that it contains specific requirements for wireless networking, including encryption, certification of cryptographic modules, and minimum key lengths. These agencies should become familiar with the requirements set by the CJIS policy prior to procurement and deployment of wireless devices.

A CJIS Systems Agency (CSA) has been designated to establish and administer an IT security program for the state's network systems that access NCIC and the CJIS systems. Agencies planning or operating such networks should coordinate their IT security plans with the CJIS Systems Officer (CSO) in the CSA. A list of CSOs is maintained on the Law Enforcement Online (LEO) Web page.

[1] Must be a Law Enforcement Online (LEO) member to acess the *CJIS Security Policy*.

Security Disciplines

Introduction

This document discusses the critical security disciplines for wireless security for each of the key objectives: Support, Prevention, and Detection and Recovery. Each security discipline is defined in Table 1—Information Security Disciplines.

Objective 1: Support

These services are generic and underlie most information technology capabilities.

- ❑ Governance
- ❑ Physical Security
- ❑ Personnel Security Screening
- ❑ Separation of Duties

Objective 2: Prevention

- ❑ Identification and Authentication
- ❑ Authorization and Access Control
- ❑ Data Integrity
- ❑ Public Access, Privacy, and Confidentiality
- ❑ Firewalls, VPNs, and Other Network Safeguards

Objective 3: Detection and Recovery

- ❑ Attack Detection and Prevention
- ❑ Security Auditing
- ❑ Risk Management
- ❑ Disaster Recovery and Business Continuity

Section Structure

In general, each security discipline section is constructed as follows:

- **Description and Purpose**—provides a summary of the discipline and the role it plays in securing information.
- **Principles**—identifies the qualities that should be in place in an organization that responsibly and securely manages justice information.
- **Policies**—contains guidance and, when applicable, references to sample policies in order to assist organizations in establishing good internal policies for securing information.
- **Best Practices**—includes tutorials and also overviews the best ways to apply the tools, technologies, and processes within each discipline.
- **References**—provides resources to assist justice organizations in designing their security practices in meeting well-established industry standards.

Table 1—Information Security Disciplines

Information Security Disciplines	Definition and Relevance
Governance	Identifies the practices applied to establish, manage, and enforce information security policy.
Physical Security	Protects against compromises in security that may arise from facility and environmental vulnerabilities.
Personnel Security Screening	Includes the processes applied to determine if personnel warrant the level of trust required to access sensitive justice information and systems.
Separation of Duties	Requires the segregation of administrative, development, security, and user functions to provide security checks and balances.
Identification and Authentication	Ensures those wishing to gain access to information resources are who they represent themselves to be. Typical methods include passwords, smart cards, and biometrics.
Authorization and Access Control	Determines what permissions and access authorization an information system user holds.
Data Integrity	Safeguards information content and protects against inadvertent or intentional information modification or loss.
Public Access, Privacy, and Confidentiality	Outlines tools and procedures to protect the privacy of individuals and information in light of the increased accessibility offered by networked information systems.
Firewalls, VPNs, and Other Network Safeguards	Identifies the tools employed to establish a barrier between private and public information in a justice organization.
Attack Detection and Prevention	Monitors computing and communications facilities for evidence of inappropriate access or use.
Security Auditing	Examines and verifies that organizational practices meet security policies and applicable regulations.
Risk Management	Protects critical information assets and its ability to perform the organizational mission.
Disaster Recovery and Business Continuity	Establishes and documents the procedures to follow in the event of a disaster so that operations that depend on the accuracy and availability of information can continue and be restored.

Objective 1: Support

Security Disciplines:

Objective 2: Prevention

Security Disciplines:

Objective 3: Detection and Recovery

Security Disciplines:

Security Disciplines for Objective 1: Support

1-1. Governance

Description

For individual organizations, governance is the source of security policy, establishing the activities required to assess risk, set direction, and monitor the application of security tools with the objective of creating a secure operating environment. In an environment in which information is shared, governance is more complex and must represent the security interests and policies of multiple organizations. This is particularly true in a wireless environment where the infrastructure (especially for broadband) must often be shared, to include nonjustice governmental entities and potentially nongovernmental organizations (such as utilities), and where the transmission medium is readily open to acquisition by nonusers. A shared, workable governance structure is critical to the successful implementation of any system that supports interoperability.[2]

Purpose

Security management encompasses a number of functions, as outlined in this document. Governance recognizes that these functions need oversight and control at a high level to assure that each is addressed appropriately. Only in this way can the benefits of a comprehensive security program be gained. Further, information sharing and joint operations are becoming increasingly important for justice and other public safety organizations. That implies the need for governance structures that cross individual agencies. Consequently, governance issues deserve prominent consideration. A common governing structure will improve the policies, processes, and procedures of any major project by enhancing communication and coordination, establishing guidelines and principles, and reducing any internal jurisdictional conflicts. The governance group should be representative of local, state, tribal, and federal entities from all participating disciplines within the identified region. A formal governance structure is critical to success.

Principles

- Governance structures for information sharing should be representative of all stakeholders.
- Governance involves technologists, operational management, and strategic business management. A good governance structure may also include appropriate elected officials, particularly for large, multiagency systems.
- At the governance level, risk assessment deals with risk to the operation, its continued viability, and the critical data it maintains.

[2] Interoperability is defined as the ability of a field officer to communicate with whomever they need to communicate, in real time, via voice or data, and as authorized.

- Information Technology (IT) and wireless management staff have the responsibility to manage security to the best standard for a given level of risk; the governance group establishes that level of risk and is accountable for setting that level appropriately.

- Governance strives for repeatable results with continual improvement.

- Governance establishes and promotes policies that ensure long-term sustainability.

Best Practices

- Include strategic business management, senior operational management, and senior IT and wireless management staff on the governance board.

- Understand that risk in a wireless environment includes many factors not commonly found in wired networks. These include vulnerability from the outside (without the need to gain facility or personnel access) to denial-of-service, interception, spoofing, etc.

- Strive for a full discussion of risk so that all participants understand the breadth and depth of the risks. Classify risks according to level, set a strategic plan to attack the highest priority risks, and know which risk each new security initiative is targeting. For example, see National Institute of Standards and Technology (NIST) Special Publication 800-63, Recommendations for Electronic Authentication, at <http://csrc.nist.gov/publications/nistpubs/index.html>.

- Understand what laws, regulations, and rules apply to the organizational participants, the disciplines, and to the information being used.

- Insist that the business purpose for each new security initiative is clear.

- Understand the total cost of ownership of each new security initiative, and make efforts to relate that cost to a return on that investment.

- Report periodically (at least annually) on progress made during the past period and the objectives set for the next period.

References

- Institute of Internal Auditors, *Information Security Governance: What Directors Need to Know*, <www.theiia.org/index.cfm? doc_id=3061>.

- Information Systems Audit and Control Association, *Information Security Governance: Guidance for Boards of Directors and Executive Management*,

<http://www.isaca.org/Template.cfm?Section=Governance&template=/ECommerce/ProductDisplay.cfm&ProductID=110>.

- IT Infrastructure Library (ITIL): Provides IT governance models.
- Control Objectives for Information and Related Technology (COBIT).

1-2. Physical Security

Description

Technologies such as Web services, wireless networking, and VPNs extend the network perimeter beyond the physical perimeter of the organization and introduce additional requirements related to physical security. For instance, because of differences in building construction, wireless frequencies and attenuation, and the capabilities of high-gain antennas, the distances necessary for positive control for wireless technologies to prevent eavesdropping can vary considerably. Therefore, organizations should be aware that physical controls are especially important in these environments. Organizations must make sure that the proper physical countermeasures are in place to mitigate some of the biggest risks such as theft of equipment and insertion of rogue access points or wireless network monitoring devices.

Purpose

This chapter identifies potential physical threats to wireless networks.

Principles

- Identify potential physical threats to departmental computer systems and networks.
- Establish policies and procedures to thwart potential physical threats.
- Conduct audits to monitor employee compliance with department policies and procedures.

Policies

An organization should consider including the following physical security policies relating to wireless in the organization's overall security policy:

- Develop security policies for securing wireless devices, including limiting physical access to wireless access points.
- Develop security policies for mobile devices, including laptops, personal digital assistants (PDAs), and cellular phones.

Best Practices

Physical security practices should address threats due to theft, vandalism, and malicious internal or external staff.

- **Theft**—Theft of hardware, software, or data can be expensive due to the necessity to restore lost data and the cost of replacing equipment and software. Mobile and wireless devices, in particular, are often targets for theft, and their loss exposes organizations to additional information security threats. Theft also causes a loss of confidence in the department that may have compromised the network.

- **Vandalism to Wireless Infrastructure**—Because the wireless infrastructure is typically located in remote and often unmanned facilities, it is frequently a target of vandalism and other attacks. Transmission towers—such as TV, radio, power, and cell and ham radio—have historically been burglarized, intentionally toppled by removal of their supports, and used for target practice and sites for suicides.

- **Wireless Threats**—Wireless technologies pose new threats that introduce additional requirements for physical security. For instance, without sufficient physical security, a malicious or irresponsible user could, physically and surreptitiously, insert a rogue access point into a closet, under a conference room table, or any other hidden area within a building.

Applying the following physical security measures mitigates these threats.

- **Identification of Unauthorized Hardware Attached to a System**—Establish policies to limit employees from accessing wireless infrastructure sites. Perform monthly audits of all wireless infrastructure sites. In particular, identify missing or misplaced hardware.

- **Protection Against Break-In**—Protect wireless infrastructure equipment in locked rooms or facilities. Any unmanned facilities, including transmission towers, should be protected with a chain-link fence with barbed wire. The exterior walls of these facilities should be reinforced concrete. The doors should be steel with locks that should be difficult to cut.

- **Entry Regulations and Controls**—Control entry into buildings and rooms housing sensitive equipment, including wireless access points which can often be reset to default configurations with physical access.

- **Security Patrol Services**—Unmanned facilities should be checked weekly, or even daily, by security patrol services. The security service provider should be familiar with the site to recognize signs of an intrusion.

- **Alarm System**—Unmanned facilities should also be protected with an alarm system that is monitored continuously by a law enforcement agency or alarm service with the ability to respond to the alarm.

- **Security of Windows and Doors**—Unmanned facilities should not include any windows. The doors to these facilities should be steel with locks that should be difficult to cut.

- **Location of Wireless Access Points in Buildings**—Wireless access points should be placed strategically within a building so that, ideally, the range does not exceed the physical perimeter of the building and allow unauthorized personnel to eavesdrop near the perimeter. In addition, some access point vendors have special features that allow control of power levels and therefore the range of the access point. However, the use of high-gain antennas can greatly extend the range of a wireless network and make limitation of the network to the physical perimeter impossible.

- **Policies for Mobile or Wireless IT Systems**—Laptop, mobile, and wireless IT systems create a greater risk of theft or damage. Due to the inherent nature of a mobile and wireless system, it will often be removed from the confines of a secure office. Therefore, policies should be implemented to safeguard mobile and wireless IT systems.

References

- National Institute of Standards and Technology Web site, *Federal Agency Security Practices*, <http://csrc.nist.gov/fasp/>.

- Karygiannis, Tom, and Owens, Les, *Wireless Network Security: 802.11, Bluetooth and Handheld Devices*, National Institute of Standards and Technology, Publication 800-48, http://csrc.nist.gov/publications/nistpubs/800-48/sp800-48.pdf

1-3. Personnel Security Screening

Description

Ensuring that the personnel within an organization who have authorized access to sensitive systems are suitable and trustworthy is the cornerstone of a good security system. Statistics show that the majority of system misuse is conducted by those with authorized access to the information. As trusted partners in justice and public safety information sharing, it is imperative that employees undergo a significant screening process to determine their suitability for access to sensitive systems and those to which they are connected. This applies to all positions and to all phases of the contracting process where access to critical systems is authorized.

Purpose

The personnel security screening discipline describes the methods that agencies must use to screen an applicant's background for past inappropriate behavior that may put sensitive but unclassified data at risk. The rigor of the screening may vary based on the applicant's access requirements to computer systems and databases. It is imperative that all applicants be screened in a standardized manner. Personnel security screening will promote trust among agency partners. From a wireless perspective, personnel screening should be the same as a wired network.

Principles

- The level of assurance of the screening mechanism employed should be balanced against the cost of the mechanism and the risk associated with incorrectly "passing" an individual trying to gain access to the information system.

- Users should be properly screened. Proper screening requires that an employer use a consistent and reliable means to conduct such screening to perform an adequate background check before authorizing access to the system.

- Personnel with direct and appropriate access to critical systems and partner systems should undergo a more rigorous background check than those with secondary access.

- Mechanisms should be in place to relieve personnel from duties requiring direct access to critical systems should their initial or subsequent background checks reveal information that would preclude their access.

Policies

Once an organization decides on an approach for personnel screening, the policies related to that approach should be documented so that there is a written guideline specifying the consistent and comprehensive application of the screening process. The personnel department will play an important role in this policy development, and new tools may need to be developed for the selection process.

Best Practices

It is a best practice to require background checks on all employees every five years.

References

For a listing of applicable security screening standards, see:

- Treasury Board of Canada, *Personnel Security Standard*, <http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/CHAPT2-4_e.asp>.

- Web site for National Association of State and Chief Information Officers (NASCIO) security policy, <http://www.nascio.org>.

1-4. Separation of Duties

Description

Separation of duties is a critical element of a robust security policy. It requires the allocation of distinct information system duties such as system security, network security, and wireless network administration, database administration, user functions, and source code access into separate job functions performed by different individuals. Separation of duties should be incorporated into change management procedures.

Purpose

Separation of duties segregates critical, operational IT functions into distinct jobs to prevent a single person from harming a development or operational system or the services they provide, whether by an accidental act, omission, or intentional act.

Principles

The approach to separation of duties should be defined in an organization's security policy.

Separation-of-duties procedures should be developed by the information system management team.

Policies

A separation-of-duties policy should be established and documented that encompasses programming, database administration, security, user functions, and source code access into separate job functions performed by different individuals. A training program should be established for impacted personnel on separation of duties, and an audit plan should be established and executed periodically to ensure compliance with the separation-of-duties policy.

Best Practices

An individual should not have access to more than one critical task as identified by management. Personnel should only perform those duties specified in their job descriptions; therefore, programming and operations functions should be performed by different individuals.

Programmers should not be able to execute any jobs in a production mode, perform database administration functions, perform application security functions, or have access to production databases.

Operators should not have the ability to make changes to production applications or system software libraries, and database changes should be administered by database administration personnel only.

Security responsibilities should be clearly separated from processing operations functions. Security functions such as authority, access to data, and restricting functions should be performed by security personnel.

Reference

- International Standard, ISO/IEC 17799, Information Technology—Code of Practice for Information Security Management.

Security Disciplines for Objective 2: Prevention

2-1. Identification and Authentication

Description

Identification and authentication security practices in wireless environments differ somewhat from those used to protect traditional wired networks. The rapid growth of Wi-Fi and other wireless technologies requires new security practices and, in some cases, new technological advancements in security that address some of the unique wireless requirements and vulnerabilities.

Purpose

While the following two definitions are an over-simplification of these two highly complex and critical processes, they do provide the correct context in which to discuss public safety unique needs in these areas when communicating across both a wired and wireless environment.

- Identification is the process through which a user presents an identifier that is uniquely associated with that user.

- Authentication is the process in which an identified user requests access to a communications network and its resources.

Principles

There are two different time frames in which a discussion on identification and authentication are useful. In addition, FIPS 199 and FIPS 200 are useful resources for profiling specific security resources.

- As mentioned previously, with the glut of commercial wireless devices on the market today, it is only logical that these devices are finding their way into public safety communications networks. So, a discussion on today's protocols for addressing these issues is necessary.

- The future of public safety communications is a rapidly evolving, moving target. As such, the environment in which public safety will find itself will be necessarily diverse. This makes it worthwhile to discuss these issues more abstractly, from a user requirements perspective rather than from a specific technological point of view.

- FIPS 199 and FIPS 200 cover impact assessment, authentication, and identification and can be used to establish a Federal Information Security Management Act (FISMA) baseline for federal networks. The security architecture used will depend on data classification and impact assessment (FIPS 199).

Best Practices in Today's Environment

The easiest technology to use in talking about today's environment is the most widely deployed wireless technology, Wi-Fi. This technology, finding a home in the IEEE 802.1x suite of standards, is the poster child for what not to do with respect to security in a wireless environment. Fortunately, this is changing with the advent of 802.11i, which specifically addresses some of the security shortfalls in the Wi-Fi family of products.

In order to correctly frame this portion of the discussion, we will talk about today's identification and authentication from a pre- and post-802.11i perspective.

To be honest, a discussion of authentication and identification pre-802.11i is moot. While there is language in the 802.11 standard that addresses an authentication mechanism, to our knowledge, not a single vendor has implemented it due to its trivial nature.

Additionally, the only identification mechanism in place for such a network will be limited to whatever third-party mechanism is installed on the platform (in most cases, nothing).

The 802.1x standard is a method for making sure that each user that connects to a network is authenticated prior to use of the network. This method was started prior to the 802.11 standard and was thus primarily meant to address wired networks. As such, some of the wording in the standard refers to physical connections between the client and the authentication mechanism. It is therefore useful, in the context of wireless networking, to consider these physical connections as logical connections instead. The 802.1x standard is the authentication method employed in Robust Security Networks (WPA2).

The following two diagrams show a simplified way of understanding the purpose behind 802.1x.

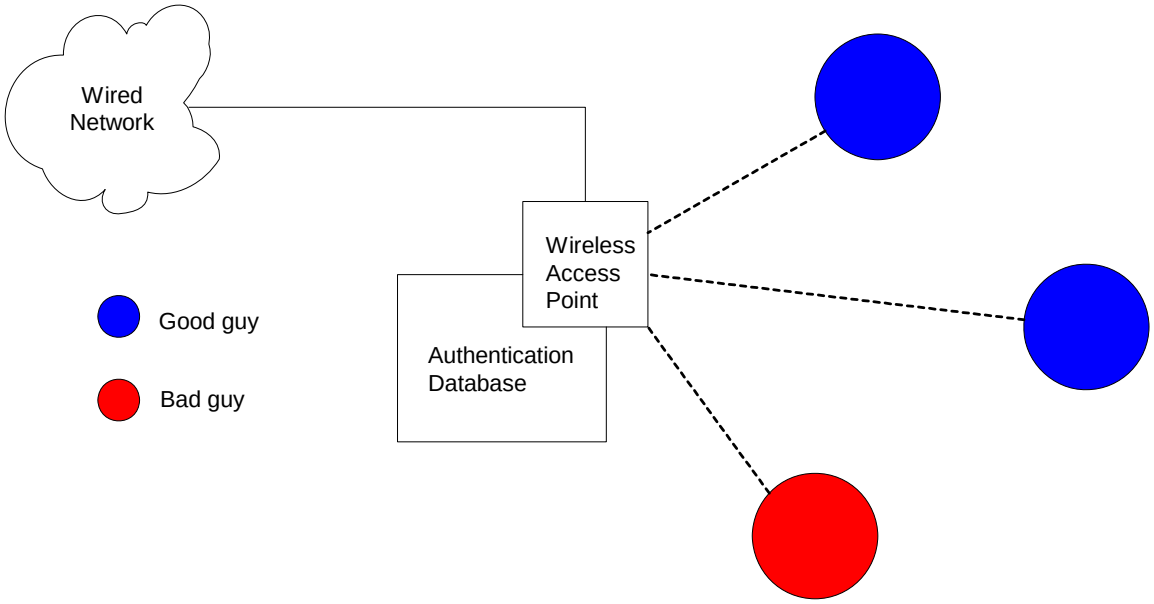

Figure 1—802.1x Organization Part 1

The users in blue are valid users in the authentication database, whereas the user in red is not. As each user requests access to the network, until properly authenticated through the database, they are not allowed access to the wired network. The following diagram depicts a conceptual method for understanding the protocol.

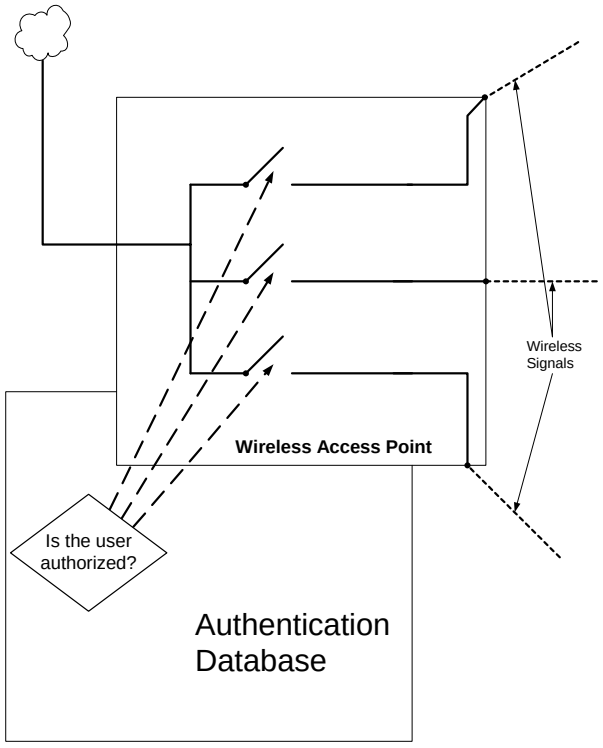

Figure 2—802.1x Organization Part 2

As each wireless user requests a connection to the wired network, an authenticator authenticates their request and identity to the authentication database. As each user is properly authenticated, their connection to the wired network becomes valid. If a user is not authenticated, the virtual switch is never closed. The recommendation is to use 802.1x which authenticates the user.

The 802.1x standard has been adopted into the Wi-Fi Protected Access/Robust Security Networks (WPA/RSN) standard that is the method for authentication. Because of its adoption into 802.11i, there is a new standard under development, 802.1aa, which will specifically address the wireless functionality behind 802.1x. The recommendation is that all wireless access points and wireless network adaptors should employ Robust Secure Network (RSN) standards that utilize both 802.1x extended authentication protocol and the Advanced Encryption Standard (AES) specified within the 802.1x.

There are two main flaws that have been identified in 802.1x: lack of required mutual authentication and session hijacking. While the use of Transport Layer Security (TLS) over Extensible Authentication Protocol (EAP) would provide strong mutual authentication, this method is often not employed and can be easily overridden. This allows for an effective man-in-the-middle attack to be used. Second, because disassociate messages are unauthenticated, an attacker could effectively forge a disassociate message to an adversary once that adversary has been authenticated by an 802.11 network via 802.1x, and once the adversary is disassociated, the attacker can effectively take over an authenticated session.

The first type of attack, as mentioned, can be mitigated through the use of TLS over EAP. The second type of attack remains a critical vulnerability to public safety networks. Until management messages in 802.1x are effectively authenticated, the networks deployed using 802.1x will remain vulnerable to these types of session hijackings and by extension, denial-of-service attacks.

In conclusion, authentication in wireless networking has come a long way since the release of the first 802.11 protocol, but we have shown that there are still areas of concern. Careful consideration and understanding can help mitigate some of the problems mentioned above but currently do not solve all of public safety's requirements in this area.

Best Practices in Tomorrow's Environment

In order to make secure identification and authentication effective as well as inexpensive, public safety is, more and more, leveraging commercial-off-the-shelf (COTS) technology and protocols. In many cases, these products do not meet the higher requirements that public safety ultimately needs.

Tomorrow's environment, with respect to identification and authentication, must take a different approach than what public safety is using today. This approach needs to look first at what their requirements are in this area, find applicable (where possible) standards-based products and protocols and, amongst the most suitable, see what changes need to be made to fully comply with these requirements. If nothing suitable exists, then public safety must pursue the creation of a standards-based solution for their requirements.

This approach is necessarily proactive in nature. Public safety will need to have a clear and consistent voice in stating their requirements and pursuing a solution. Public safety will need to take an active role in working with the standards development organizations to forward their concerns and suggestions.

What is believed with some measure of certainty is that public safety will require a diverse set of solutions for security. Therefore, we should not push toward a single solution to this series of problems. Instead, effort should be made to allow for a diverse set of solutions to be deployed, all of which must be interoperable with the other. This will allow for the greatest flexibility for each agency to make the decision best suited for its mission.

2-2. Authorization and Access Control

Description

After a user has been properly authenticated, the system knows who a user is. The system must then determine what permissions and authorizations are available to the user. Authorization and access control are an essential part of maintaining need-to-know and privacy policies and protecting sensitive information. They also support data integrity by restricting the rights to modify information to those who are authorized to do so.

Purpose

Authorization and access control are generally covered well in the *Applying Security Practices to Justice Information Sharing* document, and it should be consulted. The purpose of this section is primarily to serve as a reminder that use of wireless devices requires a consideration of the risks involved, and that authorization and access control are a key part of managing the risk.

For example, some agencies may determine that it is inappropriate to allow certain intelligence data to be transmitted wirelessly or to be stored on mobile devices. Another possible consideration might be whether or not sensitive personnel information should be available only at certain locations on the internal network and not through dial-up.

Principles

- Access or usage privileges may be based not only on user roles but also on consideration of environmental factors, such as device type or status.

- Access privileges should be granted based on a written policy.

Policies

Well-defined access policies are important to the security of an information system. The policy should consider the sensitivity of the information, need-to-know considerations, privacy restrictions, and environmental factors.

Some factors that might be considered include the user identification, device type or status, user or device location, and even the authentication mechanism. This is not meant to be an all-inclusive list but should be used as a starting point for planning and consideration. In the context of wireless security, clearly, the device type is most important, but device location and status might also be important, since a laptop, for example, might be connecting through a wireless access point or through a fixed point on the network.

The Internet and a proliferation of new wireless technologies have all but eliminated geographic barriers to communications and data sharing. They have also combined to create the need for user authentication, authorization, and access control that is portable across networks. A user authenticated on one agency's network could be recognized on another participating agency's network and granted or denied authorization to access resources based upon the authentication. Similar to the real-world passport authority in which citizens apply for a passport to be granted permission to visit another country, a user's identity is based on a locally valid credential and is issued a "passport" that can be trusted and accepted by another network. This portability of authorization and access control is being referred to as "Federated Identity and Privilege Management" and should be considered by agencies developing policies to participate in data sharing arrangements, e-commerce, and/or Web services.

Federated Identity and Privilege Management standards are in the early stages of development, but a combination of Security Assertion Markup Language (SAML), Extensible Markup Language (XML), Access Control Markup Language, and Services Provisioning Markup Language is receiving strong support with some security-focused companies already providing products.

Best Practices

Access controls must take a different approach than what public safety has been accustomed to. The traditional approach to creating and managing user accounts leads to administration, single sign-on, and compliance issues. The federated concept of identity and privilege management allows for the provider of a service or application to leverage the vetting and user-administration work already being performed by another organization to enable users with recognizable identification to securely be allowed access to the network.

Authorization to different levels of network accesses may reasonably be based not only on user identification and roles but also on the characteristics of the device being used by the user. This may require that the device be authenticated as well as the user. There are tools available that enable security administrators to establish access control rules which include consideration of environmental factors and user identification, including tools that focus primarily on just confirming that a device which has been approved is meeting enterprise standards for firewall or antivirus protection.

While it does not directly address the issue of authorization based on environmental factors, NIST Publication 800-48, *Wireless Network Security: 802.11, Bluetooth and Handheld Devices*, does include specific mention of the use of Ethernet MAC Access Control Lists (ACL) as a way to restrict network access to only those devices that have been approved by network security administrators. This is a form of device identity-based access control.

Reference

- <http://csrc.nist.gov/publications/nistpubs/index.html>.

2-3. Data Integrity

Description

When it comes to securing data as it traverses a wireless network, there are two major packet level security considerations that must be addressed: the integrity of the data and keeping the data private.

Purpose

Data integrity in this context means that the intended recipient of any data transmitted must be able to detect any modification in the data from its original form. In other words, the receiver must be able to detect tampering with the data while it was in transit. This need can be distilled down to a set of requirements as detailed in the principles section below.

Principles

- The communication system must be immune to attacks against the integrity of communications traffic. This requirement is simple; it is trying to prevent undetected modification of traffic while in transit on the public safety communications network. This type of security is critical to the overall security of the network.

- The system must conform to the Federal Information Processing Standards (FIPS) publication for data integrity or its current equivalent. The primary purpose of this requirement is to prevent a nongovernment-approved integrity mechanism from being used. The 802.11 standard is a prime example of the risk of not following a FIPS standard.

- The system must allow the administrator to implement policies as to the appropriate level of information protection. Each user on the network is not expected to be comfortable or capable of determining the level of information protection required to complete their job. As such, it will be the primary responsibility of a system administrator to determine this level, in accordance with local policy.

- The system must provide safeguards to detect and prevent unauthorized access, reading, and modification or destruction of data.

- The system must be capable of meeting its requirements in the face of a denial-of-service attack, whether distributed or not.

Best Practices

There are two ways in which the data integrity requirement of preventing known wireless attacks will impact the network. First, it will add to the overall overhead sent with each packet, as each packet will need to be protected against modification, and second, there will be some amount of pre- and post-processing associated with each packet, as it is sent and received respectively.

Ultimately, following these principles will have the affect of raising the level of integrity of the network, as the users will not be allowed to change the integrity of their traffic to an inappropriate level, as determined by local policy.

In other words, only the intended recipient for a particular piece of data should be capable of accessing, reading, modifying, or destroying data and not always that either. The policy for a given jurisdiction may be that only authorized system administrators be capable of destroying data. As such, there should be a safeguard that does not allow unauthorized users to do so.

The solution to this requirement can take on many forms. This certainly implies some kind of security method that disallows anyone but the intended user to even access received data, but it also means that a system administrator might also be able to access the same data. Ideally, the user and the system administrator would be able to access the data using different keys. A solution may require additional overhead be embedded in each packet.

It is understood that there currently is not a recognizable method of meeting all security requirements. That said, it is worth mentioning that justice and public safety users cannot afford to have their services denied to them, as life and death situations are a matter of course in this line of work. While many wireless attacks have been thoroughly researched, most of them have yet to be deployed against an active public safety wireless network.

2-4. Public Access, Privacy, and Confidentiality

Description

Public access denotes the extent to which the public (and the news media representing the public) are able to view and copy information collected and used by a criminal justice entity. It includes not only whether a particular piece of information is available to the public but also when, where, and how access is provided. The principle public access issue today is the extent to which information is made available electronically, especially on the Internet. In the past, much information—for instance, court files—has been public as a matter of law but private as a matter of practice due to the difficulty of accessing it. Only those who are intimately familiar with the operations of the entities know how to obtain the information. When court and other criminal justice entity data is placed on the Internet, or otherwise made available electronically, information that was protected by its "practical obscurity" becomes readily, cheaply, and practically available to the public and to the news media. Disclosure of certain information can be life-threatening to the subject: for example, victims of domestic violence (when the victim is at risk if the abuser locates the victim) or a criminal informant (if the criminals with whom the informant is associated learn of the informant's status).

Confidentiality is the assurance that information is shared only among authorized users. The sensitivity classification level of the information should determine its confidentiality and, hence, the appropriate safeguards.

Privacy requires confidentiality mechanisms. Privacy applies to when, how, whom, and to what extent personal information is shared. There exists no explicit federal constitutional right to privacy. However, privacy rights have been articulated in federal and state case law and statutes governing the areas of medical, financial, educational, and consumer data.

Personal information may be linked to an individual at the time of release or subsequently linked through analysis. It may be accessed or released inappropriately, causing possible loss of employment, diminished social status, or other highly adverse consequences. Personal information may include:

- Race, national or ethnic origin, religion, age, sex, sexual orientation, or marital or family status.
- Education, medical, psychiatric, psychological, criminal, financial, family, or employment history.
- Any identifying number, symbol, or other particular information assigned to the individual.
- Name, address, telephone number, fingerprint or voiceprint, photograph, blood type, or DNA.

Purpose

Criminal justice and public safety entities have historically dealt with and instituted policies concerning access to the information they collect in the course of their work. For instance, the National Crime Information Center (NCIC) has had privacy and security policies in effect for over thirty years. However, the ubiquity of electronic data and electronic documents, their exchange among criminal justice agencies, and their increasing availability over the Internet have caused the public, legislators, and criminal justice entities themselves to reexamine their historic practices. Entities are deciding that certain "public" information should no longer be public or should be made public only through traditional, paper-oriented processes. Further, concerns about public access, privacy, and confidentiality of their data create reluctance on the part of some criminal justice entity leaders to enter into information sharing arrangements. Consequently, it is critically important in today's environment for every entity to review and restate its own public access, privacy, and confidentiality policies and for information sharing agreements to include formal understandings regarding these matters.

Principles

- The communication system must allow only intended and authorized recipients to hear/see/read information.

- The communication system must be immune to traffic flow monitoring analysis from unauthorized users/devices. Enough information in each packet transmitted on the system must be encrypted to make traffic flow analysis difficult to impossible. It will be critical to prevent adversaries from doing effective traffic flow analysis against public safety, particularly law enforcement, as it could tip them off about operations that are in progress.

- The public possesses statutory, First Amendment, and common-law rights to access most justice information.

- Justice agencies use information to protect society at large. The way in which a justice agency uses personal information in the administration of justice is crucial to the protection of society and can result in life-or-death consequences. Confidentiality is required during open investigations to preserve information sources, prevent interference with the enforcement proceedings, ensure a fair trial, prevent disclosure of investigative techniques and procedures, and preserve life and safety.

- An individual's right to privacy has been articulated in state and federal case law and statutes governing the areas of medical, financial, educational, and consumer data.

- Conflicting interests must be weighed between the data subject, justice system, and the public, including the media and commercial sector.

Policies

- National Criminal Justice Association, September 2002, Justice Information Privacy Guideline: Developing, Drafting, and Assessing Privacy Policy for Justice Information Systems, <http://www.ncja.org/publications.html#>.

- State of Arizona, Government Information Technology Agency, Statewide Privacy Policy, <http://gita.state.az.us/policies_standards/html/p170_privacy_policy htm>.

Best Practices

In the public safety communications system, only intended and authorized recipients must be allowed to hear/see/read information. This requirement is where we first see a hard-and-fast rule to encrypt the payload of traffic. Encrypting the traffic in a manner that protects both the data in real-time or near real-time, in addition to providing forward secrecy, is important in the context of public safety job completion.

This requirement will certainly cause additional delay in the pre- and post-processing of the data, much like adding integrity to the data will. Additionally, the processing capabilities of a public safety wireless communications device will determine the efficiency in which this requirement can be met.

Public Access—Public access has changed with the development of technology. Privacy issues for public access include:

- **Should the information be made public at all?** Keep in mind the possibility of lawsuits for inappropriate release or for not releasing information, as well as the need to release data necessary for public safety. Also, once data is made public, it is forever public and beyond the control of the disseminating agency. Corrections and updates might be impossible to circulate. Each justice component must have some public access method.

- **At what point should justice information be made public?** For example, information should remain closed during an investigation but be made public during the trial.

- **How long should it be accessible?** Should there be a record that the deleted record once existed?

- **What is the fiscal cost of making the information public?** Ideally, it should be disclosed using all access methods (in person, telephone, or Internet). Should fees be charged to recoup the cost, or would the charges be so high that they unreasonably limit access to the information? A privacy plan must be implemented that protects the privacy of the information yet allows the agency to still protect society at large. A plan is necessary to ensure standardized implementation and enforcement of privacy.

Privacy Principles—The first step in implementing a privacy plan is to develop a privacy policy. Those developing privacy policies should look at all applicable laws, regulations, and policies already in effect. More often than not, legislative action may be needed to put the policy in place. There are eight principles to be included in the privacy policy that enforce privacy of personal information while allowing the agency to perform its vital function:

- **Purpose Specification**—Document the purpose for which personal information is collected no later than the time of data collection. Design technology to allow access restrictions to outside parties.

- **Collection Limitation**—Collect personal information by lawful and fair means, and try to collect only pertinent data. Where applicable, obtain the subject's consent. Design the technology to not require unnecessary data.

- **Data Quality**—Personal information collected must be accurate, complete, and current. Public access to inaccurate data may be worse than no access at all. If the subject has access to the data, allow for them to verify the data. If the subject does not have access, set up other means for verification, such as passive data analysis, including cross-referencing that identifies anomalies. Require logging whenever the data is accessed or modified, recording the changes by whom, when, and for what reason, to ensure accountability. Try to include tags for confirmed or unconfirmed and accurate or inaccurate data.

- **Use Limitation**—Personal information is to be used solely for the purposes specified (except with the consent of the data subject) by authority of law, for the safety of the community, or pursuant to a public access policy. Use limitation is generally applicable to disclosure outside the justice system but may also apply between agencies if disclosure is not mandated by law. The policy should also consider possible secondary- or third-party usage of the information. An audit trail should be incorporated in the technology to enable a use assessment.

- **Security Safeguards**—Protect personal information with reasonable safeguards against risk of loss or unauthorized access, modification, use, destruction, or disclosure. A risk assessment should be performed with security modifications made, as necessary. Also, an information classification review should be done periodically to ensure data is being safeguarded at the proper security level. The system should log all attempts to alter information or attack the system.

- **Openness**—Provide notice to the data subject about how the personal information is collected, maintained, and disseminated. Provide notice to the public of the existence of personal data and access to data in accordance with a public access policy. Openness includes public access to the management practices of the data, except where it directly relates to an investigation, a pending or open case, or safety concerns and other factors that a government determines as necessary exceptions. The technology system must log all

transactions on an individual's file and allow for independent oversight for accountability purposes.

- **Individual Participation**—Allow affected individuals to access their personal information, except where it would compromise an investigation, case, or court proceeding. Subjects should be able to:

  - Obtain confirmation that the agency has their data.
  - Obtain data relating to them within a reasonable time, at a charge (if any) that is not excessive, in a reasonable manner, and in a form that is readily intelligible.
  - Be given reasons if an access request is denied.
  - Challenge a denial and, if successful, have the data erased, rectified, completed, or amended.
  - Provide an annotation to data where an organization decides to not amend the information as requested.

  The technology must be designed to create copies of the personal information and to amend or annotate information subject to disagreement over accuracy. The system must also have the capacity to notify third parties, in a timely manner, which have either provided or received incorrect information.

- **Accountability**—Oversee and enforce the other seven privacy principles. An individual must be designated as the information steward responsible for establishing regular security audits, privacy impact assessments, and privacy audits. The steward should have a procedure in place for challenges to the system and should assure that timely, fair responses are made to inquiries. He is also responsible for training staff on privacy protection requirements.

  A privacy plan requires cooperation between each agency accessing the data. Sharing personal information becomes even more difficult because agencies have different functions and differing statutes and regulations. What one agency considers sensitive may be open to the public in another agency. For instance, information from closed-record states becomes publicly available once it is shared with an open-record state. Compiling public data from several different agencies may also yield obviously confidential information.

  Current systems range from paper-driven to the highly automated. Also, many of the current systems were developed without proper thought to privacy concerns. This can result in having to manage unintended privacy issues and having to retool the system—both of which can be quite expensive. The ideal is to address privacy during the planning stages of information system design.

Each agency should classify the information they create and maintain with an appropriate confidentiality level. Procedures should be documented stating when and where this information may be disclosed to the public or other agencies. Disclosure should be determined by the type of information and the context in which it is shared. For example, local security procedures should be classified at least at Level 3. Each agency must also review the privacy and public access policies of the agencies with which it exchanges information. To ease the transfer of data, the agencies should adopt the same terms, data entry fields, data definitions, and data structures.

The information steward for each agency should perform a Privacy Impact Assessment that has three components:

- A map of the information flow. Each justice agency should map the flow of the information it maintains. The map must include each data element in the justice record. At each mapped decision point, it should indicate the type of received information, the purpose for which it may be used, whether it is personally identifiable, and when and to whom it may be disclosed.

- A privacy analysis of the information flow, indicating adherence to the privacy policy.

- An assessment of the issues uncovered in the analysis and options to mitigate privacy risks.

After each agency has performed their Privacy Impact Assessment, a second assessment should be completed on the entire integrated information sharing system for the information exchanged between agencies.

References

- Organization for Economic Cooperation and Development, *(OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, <http://www.oecd.org/>.

- Health Insurance Portability and Accountability Act (HIPAA) of 1996, Standards Model Compliance, <http://www.cms.gov/hipaa/>.

2-5. Firewalls, VPNs, and Other Network Safeguards

Description

Wireless networks are susceptible to all of the same vulnerabilities that exist in conventional wired networks. In addition, users may gain access to a network through wireless access points. Depending upon the configuration of the network, this may allow malicious users to bypass any protections in place that protect the wired network from external intruders. Furthermore, users (both authorized and nonauthorized) may deploy unauthorized equipment that enables access to the wired network that bypasses perimeter protections.

Purpose

Technologies such as firewalls, virtual private networks (VPN), and virus protection systems are already widely deployed in wired private networks that need to access public networks. These are also needed in a wireless environment, and a judicious implementation of these technologies can help mitigate the risks of deploying a wireless network.

Principles

The principles underlying firewalls, VPNs, and virus protection systems in the wireless environment are basically the same as for the wired environment. The only significant change is that best practices suggest that, because of their vulnerabilities, wireless access points should be considered untrusted devices.

Policies

A comprehensive set of security policies should be developed and maintained through periodic review and updates, regardless of the type of network employed. These policies should include comprehensive coverage of wireless devices of all types.

Best Practices

Virtual Private Networks (VPNs)—Clearly, in any wireless technology, additional security precautions should be deployed beyond relying on the basic defaults. VPN and other similar technologies (e.g., SSH, SSL) provide a means for enhancing security.

Most VPN technologies operate independently of the communications link. The same VPN technology that works for dial-up connections, cable, and Integrated Services Digital Network (ISDN) will also work for Personal Communications Services (PCS) wireless data connections (e.g., GPRS/EDGE, 1xRTT, and Wi-Fi (802.11)). This, however, does not mean that VPN technology should not be augmented with certain capabilities to make the wireless experience as secure and robust as the wire-line experience.

Considerations for VPNs in the Wireless Environment—The benefits of VPNs have long been established. Almost all VPNs can work both in the wire line and wireless environment, but it

does not mean that they all provide the same level of service or functionality. In short, they are not all created equal.

Most VPNs have been designed for stationary users and point-to-point networks. They were built without consideration for mobility. Therefore, they do not support roaming from one network type to another (e.g., going from GPRS to Wi-Fi) nor are they very robust in handling network disconnects and network time-outs. They do not support automatic security enablement. Finally, VPNs, as a rule, do not automatically select the best transmission means when more than one wireless option is available.

When examining VPNs for use within a wireless environment, the following items should be considered:

- Seamless roaming between networks and technology.
- Application persistence during roaming.
- Connection management and prioritization based on bandwidth.
- Type of compression offered.
- Comprehensive and automatic security (e.g., end-to-end encryption using current industry standards like Advanced Encryption Standards (AES) and 3DES).
- Authentication capabilities (e.g., RADIUS, Microsoft Active Directory).
- Existence of integrated firewall.

Connecting the Wireless Network and the Wired Criminal Justice Network—Once the networking on the mobile side is finalized, security between the wireless operator's network and the criminal justice network needs to be considered. If the criminal justice network currently allows for access via VPN, using the public infrastructure with the VPN may be enough. However, if more security is required with a more reliable network connection, consider dedicated facilities (e.g., frame-relay circuit) or a dedicated serve-to-server VPN connection between the wireless carrier and the criminal justice intranet.

Many VPN devices today have integrated firewalls. These firewalls can help to restrict traffic to certain locations within the larger wired enterprise network, thus providing an additional layer of protection. Use of an integrated VPN/firewall device can reduce costs and administrative burden.

Firewalls—Firewalls are a security system to protect a network containing servers, client computers, and intelligent communication devices from intentional or accidental damage or unauthorized access implemented by either hardware or software. The function of a firewall is the same, whether deployed in a wired environment, a wireless environment, or a mixed environment. A firewall should be considered a fundamental piece of any wireless network infrastructure.

Considerations for Firewalls in Wireless Environments—Cellular carriers will most likely provide firewall protection within their networks. While this provides a level of protection

during transmission that does not exist with Wi-Fi-based systems, it is still not a totally secure solution. Users are well advised to deploy their own firewalls as supplements. Systems relying on cellular carrier-based technologies may need to work with the carrier to ensure that existing enterprise firewalls and the carrier's system will work well together. Carriers may work with you to configure your existing enterprise firewalls to work with the wireless system. Some carriers may also offer to set rules within the carrier-based firewalls that will provide additional protection to your network (for example, limiting access to specified devices). Be sure to investigate these options (and their costs) when considering any cellular-based system.

As mentioned earlier, a key principle guiding the deployment and use of firewalls is that any wireless access point should be considered to be an untrusted device. This should be viewed as particularly true for Wi-Fi-based access points, given the current weaknesses in Wi-Fi security. The ability to tailor the firewall rules to the specific users and environment is an important consideration in selecting a firewall for the wireless environment.

Connecting the wireless network and the wired criminal justice network—Best practices in security encourage the use of subnets within the wired environment. For example, many enterprise networks utilize internal firewalls to restrict access to internal networks that perform sensitive functions, such as accounting, human resources, or other competition-sensitive material or functions.

In the wireless environment, establishing subnets for wireless access points is clearly a best practice. This means that wireless access points should be installed on a separate network(s) dedicated to wireless users, with a firewall between the wireless network(s) and the enterprise wired network. All traffic that travels from a wireless network to the wired network must go through a firewall. The firewall will control what internal resources are available to wireless users. These resources may vary by user and may be different from that same user's access rights if they connect through the wired environment.

Simply separating the wired and wireless networks by a firewall may not be sufficient if the wired network contains particularly sensitive data. For greater security, a VPN connection in combination with the firewall may be used between the wired network and the wireless subnet. VLAN implementations have been shown to be susceptible to VLAN hopping, particularly in the trunking between switches. Therefore, the recommendation is that network designers should consider that separate physical switches be used for the wired and wireless networks when practical and not cost prohibitive.

Firewalls and Wireless Clients—In a wired network, the need to use a personal (or client-based) firewall depends largely upon the data present on the device. As a best practice, personal firewall software should be installed on all wireless clients. Personal firewalls help to protect client devices against wireless network attacks, particularly when used in public or shared Wi-Fi access areas, where files on an unprotected device may be available to all other users of that wireless access point.

Antivirus Software—A computer virus is a malicious set of programming instructions that are disguised and incorporated into files. Operating at times outside of the secured wired environment, mobile devices may be more likely to be exposed to viruses than devices that

are permanently attached to the wired network. Just as every desktop computer in a wired environment should be protected, so should every mobile device have an antivirus software application installed on it. Ensuring that the antivirus applications are regularly updated should be enforced as well.

Wireless Network Interface Card (NIC) configuration—Due to the ease with which an attacker may counterfeit a trusted access point, it is recommended that Wireless NICs are configured to not permit auto association with access points not employing mutual authentication. Wireless NICs typically connect to any available access point or ad hoc peer. This default configuration provides a connection to the user system that may allow for intrusion.

Other Network Safeguards—Another line of defense against intrusion through the wireless network is to install services that ensure that the client meets all established security policies before granting the user access to the network. These requirements could include having up-to-date and running virus scanning software, running personal firewall and/or VPN software, and any other administrator-defined parameters. This type of service requires both a client-based application and a network-based service. Users that pass all the checks are allowed appropriate access to the network, while those who do not meet the access criteria can be directed to a different location to get the required updates.

Intrusion Detection System/Intrusion Prevention System (IDS/IPS)—The IDS/IPS monitors events occurring on a network or in a computer for evidence of intrusions, which can be unusual usage patterns or attempts to bypass security to compromise the integrity, availability, or confidentiality of a network or computer. An IDS is just one of the many safeguards required to protect an organization's information technology resources. The original Applying Security Practices references IDS in Section 3-1.

An IDS can be compared to a home alarm security system because they both provide an alert when an abnormal or predefined event occurs. IDS technology has evolved over the past 20 years, and IDSs that are currently available can identify the type of event that has taken place, when the event occurred and, in some cases, the sources of the intrusion. The IPSs provide the capability to program automated responses and deterrents to some alerts.

An IDS/IPS is recommended and is almost mandatory in the wireless environment. Data classification and impact assessment (FIPS 199) are helpful resources in determining which security architecture is required to safeguard the network.

Security Disciplines for Objective 3: Detection and Recovery

3-1. Attack Detection and Prevention

Description

When it comes to wireless security, it is not easy to distinguish myth from reality. We often hear information in the media, and even in the security community, regarding what attacks are possible, and it is easy to wonder whether some of these claims are exaggerations. To complicate matters further, as technology improves over time, previously infeasible attacks become practical and worthy of attention. This section attempts to separate myth from reality by describing the major variations on each of the four types of wireless attacks (eavesdropping, modification, masquerading, and denial-of-service) and discusses their feasibility with current attack tools.

The most likely threats to public safety wireless deployments, especially those using 802.11 technologies, are passive eavesdropping, masquerading, and denial-of-service attacks. All of these are supported by widely available tools and can be difficult to detect. In addition, passive eavesdropping and denial-of-service can never be completely prevented.

Eavesdropping attacks are designed to expose protected information. Passive eavesdropping, the most likely eavesdropping threat, can be best prevented through the use of strong encryption.

Masquerading attacks involve the attacker inserting themselves into the wireless network. In most of these attacks, the attacker simulates the wireless access point itself. Fortunately, the Wireless Protected Access (WPA) and 802.11i technologies are effective defenses against these attacks and are becoming widely available.

Denial-of-service (DoS) attacks can shut down a wireless network to some or all of intended users or systems. DoS attacks are a common threat to all wireless technologies, but 802.11 networks are particularly vulnerable to these attacks. Although there are tools for detecting and triangulating the source of a DoS attack, there are no effective ways to prevent them making these attacks virtually inevitable. Therefore, all public safety agencies should identify a backup communication mechanism to use in the event that the wireless network is unavailable.

Monitoring in a Peer-to-Peer Transaction

There are two consistent forms that communications can take on any data network: client/server and peer-to-peer. In either form, a public safety data network must retain the capability to monitor the communications occurring, both for reasons of security and nonrepudiation.

In client/server communications, monitoring transactions is trivial and is typically done at the server side of the communications, where resources available on the server allow for easy storage of any log files generated while monitoring the system. It is simple to add more

resources to the server side of a client/server transaction to monitor the actions as the number and scale of the actions tracked grows.

In peer-to-peer communications, monitoring transactions is anything but simple. The form factor of the device used in public safety peer-to-peer communications (such as a PDA) makes creating and storing log files taxing from a processing and memory perspective. It presents a security risk that the only log for such a transaction resides on a device that is less physically secure than a server in a hardened data center. If a log were to be kept on a device other than those involved in the peer-to-peer transaction, some of the advantages to having peer-to-peer transactions are lost, such as no need for centralized service management. For instance, if each action required to be captured is saved to a database somewhere on the network, a vast amount of traffic traveling on the network will be associated with monitoring and nonrepudiation and not the primary mission of public safety. If, on the other hand, all of the information is collected locally to each communications device associated with the data to be collected, the overall network traffic decreases, but the local storage requirement for each device grows a great deal, in addition to the physical security issue pointed out earlier.

Known Wireless Attacks (Myths and Reality)

There are four main methods of attacking a wireless network: eavesdropping, modification, masquerading, and denial-of-service. Each method of attack has several submethods, which will be described in the appropriate following section. In addition to describing the methodology behind each attack, the attacks will be analyzed for their feasibility from an attacker perspective, i.e., how difficult is the attack to implement and is there a justifiable return on the investment for each attack type.

Eavesdropping—There are three kinds of eavesdropping attacks that are pertinent to public safety communications: traffic analysis, passive eavesdropping, and active eavesdropping. These types of attacks are the least intrusive of the four methods under analysis in this guide.

Traffic Analysis—Traffic analysis is a technique where the attacker discerns information about the traffic traversing a communications network by analyzing the unencrypted portions of the traffic. A now classic example of traffic analysis can be shown with respect to the start of the second Gulf war. Several hours prior to the commencement of military strikes against Iraq, the Pentagon ordered several thousand pizzas from local pizza shops. An attacker need not have listened in on the actual conversation or been inside the Pentagon, thus making the confidentiality of the messages irrelevant. Instead, the attacker only needed to be cognizant of the fact that there was an impending invasion being planned to figure out what was going on.

In an Internet Protocol (IP) network, there are four pieces of information that can be used for basic traffic analysis: the number of packets traversing the network, their size, the source of the traffic, and the destination of the traffic. These pieces of information are open to analysis for all IP traffic, as it is required for intermediate routers to ensure delivery of the traffic from source to destination. So, as in the example provided above, breaking the confidentiality of the messages is unnecessary for basic traffic analysis.

In a public safety environment, there are additional types of information that can be gathered with this type of attack. Through the use of a yagi, or helical directional antenna, the attacker can not only increase the distance from which this attack can be performed, but information as to the geographical location of transmission can also be gathered. This holds true for both the public safety first responders themselves, as well as pieces of infrastructure, whether fixed or mobile. The feasibility of such an attack is simple. Creation of a yagi antenna involves nothing more than a Pringles can, a steel rod, and a few washers. In fact, this technique is the same technique used by the military to triangulate the position of radio communications in the field for calculating firing positions for aircraft or artillery (but without the Pringles can).

Passive Eavesdropping—Passive eavesdropping will also benefit from some of the same techniques used in traffic analysis, such as the use of a yagi antenna to increase the distance from which the eavesdropping can be performed. With this type of attack, the attacker simply monitors traffic traversing a particular link.

There are two types of information that can be garnered from this type of attack: analysis of the data transmitted during a particular session and information that could be used for basic traffic analysis. In an unencrypted channel, where the public safety first responder does not have another layer of security added through some other mechanism, this type of attack can be particularly damaging, not to mention trivial to carry out.

From a public safety standpoint, this type of attack will be nearly impossible to prevent and trivial to attempt. The only real way to mitigate the affects of such an attack is to use strong encryption. Depending on the security system deployed, this encryption can be broken as a function of the rate of traffic transmitted on the transport. As such, extra security measures would necessarily need to be deployed.

Modification—There are two kinds of modification attacks that are pertinent to public safety wireless communications: packet modification and packet injection. Both attacks are also known as active eavesdropping. These types of attacks are intrusive attacks but are more subtle in their methodology than a masquerade or denial-of-service attack.

Active Eavesdropping—The name of this method sounds counterintuitive. In fact, the name is very appropriate. This type of attack involves the attacker invoking a passive eavesdropping attack against a network, but in addition to simply monitoring the network, the attacker will inject bogus traffic into the network from time to time to help decrypt the data, if it is encrypted at all.

This type of attack can take one of two different forms: the attacker can modify a packet in transit, or the attacker can inject a new packet into the network. Modification of a packet while in transit is not a trivial attack. In order to effectively perform this kind of attack, the attacker must prevent the packet's destination from receiving the packet intended for modification, while modifying the packet in such a way as to generate an unencrypted packet sent to itself. One method of accomplishing this is to modify a packet's destination IP address while in transit. This is shown in the diagram below.

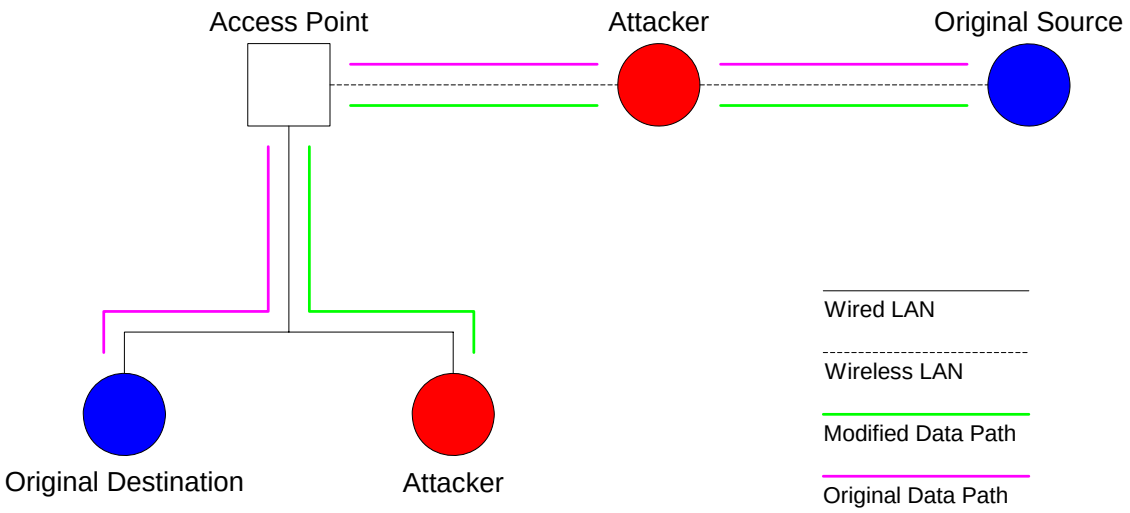

Figure 3—IP Spoofing

Using an 802.11 Wireless Local Area Network (WLAN) as an example, the original source of the data that is being attacked is sent through the attacker on the WLAN. If the packet is encrypted because Wired Equivalent Privacy (WEP) uses a cyclical redundancy check (CRC) for maintaining the integrity of the data, the attacker can modify the destination IP address to one that the attacker controls, modify the CRC accordingly, and retransmit the packet to the access point. With 802.11i, this attack becomes nontrivial to implement and will most likely not be encountered with 802.11i deployed in the near term. The access point that receives the modified packet then decrypts the packet and sends it unencrypted to the modified destination. This type of attack actually accomplishes two things. First, the modified destination now has an unencrypted portion of data, and second, it provides the attacker the ability to perform a known plaintext attack against the key used in encryption. This type of attack is easier than a brute force attack.

In the case where the attacker cannot implement this "man-in-the-middle" style of attack, modifying traffic in transit becomes even more difficult. Generally speaking, attackers will not have the technical sophistication to implement this type of attack. It involves radiating a signal at the wireless access point at the same time that the source is transmitting its data. While the source is transmitting its data, the attacker radiates only when it intends to change a particular bit that the source is sending. This involves incredibly precise timing in order to achieve success.

With the injection of a new packet into the network, the attacker is trying to take advantage of weaknesses in WEP and other symmetric ciphers. In order to achieve success in this type of attack, the attacker usually must be an insider. This will allow the attacker to transmit encrypted traffic to the access point. In this fashion, the attacker will now have a copy of its encrypted traffic and the traffic prior to encryption that is resident on its attack platform. With this information, it will be trivial to obtain other encrypted traffic due to the following: C_1 XOR C_2 = P_1 XOR P_2. The attacker has C_1, which is the cipher text of its transmission, as well as P_1, which is the plaintext involved in its transmission. It obtains C_2, which is the data under attack. If the initialization vector has not changed between the transmissions, then

obtaining P_2 is trivial. The only real method to mitigate this attack is to change the initialization vector frequently. Even then, rotating the initialization vector only becomes a race with the attacker, not a sure form of security. Again, the use of an 802.11i protected system will make this attack virtually impossible to perform effectively with today's computing systems, if at all.

Are these types of attacks feasible, with or without regard to public safety? In the case of in-the-air modification, the engineering resources necessary to carry out such an attack make it infeasible. In fact, though technologies such as software defined radio (SDR) are commonly discussed as a platform with which to carry out such an attack, the availability and cost of such devices are rare and expensive. Additionally, should an attacker acquire one of these devices, the technical expertise required to instigate an attack with the device is nontrivial. While this problem will continue to grow with the increasing availability of such radios, the security against such attacks is also expected to grow, hopefully keeping pace with or staying ahead of their deployment.

For our purposes, masquerading is the attempt of an attacker to create a deceptive appearance, where in most cases that appearance was of a trusted wireless access point. It is somewhat indicative of the methodology employed by attackers performing masquerade attacks. One of the most common masquerade attacks is the man-in-the-middle attack. One subset of the man-in-the-middle attack is the ARP Cache Poisoning attack. Another type of man-in-the-middle attack is a replay attack. The last masquerade attack that will be covered in this section will be session hijacking.

Man-in-the-Middle-Attack—A successful man-in-the-middle attack is really about the attacker attempting and succeeding at masquerading as the wireless access point that the user is trying to maintain a session with. Figure 4—Man-in-the-Middle Attack Stage 1 depicts the first stage in the man-in-the-middle attack. The attacker sends 802.11 disassociate messages to the source under attack. Once the source has successfully been disassociated with the access point, the attack progresses to Stage 2.

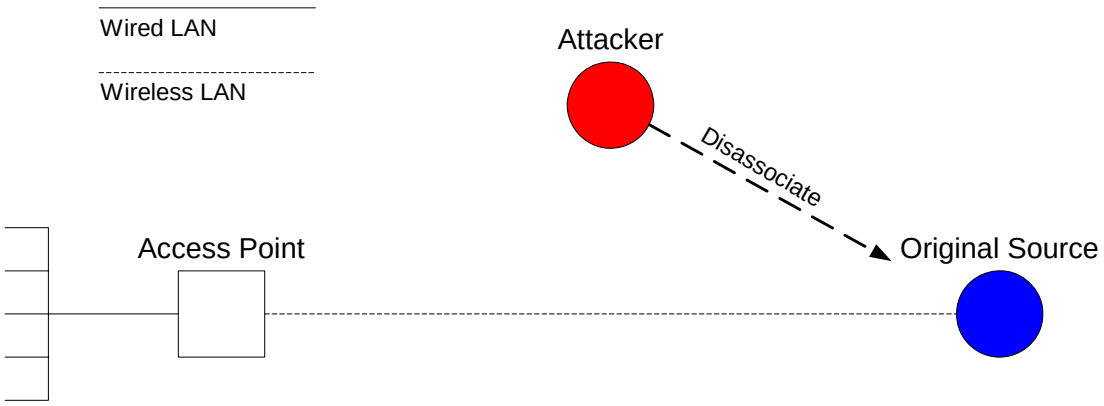

Figure 4—Man-in-the-Middle Attack Stage 1

In Stage 2 of the attack, depicted in Figure 5—Man-in-the-Middle Attack Stage 2, the attacker masquerades as a wireless access point so that the source under attack will attempt

to associate itself with the attacker. The attacker will also seek to associate itself with the original access point. Once the association is completed, the attacker will relay all of the traffic from the source to the original access point but only after having complete access to all of the source's traffic.

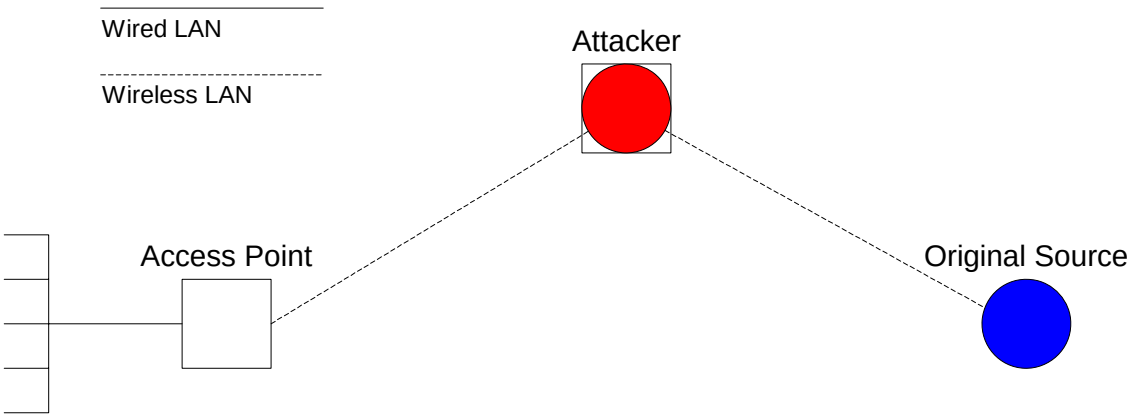

Figure 5—Man-in-the-Middle Attack Stage 2

These types of attacks could be particularly damaging to a public safety user due to the power that the attacker can exercise with respect to the traffic the source sends and receives. For instance, if a user is trying to send a distress call to an incident commander during a particular emergency, the attacker can choose to not relay that particular message onto the incident commander and can then respond with a message as if the incident commander did indeed acknowledge the message, giving the user a false sense of security and safety in an otherwise dangerous situation.

The feasibility of such an attack is known. There are software packages that provide the fundamental tools necessary to perform this attack on 802.11 networks. The code in the tool does not actually work properly at the time of writing, but it is only a matter of time before a working version of the code becomes widely available. If public safety were to deploy an 802.11 network, the network would necessarily inherent this vulnerability.

ARP Cache Poisoning Attack—Address Resolution Protocol (ARP) attacks are a subset of the attacks described in a man-in-the-middle attack. These attacks differ from traditional man-in-the-middle attacks in that the attacker is not trying to masquerade as the source under attack. Instead, the attacker is trying to reroute all traffic of the source through itself. This is accomplished by taking advantage of the ARP cache on the source's radio.

ARP is a method of mapping Layer 2 Medium Access Control (MAC) addresses to Layer 3 IP addresses. Every time the source issues an ARP request for traffic that it wants to send to the specified destination, the attacker will respond with its MAC address mapped to the particular IP address, as opposed to the true MAC address associated with the IP address in question. This will enable the attacker to effectively serve as a repeater for all traffic between the source and its destination. One additional and powerful effect of this type of effect is that it is not limited to the wireless clients associated with a particular wireless access point. The

attacker can also effectively present modified ARP replies to wired clients as well. The traffic that is routed through the attacker can be used for all of the eavesdropping attacks.

This attack will be possible with an 802.11 deployment that uses WEP as security for the system, but as WPA and RSN (802.11i) become more widely deployed, the ARP traffic will become much more difficult to poison, as the traffic will be encrypted beyond a point which is trivial to crack. Up until that point, this attack could significantly hobble a public safety network.

Session Hijacking—Session hijacking is an attack where the attacker takes control of a validated, authenticated session. The original user of the session may become aware that the session is no longer available but will most likely not know the reason behind the loss of the session. This attack must occur while the session is active on the part of the original user, but due to the nature of the attack, the attack can continue long after the original user is on the network.

There are two steps to successfully completing a session hijacking. The first step is that the attacker must represent itself to the network as the user it is trying to gain control of the session from. This is accomplished by having first performed a successful eavesdropping attack against the user to gain access to any encryption used, which will garner authentication tokens for use in maintaining the session. The second step is that the attacker must force the user to stop using the session. Much like the man-in-the-middle attack, the attacker can issue a series of disassociate messages to the user to force them off the session under attack.

This type of attack could cause significant headaches within a public safety network. Effectively, the attacker would "become" an authenticated user on the network, with full access to network resources.

The feasibility of such an attack is the same as with the previous ARP poisoning attack, where the vulnerability exists in WEP-protected systems, but becomes mitigated with the use of WPA and RSN (802.11i).

Replay Attack—Replay attacks are attempting to get the same type of network access. The primary difference is that in session hijacking, the attacker is trying to wrest control of a session from the user in real-time. While in a replay attack, the attacker is trying to gain network access after the original session between the authenticated user and the network has expired.

First, the attacker must engage in passive eavesdropping on a session or group of sessions. Timing is important in this aspect of the attack, as the attacker must be able to catch a user authenticating into the system, not capture data in the middle of a session. The next part of this attack involves the decryption and/or modification of the authentication packets that were captured in the first part of the attack. If the authentication packets are encrypted and the attacker cannot decrypt the packets, this does not prevent the attacker from making modifications to the packets. Once the attacker has the authentication packets ready, the attacker will send them to the wireless access point, gaining entrance to the network with a new session.

Just as in the session-hijacking attack, this attack could be particularly damaging to public safety, in that an attacker could gain access to resources that would undermine the ability of the users to do their jobs. These types of attacks are also feasible when used against a WEP network but become ineffective with 802.11i.

Denial-of-Service (DoS) Attack—A denial-of-service attack can be the most damaging of the attacks discussed thus far. The obvious reason for this is that it completely denies authorized users access to the network resources necessary to do their job. This does not mean that the attacker cannot use the network either. On the contrary, depending on the method of denial-of-service used, the attacker could deny service to all authorized users, while allowing access for itself to the network.

Additionally, these types of attacks are commonly misunderstood to be attacks where the attacker floods the network with so much traffic that authorized users cannot access the medium to transmit valid traffic. The DoS methods described in this section do not flood the network with traffic in an attempt to deny service, instead taking advantage of security vulnerabilities in the network management itself.

There are three main types of denial-of-service attacks that will be covered in this guide: routing attacks, identity attacks, and medium access control attacks.

Routing Attacks—A routing attack is an attack against a mobile environment's routing tables. These routing tables are used by a network to create a mechanism to get traffic to its intended destination, as well as can be done, measured against the particular metric used by the routing protocol selected for the network.

An attacker in this type of network can operate in one of two modes: it can be an active participant in the network, thus enabling itself to act as a repeater when needed, or it can operate outside of the authenticated network.

In the first mode of operation, the attacker must gain access to the system if it is encrypted. Once access to the system has been achieved, the attacker can begin decimating any traffic that is routed through it. This will result in an overall decrease in the quality of service available on the network (with traffic routed through that particular node).

In the second mode of operation, the attacker must also gain access to the system. Once the attacker has access to the system, it can begin poisoning the routing tables of nodes on the network by sending out spurious routing tables. This will effectively force the nodes on the network to transmit traffic with routing information that is in error, resulting in lost traffic.

Identity Attacks—Identity attacks are attacks that take advantage of the trust automatically generated between a user on the network and the wireless access point on the network. Management traffic sent from the wireless access point to the user nodes is sent in the clear, making it relatively easy to generate an attack based on this traffic. There are three main types of identity attacks that can be used on an 802.11 system: disassociation, deauthentication, and power-saving attacks.

All three of these attacks have the same potential for damage to a public safety user network. Each of these attacks is a feasible attack, and trivial due to the fact that, if encrypted, the network key need not be known to implement these attacks anyway. These attacks can effectively shut down the entire network for any number of users that are targeted by the attacker.

Public safety networks that take advantage of 802.11, even with WPA and RSN, will be continuously vulnerable to these types of attacks, as the ability to forge management frames within the network will still be possible. This type of attack will require that extreme caution be used during deployment of any public safety 802.11.

Disassociation—The 802.11 standard provides for a disassociation message that is unauthenticated between the user and its associated wireless access point. The standard clearly states that neither the user nor the access point can ignore a disassociation message that is sent. There are nine different reasons that can be used for disassociation, any of which will cause the state machine of the recipient to change to disassociated.

While this attack can be effective, it is less efficient than the deauthentication attack because the disassociation attack just causes the user to do extra work in order to reassociate with the access point. In order to effectively deny service to the user under attack, the attacker must scan the network listening for each reassociation attempt by the user (or association attempt if it is the first try by the user) and actively disassociate the user after each successful association.

Deauthentication—Much like the disassociation attack, deauthentication messages are not authenticated between the user and the wireless access point. This allows for deauthentication messages to be forged by an attacker. How fast a user begins the process of reauthenticating into the network will determine how often the attacker needs to undergo the process of deauthenticating the user.

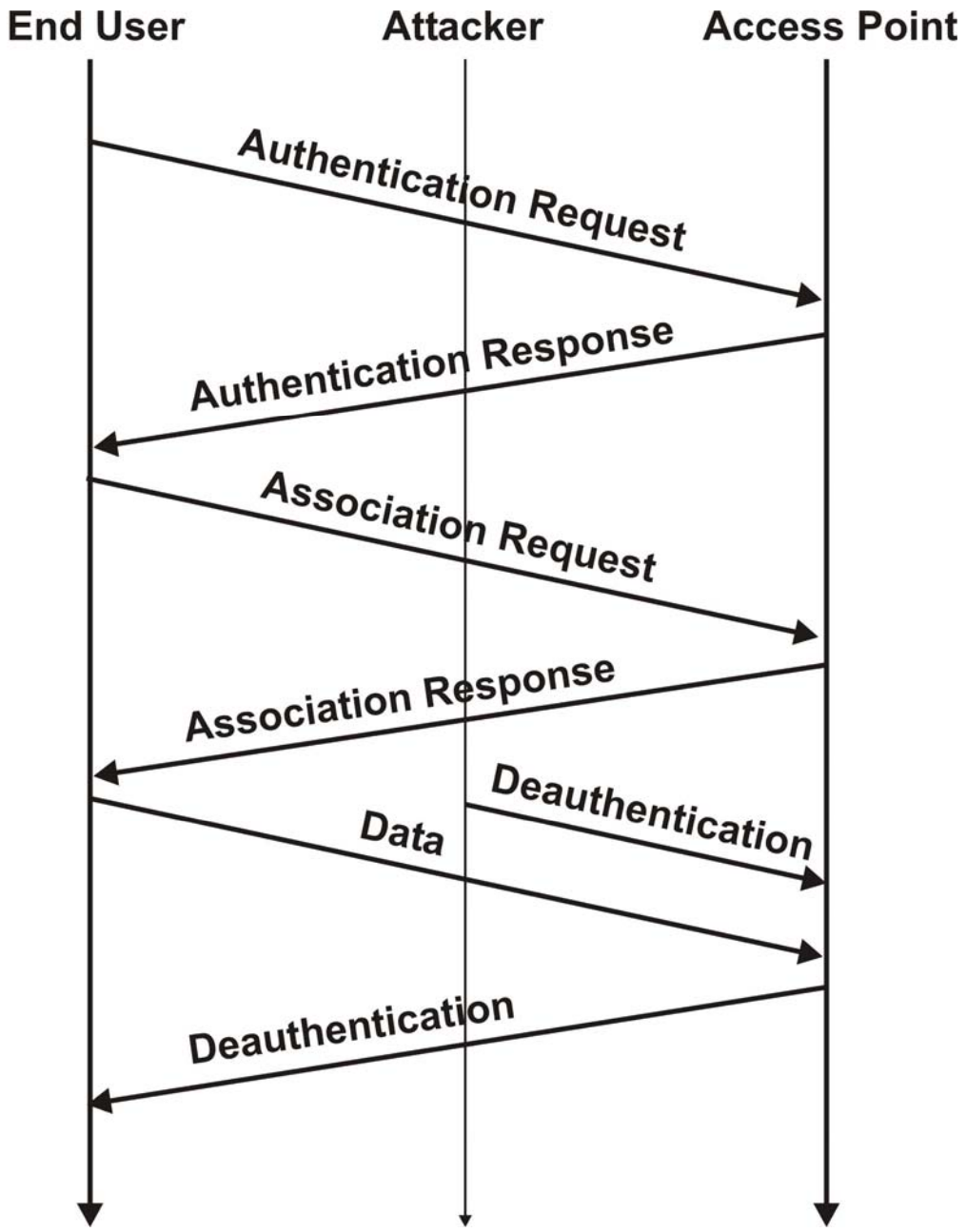

Figure 6—Deauthentication Denial-of-Service Attack[3]

Because association is a prerequisite of authentication in 802.11, deauthenticating a user will also necessarily disassociate the user as well.

Power Saving—A power saving attack stems from the functionality built into 802.11 that allows a user device to sleep for a period of time, waking and polling the access point to send

[3] Compliments of John Bellardo and Stefan Savage in *802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions*

any data that has been queued for the particular user device. There are three main attack methods with regard to power saving.

The first and easiest to implement is an attack where the attacker masquerades as the user, periodically polling the access point for the user's data, effectively preventing the user from receiving any data. After each polling message sent by the attacker, the access point will transmit the data and then discard it.

The second type of attack mimics the first attack somewhat, but in this case, instead of convincing the access point that the attacker is a user, the attacker convinces the user that it is the access point. This is accomplished through the transmission of a traffic indication map (TIM) packet to the user. This type of packet could be spoofed by the attacker, convincing the user that there is no data available for it, which effectively puts the user back to sleep again.

The third type of power attack revolves around the time synchronization between the user and the access point. The timing messages transmitted by the access point to the user are sent in the clear. The attacker could spoof these packets so that the user falls out of synchronization with the access point, effectively denying the user access to any buffered data.

While this type of attack could prove effective against public safety, it is unknown at the time of writing whether or not this type of attack is feasible with commercial off-the-shelf (COTS) equipment and software.

Medium Access Control Attacks—Medium Access Control (MAC) attacks are possible due to the assumption of universal cooperation between all nodes on the system. The cooperation is, in effect, a method of avoiding transmission collisions between users in the same spectrum. There are two main methods of collision avoidance: the first employs the standard MAC mechanism defined in the IEEE 802.11 standard, and the second method solves the hidden node problem shown below.

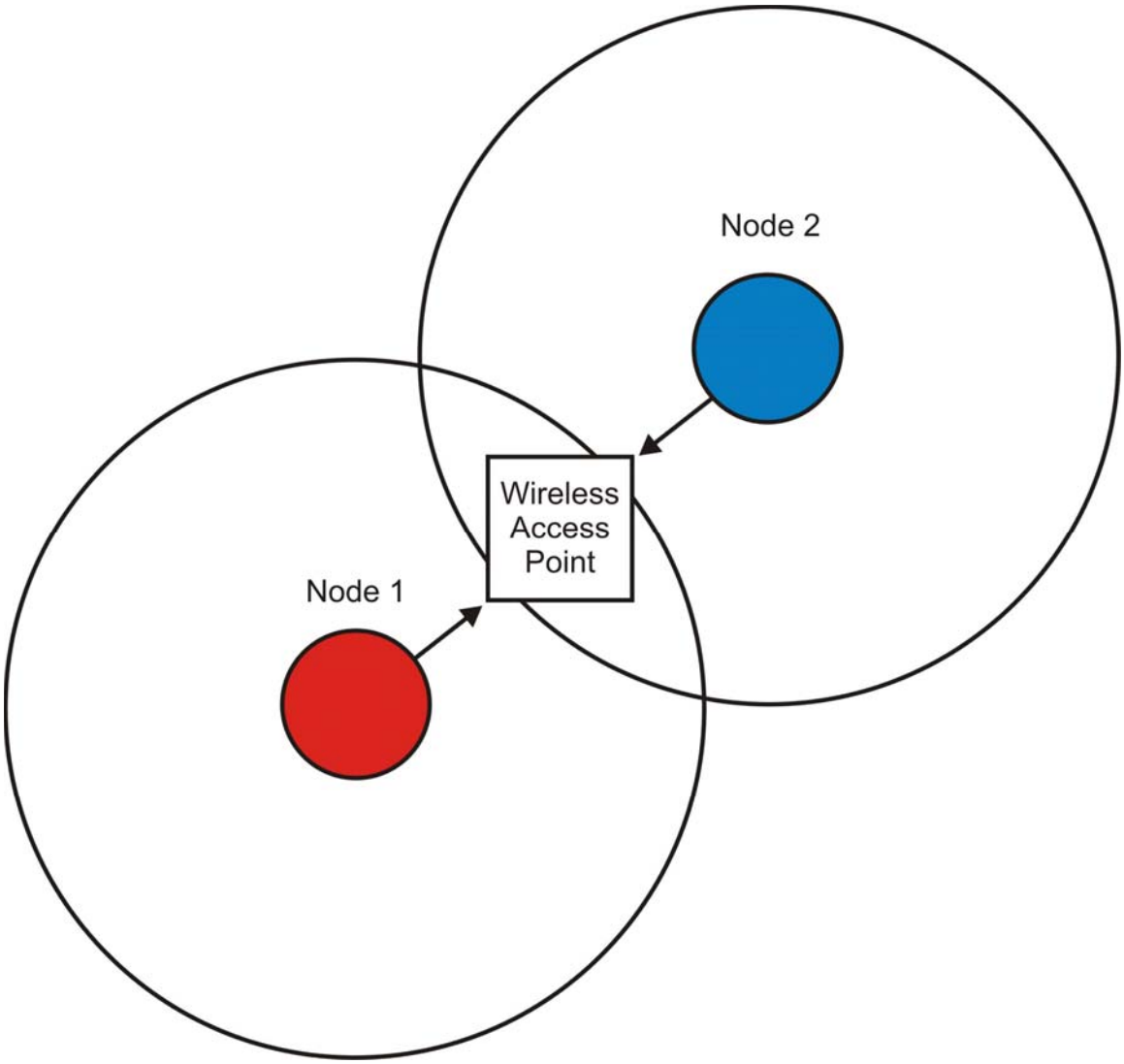

Figure 7—Hidden Node Problem

Both Nodes 1 and 2 have data to transmit at the same basic time. Neither node can sense that the other is transmitting data to the access point, so both nodes end up transmitting at the same time, negating the ability of the access point to successfully receive either. This problem is solved through the user of both carrier-sense and virtual carrier-sense methods, namely the Request To Send (RTS)/Clear To Send (CTS) method.

Both the RTS/CTS method and the standard MAC implementation without RTS/CTS are vulnerable to denial-of-service attacks.

Virtual Carrier Sense Attack—Virtual carrier-sense is the method described above where the use of RTS/CTS frames reserves the medium for a period of time for all users within transmission distance of both the access point and the user preparing to transmit. A discussion of this method is outside of the scope of this document. For more information, please see Section 9.2 of the ANSI/IEEE Standard 802.11, 1999 Edition.

The denial-of-service attack that is made possible through the use of the virtual carrier-sense mechanism in 802.11 concentrates on the Network Allocation Vector (NAV), which is a value transmitted in both the RTS and CTS packets. This field contains the duration necessary to complete the entire transaction on both the part of the user and the access point. The attack here is simple; the duration field has a maximum value of 32767, or 32.767 milliseconds. The attacker would necessarily have to have access to the network to employ this attack. Once access has been gained, the attacker could simply transmit RTS packets with the NAV value set to its maximum. In order for the attacker to maintain this attack and shut down the entire network, the attacker would have to transmit 30.5 packets per second. This is a relatively small duty cycle compared to the other denial-of-service attacks that will be covered in this section.

Unfortunately for the attacker, this attack is not terribly feasible for a variety of reasons. First, the attacker would have to have access to the 802.11 network stack in order to actually set this value, as this value is set in the firmware of a COTS 802.11 radio. Second, it has been found that most CTS 802.11 radios actually incorrectly implement the NAV functionality,[4] ignoring the duration field altogether. Thus, for the time being, this attack has no real impact on public safety. In the future, however, this attack will be considered a threat. This is due to the fact that if the Quality of Service (QoS) mechanisms being discussed in 802.11e are to be implemented, adherence to the NAV will be critical.

Management Attacks—Management denial-of-service attacks focus on the management frames that are used to manage an 802.11 network. These frames, for a DoS attack, typically consist of disassociation and deauthentication frames. These attacks are also known as identity attacks.

Brute Force Attacks—There is an inherent amount of trust required to successfully deploy an 802.11 network. One aspect of that trust is with respect to the time windows, or interframe spaces (IFS), defined by the standards that are used to determine carrier sense for transmission.

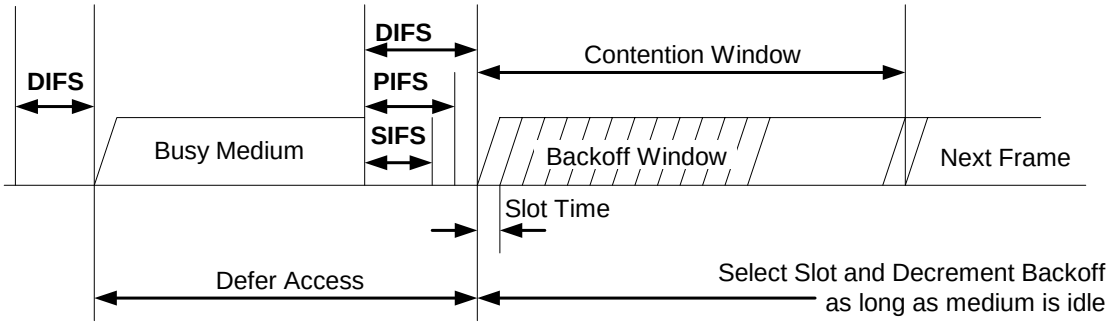

Figure 8—Interframe Space Relationships

[4] *802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions* by Bellardo and Savage.

Some quick definitions:

- SIFS—short interframe space—This spacing is used as a spacer between transmissions for a continuous session. For example, transmission of data that requires an ACK will have a SIFS spacing between the data transmission and the ACK transmission.
- PIFS—PCF interframe space—The PIFS is used in stations running PCF. Due to the lack of wide deployment, attacks against PIFS are out of the scope of this document.
- DIFS—DCF interframe space—The DIFS is used by devices as a timer to sense whether or not a channel is idle or not. If a device that has data to transmit senses that the channel is idle for DIFS time, it starts counting down in its random backoff window (described below). Once the countdown reaches zero, if the channel is still clear, the device will initiate its transmission.
- Random Backoff Window—This is used to manage multiple devices that have data to transmit at the same time. For example, if three devices were all waiting for the channel to go idle and they all waited DIFS time once the channel went idle and then transmitted, there would be a collision. By requiring that each device have a random backoff timer that must countdown prior to transmission, the chances of a collision are reduced.

The attack against the interframe space relationships is simple. Using 802.11b as an example, SIFS is stated to be 10μs. Because every transmitting node must wait at least SIFS time prior to transmission, an attacker could tie up the channel simply by transmitting every 10μs. This is the shortest spacing to effectively deny service to all devices on the network. This number could be as large as 50μs which is the DIFS time.

There are two main problems with this kind of attack. First, the duty cycle for maintaining such an attack will range from 20,000–100,000 packets per second. This will cause the first problem, which is rapid battery drain if the device is portable. The second is that with this type of duty cycle, it will make it easier for public safety to geolocate the source of the jamming, where as an aperiodic attack with a greater duration between transmissions would be much more difficult to locate.

This attack would prove devastating for public safety users; however, due to the nature of the attack, it is not terribly feasible. First, in order for an attacker to mount this type of attack, they would have to acquire and program specialized equipment, which while possible, is not trivial. Next, the attacker would have to ruggedize the platform for use in the field, in addition to supplying battery power.

Distributed DoS Attacks—Distributed denial-of-service attacks are a tool for attackers to accomplish two primary purposes: first, it enables an attacker to physically distribute the attack, making it more difficult for public safety users to triangulate the source of an attack, as there are more targets, and second, it enables the attacker to maximize the resources available to each attack device by splitting the attack amongst all of the devices employed in

an attack. This can effectively extend the duration of an attack due to battery power conservation. While no examples of this type of attack having been implemented have been found, this does not mean that they are not possible. For example, though many of the denial-of-service attacks described in this guide are infeasible for an attacker to implement today, distributing a series of PDAs with 802.11 cards running a disassociation attack is feasible.

3-2. Security Auditing

Description

The advent of wireless technology provides justice agencies a new flexibility in data and voice communications. Although radio, cellular systems have been deployed in a variety of justice agencies for many years, the rapidly expanding 802.1x series of 2.4GHz and 5.3 GHz devices provides a tempting low-cost option for many small- to medium-sized agencies.

The temptation to rapidly deploy wireless technology throughout the organization is high. Organizations need to resist the temptation to deploy this technology until a security plan is established, as security of wireless technology has unique issues that must be addressed before it can be considered for deployment. Part of an effective deployment of wireless technology involves an ongoing and comprehensive security audit. This section will address the auditing issues unique to wireless deployments, deferring normal auditing practices to the previous security publication issued by the Global Security Working Group entitled *Applying Security Practices to Justice Information Sharing*.

Purpose

When used in conjunction with other standard security practices, an effective audit can discover and correct many security flaws before they become security compromises. A management review of the audit results can assist an organization in maintaining a reliable and effective wireless communications infrastructure that will serve the business needs of an organization over time and be flexible enough to adapt to changes in the technology and security landscape.

Vulnerability Issues Unique to Wireless Networks

Unlike wired networks within the organization, the transmission medium of wireless networks often extends beyond the physical boundaries of the organization. In the case of 802.1x networks, they use an access point where wireless clients can communicate with the information infrastructure when they are in proximity to the access point. The defaults on many of these access points are set to allow any wireless client to connect without additional authorization or authentication. Person(s) outside of the agency may be able to eavesdrop on communications or make unauthorized connections to the access point. Due to the range limitations of the access point, wireless attacks are "active" in nature, requiring the attacker to be in proximity to the access point to be able to launch the attack. The use of directional antennas by intruders can extend the effective range of an access point for a considerable distance and must be taken into account when assessing vulnerability.

Wireless access points sold at the consumer level are not normally enabled with strong encryption. The Wireless Equivalent Privacy (WEP) capability loaded on most consumer-level wireless access points is vulnerable to attacks that allow an unauthorized user to discover the WEP key and access the access point. Even the new 802.11i security standard using Wireless

Protected Access (WPA)[5] is susceptible to a key attack if the key length is not random or of sufficient length.

Wireless networks work in two different modes, "peer-to-peer" mode (sometimes referred to as "ad hoc" mode) and "infrastructure mode." Peer-to-peer communications are initiated between two clients directly without wireless access point. If allowed, peer-to-peer communications are only secured at the device level and bypass other network security. This can allow sensitive information stored on remote devices to be compromised outside of the control of network security administrators and without detection. Additionally, unrestricted peer-to-peer connections can import viruses and Trojan programs into the infrastructure without screening by network security appliances and software.

In infrastructure mode, the client connects to the wireless access point by means of a four-way handshake. In the default configuration, many access points do not require authentication or authorization for a connection. Once connected to the access point, the client has access to the network infrastructure available to that access point. The connection to the access point is not normally filtered by Intrusion Detection Systems (IDS) or firewall appliances until after the connection is made and the access point compromised. If the access point is attached behind the firewall, the wired network may also be compromised at that time.

Because wireless access points are available to any client within range, they are also susceptible to denial-of-service attacks from remote transmitters. A transmitter set to the proper frequencies and placed within range of an access point can be triggered remotely to flood the access point with connection requests effectively denying access to legitimate clients. These attacks are active in nature and require the transmitter to transmit within the range of the access point.

Wireless networks present unique security challenges for an organization deploying them. This section outlines some of the risks associated with wireless access points and clients within an organization and is included herein to lay the foundation for appropriate auditing protocols designed to manage the risks and provide good wireless security for the organization.

Wireless access points are identified over the wireless channel by their Service Set ID (SSID) designation and their Media Access Control (MAC) address. Most consumer level access points use default SSIDs that can provide an intruder with insight into the type of system they are attacking. The SSID and MAC are normally transmitted in "broadcast" mode to announce their availability to clients within range and can easily be detected by clients using scanning programs like "Netstumbler" that are designed to find access points. The default for most consumer level wireless access points has the broadcast mode set to "on." Some scanner programs allow the client to modify its MAC address when attempting to connect to the access point.

[5] <http://www.wifinetnews.com/archives/002453.html>.

Employees can set up "rogue" access points within the infrastructure. These unauthorized access points can be connected to the wired network in an office or cubicle and can jeopardize the enterprise by allowing direct and unmonitored access to the organization's information infrastructure without the knowledge of the system administrator. Employees who are not trained in security practices may not understand the seriousness of their actions when setting up rogue access points inside the infrastructure.

Best Practices

Many of the aforementioned vulnerabilities can be addressed through a well-planned and effective auditing strategy within the organization. This section will address areas that should be closely monitored and audited to minimize the risk of compromise over a wireless connection. A good audit will look at multiple levels of the security infrastructure to insure that a good security posture is maintained throughout the organization. These areas are *Security Policy, Physical Security, Personnel*, and *Technical Infrastructure*. Security audits should be conducted regularly and the results documented in a comprehensive report to management with recommendations for improvements.

Security Policy

The first step in a good audit protocol is to evaluate the business need for wireless access to the infrastructure. The security risks must be weighed against the business need, and a strong security policy must be in place describing how and when wireless technology should be deployed within the organization. The audit should establish that such a policy exists and that the policy is clear and concise on how and when wireless technology is to be deployed and used within the organization.

The policy should also address how the infrastructure will be maintained and outline protocols for adding new technology and personnel to the existing infrastructure. Rogue access points and wireless devices should be prohibited by policy.

Wireless configurations must be documented and regularly backed up. There should be a documented policy for regular backups and change control that allows for a rollback to a previous configuration if network configuration changes have unforeseen consequences. Additionally, the policies should consider disaster recovery protocols should the network be damaged or destroyed by a natural or other disaster. A good audit should check for the existence and effectiveness of these policies.

Ongoing risk assessment procedures should be in place to identify new and emerging threats to the wireless infrastructure and to look into cost-effective means to mitigate those risks. Monitoring of security-related publications and alerts should be a matter of policy to provide early warning about new and developing threats, allowing systems administrators to maintain a proactive security posture and adapt to changing threats on a timely basis.

Procedures and policies should be in place to address the use of mobile devices and the security of those devices both inside and outside the physical plant. Policies for access to open networks should be developed and designed to reduce the risk of compromise of a

client device while it is in the field. The procedures should address the proper reporting and protocols for remotely disabling a compromised client.

A clear policy should be in place to ensure that encryption keys and system passwords are changed regularly and that pass phrases used to generate encryption keys are random and consist of at least 20 characters to prevent the generation of weak WEP or WPA keys.

Physical Security

The physical location of access points is part of a good wireless security posture and should be part of any security audit. Wireless access points should be places near the center of buildings and away from exterior walls and windows to limit the broadcast range outside of the physical plant. Monitoring of the range of the access point should be conducted regularly to insure that outsiders cannot monitor transactions on the wireless network without being observed and detected. Administrators should establish the effective perimeter range of their access points through the use of directional antennas.

The wireless access point must be physically secured in its position to prevent movement and tampering from within the organization. Cable runs connecting the wireless access point to the wired infrastructure should be enclosed and protected against damage and tampering.

Wireless clients should be checked to make sure they include internal identification and antitheft measures. Cable locks and other physical security devices should be provided to employees who travel to reduce the chance of physical theft of a remote device.

Personnel

The audit should insure that the organization has a program of employee security awareness training that addresses the use of wireless devices both inside and outside the organization. Employees should have clear guidelines on how to utilize their wireless devices and how to safeguard them against unauthorized access or physical theft.

Employees should be instructed in the use of personal firewalls and antivirus software in the field and shown how to properly utilize the software to protect their wireless devices.

Employees should be instructed on how to turn their wireless devices off when not in use in the field to prevent unauthorized peer-to-peer connections.

Technical Infrastructure

Patch control protocols should be in place. The audit should verify that the organization has a policy and is proactive in maintaining the wireless network with the latest security patches available from the manufacturer. Many systems are compromised by exploitation of documented vulnerabilities for which patches were available but not installed on a timely basis.

The audit should assess whether or not the organization has implemented a good client-to-base station authorization and authentication. Wireless networks should not be left open to any client that happens by. The organization should have implemented features like WEP, WPA, and/or TKIP (Temporal Key Integrity Protocol), as well as MAC address access control lists (ACLs) in access points to help prevent unauthorized clients from accessing the wireless access point. The recording and screening of MAC ACLs becomes ungainly in large wireless networks but should work well in small networks.

The client configuration controls should be locked by the system administrator to insure that the user cannot tamper with the security settings on the wireless device.

Auditors should check to insure that the access point is attached outside of the firewall and that any communication emanating from the access point must pass through the firewall and some type of user authentication server, as well as being monitored by an Intrusion Detection System (IDS) before access to the internal infrastructure is granted. The use of a properly configured and well-maintained Remote Authentication Dial-In User Service (RADIUS) combined with a Virtual Private Network (VPN) can help block unauthorized access through the wireless access point.

Auditors should check to see that SSID "broadcast" is disabled on the system and that default SSIDs are changed. Names for SSIDs should not reflect the nature of the systems they represent. WEP, WPA, and/or TKIP should be enabled, and legitimate clients should be preconfigured with the appropriate SSID and encryption keys before they are delivered to the end user.

Auditors should ensure that all connections to the wireless access point are logged and that logs are analyzed frequently for unauthorized attempts against the system.

Auditors should check to make sure the system administrator regularly scans for "rogue" access points within the infrastructure. Removal and reporting guidelines should be in place in the event a "rogue" access point is detected.

Auditors should conduct periodic penetration testing against the wireless network using common attack tools as a means of identifying vulnerabilities and correcting them before the network is compromised by outsiders.

References

- Washington State Information Technology Security Policy Audit Standards, <http://www.sao.wa.gov/StateGovernment/ITSecurity/ITStandards.htm>.

- NIST: *Security Self-Assessment Guide for Information Technology Systems*, <http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf>.

3-3. Risk Management

Description

Every organization has a mission. In this digital era, as organizations use automated information technology (IT) systems to process their information for better support of their missions, risk management plays a critical role in protecting an organization's information assets, and therefore its mission, from IT-related risk.

An effective risk management process is an important component of a successful IT security program. The principal goal of an organization's risk management process should be to protect the organization and its ability to perform their mission, not just its IT assets. Therefore, the risk management process should not be treated primarily as a technical function carried out by the IT experts who operate and manage the IT system but as an essential management function of the organization.

Organizations using wireless technologies should be aware that maintaining a secure wireless network is an ongoing process that requires greater effort than that required for other networks and systems. Moreover, it is important that organizations assess risks more frequently and test and evaluate system security controls when wireless technologies are deployed.

In particular, organizations should not undertake wireless deployment for essential operations until they have examined and can acceptably manage and mitigate the risks to their information, system operations, and continuity of essential operations. Organizations should perform a risk assessment and develop a security policy before purchasing wireless technologies, because their unique security requirements will determine which products should be considered for purchase.

Purpose

Risk is the net negative impact of the exercise of a vulnerability, considering both the probability and the impact of occurrence. Risk management is the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level. Organizations should develop an effective risk management program, containing both the definitions and the practical guidance necessary for assessing and mitigating risks identified within IT systems. Once a risk management framework is in place, cost-effective security controls can be used to mitigate risk for the better protection of mission-critical information and the IT systems that process, store, and carry this information.

Principles

- ❑ Reduce risk to an acceptable level.
- ❑ Assume that external systems are not secure.

- Identify potential trade-offs between reducing risk and increased costs and decrease in other aspects of operational effectiveness.
- Implement tailored system security measures to meet organizational security.
- Protect information while being processed, in transit, and in storage.
- Consider custom products to achieve adequate security.
- Protect against all likely classes of attacks.

Policies

A comprehensive risk management program should include a risk assessment policy that empowers IT staff and delegated third parties to perform periodic information security risk assessments for the purpose of determining areas of vulnerability and to initiate appropriate remediation.

Best Practices

Risk is the possibility of something adverse happening. Risk management is the process of assessing risk, taking steps to reduce risk to an acceptable level, and maintaining that level of risk. Risk management requires the analysis of risk relative to potential benefits, consideration of alternatives and, finally, implementation of what management determines to be the best course of action. Risk management consists of two primary and one underlying activity. Risk assessment and risk mitigation are the primary activities, and uncertainty analysis is the underlying one. An organization should consider the following when assessing risks.

Risk Assessment

Risk assessment, the process of analyzing and interpreting risk, is comprised of three basic activities:

- **Determine the Assessment's Scope and Methodology**. The first step in assessing risk is to identify the system under consideration, the part of the system that will be analyzed, and the analytical method, including its level of detail and formality.
- **Collecting and Analyzing Data**. The many different components of risk should be examined. This examination normally includes gathering data about the threatened area and synthesizing and analyzing the information to make it useful. The types of areas are:
  - *Asset Valuation*. These include the information, software, personnel, hardware, and physical assets (such as the computer facility). The value of an asset consists of its intrinsic value and the near-term impacts and long-term consequences of its compromise.

- *Consequence Assessment*. The consequence assessment estimates the degree of harm or loss that could occur.

- *Threat Identification*. A threat is an entity or event with the potential to harm the system. Typical threats are errors, fraud, disgruntled employees, fires, water damage, hackers, and viruses. Threats should be identified and analyzed to determine the likelihood of their occurrence and their potential to harm assets.

- *Safeguard Analysis*. Safeguard analysis should include an examination of the effectiveness of the existing security measures.

- *Vulnerability Analysis*. A vulnerability is a condition or weakness in (or absence of) security procedures, technical controls, physical controls, or other controls that could be exploited by a threat.

- *Likelihood Assessment*. Likelihood is an estimation of the frequency or chance of a threat happening. A likelihood assessment considers the presence, tenacity, and strengths of threats and the effectiveness of safeguards (or presence of vulnerabilities).

❑ **Interpreting Risk Assessment Results**. The risk assessment must produce a meaningful output that reflects what is truly important to the organization. The risk assessment is used to support two related functions—the acceptance of risk and the selection of cost-effective controls.

Risk Mitigation

Risk mitigation involves the selection and implementation of security controls to reduce risk to a level acceptable to management. Although there is flexibility in how risk assessment is conducted, the process of risk mitigation has greater flexibility than the sequence of events conducted in a risk assessment. The following activities are discussed in a specific sequence; however, they need not be performed in that sequence.

❑ **Select Safeguards**. The identification of appropriate controls is a primary function of computer security risk management. In selecting appropriate controls, the following factors should be considered:

- Organizational policy, legislation, and regulation.

- Safety, reliability, and quality requirements.

- System performance requirements.

- Timeliness, accuracy, and completeness requirements.

- The life-cycle costs of security measures.

- Technical requirements.
- Cultural constraints.

- **Accept Residual Risk**. Management needs to decide if the operation of the IT system is acceptable, given the kind and severity of remaining risks. The acceptance of risk is closely linked with the authorization to use an IT system, often called accreditation. (Accreditation is the acceptance of risk by management, resulting in a formal approval for the system to remain or become operational.)

- **Implementing Controls and Monitoring Effectiveness.** The safeguards selected need to be effectively implemented. To continue to be effective, risk management needs to be an ongoing process. This requires a periodic assessment and improvement of safeguards and reanalysis of risks.

Uncertainty Analysis

Risk management must often rely on speculation, best guesses, incomplete data, and many unproven assumptions. An uncertainty analysis should be performed and documented so that the risk management results can be used knowledgeably. There are two primary sources of uncertainty in the risk management process:

- A lack of confidence or precision in the risk management model or methodology.

- A lack of sufficient information to determine the exact value of the elements of the risk model, such as threat frequency, safeguard effectiveness, or consequences.

Incident Response

The use of an incident response team and an incident response plan are the same as would be deployed in a security incident involving a wired network. Wireless networks differ in that the perpetrator must be within range of the wireless access point to perpetrate the attack. That range may be deceptive in that the use of a wireless antenna can increase the effective range of network communication considerably. In the case of 802.1X networks, this range can be up to a mile or more from the access point. Given this limitation of the attacker, a good wireless incident response plan should provide for a physical proximity check within the effective range of the wireless access point, looking for suspicious subjects or vehicles, particularly those deploying directional antennae.

In any response to a wireless attack, the response team must have a separate channel for communications besides the channel under attack. This may involve cellular networks, wired networks (not tied to the network under attack), encrypted radio systems, or landline telephone systems.
Preestablished response protocols should be implemented and communications minimized in case other communications infrastructures are also under attack. Preplanned response

protocols may help avoid confusion and prevent the suspect from intercepting communications of the response team.

One of the early decisions in a response plan is whether or not the wireless access point should be shut down immediately upon discovery of the attack or if it should be left open and monitored in an attempt to identify the intruder. State and federal laws notwithstanding, this is also a business decision of the affected agency. It may be better to shut down the wireless access point and disrupt normal business operations rather than risk further system compromise. The trade-off in this is that the response team may not be able to locate the intruder and chance another attempt at a later date.

Wireless network disruptions will normally require the attacker to transmit a communications signal. It is possible to detect and triangulate the signal with the proper equipment. Radio detection equipment is not normally available to the average criminal justice agency, so the response plan should identify what equipment will be required and where that equipment can be obtained in the event of an incident. Having a predesignated source for detection equipment and expertise can make it possible to physically locate the attacker.

Direction-finding equipment and techniques will not work against an attacker who is monitoring signals emanating from the wireless network. In that case, the physical search may be the only chance to identify the physical location of the intruder. Knowing the reception range and "blind spots" for a particular access point can go a long way to helping the response team narrow their search area.

Another technique that may be employed against an attack is to physically move the access point in multiple directions from its normal base and see if there is any particular area where the signal to the intruder is interrupted. When done in conjunction with perimeter monitoring, it may be possible to force the intruder to move to locations where he/she can receive a better signal. Movements on the perimeter corresponding to movements of the access point should be noted and investigated.

As with any security incident, there should be a formal debriefing after the event. All response team members and others affected by the event should have the opportunity to review the event and analyze it with an eye to the development of better response guidelines and improved security.

References

- Stoneburner, Gary, Goguen, Alice, and Feringa, Alexis, *Risk Management Guide for Information Technology Systems*, National Institute of Standards and Technology, Publication 800-30, http://www.csrc.nist.gov/publications/nistpubs/index.html.

- Karygiannis, Tom, and Owens, Les, *Wireless Network Security: 802.11, Bluetooth and Handheld Devices*, National Institute of Standards and Technology, Publication 800-48, http://csrc.nist.gov/publications/nistpubs/index.html.

- International Standard, ISO/IEC 17799, Information Technology—Code of Practice for Information Security Management.

- Control Objectives for Information and Related Technology (COBIT).

3-4. Disaster Recovery and Business Continuity

Description

A disaster is any event that can cause a significant disruption in operational or computer processing capabilities for a period of time. Disasters can include the loss of a critical file, the rapid spread of a virus, a denial-of-service attack, the loss of a network segment or critical link, or loss of an entire facility or personnel from a fire or bomb. Although the probability of a major disaster is remote, the consequences of an occurrence could be catastrophic, both in terms of operational impact and public image. Disasters have an uncanny habit of occurring at the most inconvenient times, damaging equipment and materials one can least afford to lose.

Disaster recovery focuses on handling the immediate emergency, whereas business continuity takes effect after a disaster and focuses on getting the critical business functions operational and eventually restored to full capabilities. Together, they cover what to do, beginning with the emergency response; continuing through crisis management, prioritized business operations recovery, and detailed recovery; and ending with full business restoration. Knowing what needs to be done before, during, and after a disaster can prevent panic, reduce the extent of the damage, and help in a coordinated recovery effort.

Purpose

The purposes of disaster recovery and business continuity plans are to prevent serious impact, to avoid disruption of services, and to coordinate the recovery tasks so that normal business operations may resume as quickly as possible. Plans are different from one organization to another because risks vary widely, as do the organizational priorities and goals. There is also a wide range of alternatives available in both method and technology. These alternatives vary in rigor (i.e., the security assurance level or the degree of protection that they provide) and cost. In general, rigor and cost are directly proportional—the more rigorous a method, the more it costs. The information system owner should look to methods that provide as high a level of assurance as possible within cost constraints.

Principles

- The amount of time and effort put into a plan should reflect the value of the information or service provided by the organization and the amount of effort required if the system had to be rebuilt from scratch. It is normally much more cost-effective to prevent or minimize damage than to repair it after the fact.

- The disaster recovery plan should address procedures such as employee safety, emergency services notifications, family and employee notifications, operational communications, identification of key personnel, emergency authorizations, power and hardware recovery, media backup and recovery, and maintaining event logs.

- The business continuity portion should address procedures such as manpower recovery, alternative business processing methods, administration and operations, budget for replacements and/or insurance, customer service, identification of key vendors, office supplies, public affairs, and premise recovery. Nontechnical management should own and control the business continuity plan in order to ensure proper funding.

- The plan should be practiced and tested. A failed test of the plan still provides valuable information about the organization and where changes should be made. It is also an invaluable tool to train personnel on how they should react in an emergency.

- No matter how good a plan is when first finished, it will almost immediately become out of date. Constant review and update is required to keep the plan pertinent and useful.

Policies

Once an organization decides on an approach for disaster recovery and business continuity, the policies for that approach should be documented. The guideline ensures the consistent and comprehensive application of disaster recovery throughout the information enterprise. The guideline should identify scope, methods, standards, and organizational and individual responsibilities. The reader may refer to the following documents for examples of disaster recovery and business continuity policy statements:

- Massachusetts Institute of Technology, Emergency Response System, <http://mit.edu>, and search on "emergency response system."

- Massachusetts Institute of Technology, Business Continuity Plan, <http://web.mit.edu/security/www/pubplan.htm>.

Best Practices

Disaster Recovery Team—A team needs to be assembled that will respond in the event of a disaster. This team should include a member of management, members of the technology unit that will perform the assessment and recovery, representatives from facilities, and members from the information user community to determine what level of recovery is needed and to verify when recovery is complete. The team takes an active part in developing the plan and carrying it out in the event of a disaster.

Threat/Risk Assessment—A threat is anything that can adversely affect the operation of an organization; i.e., fire, natural disaster, virus, bomb, and strike. The threat assessment is the process of formally identifying the nature of the threats and degree of damage each can do to an organization. This includes damage to all assets, including, but not limited to, personnel, facilities, computer systems, and reputation.

The risk assessment takes the threats identified for the organization, assesses the adequacy of the controls in place, determines the expected loss for each threat, and then establishes the degree of acceptability to system operations. It will also recommend changes to controls to improve the current security protection. Steps include the following:

- Assess the current computing and communications environment, including personnel practices, physical security, operating procedures, backup plans, systems development and maintenance, database security, data and voice communications security, systems security and access control, application controls, security administration, insurance, and personal computers. Inventory all equipment, and make a list of the vendors.

- Define all critical information needed to operate. Retention schedules, federal mandates, state law, or business needs will define this subset of data. Note the location of all critical information. Depending on the criticality of the information, either backups or safe storage containers should be considered. Store backups of critical information off-site.

- Define critical personnel, equipment, facilities, and single points of failure. Try for redundancy, or make arrangements to quickly replace these assets. Potential sources of failure include network, hardware, software, malicious attack, physical damage to the facility, and loss of personnel.

- Assess the insurance needs of the organization and the budget required to purchase replacements.

- Assess any dependencies on critical partners. Utilities, vendors, customers, and building partners are examples.

- Assess the risk of denial-of-service attacks to wireless systems. These attacks can be difficult and time consuming to track and stop.

Business Impact Analysis (BIA)—Complete a BIA to identify the critical processes and functions of the organization.

- Set priorities for restoration based on the overall impact by looking at the interdependencies of the departments within the organization.

- Determine maximum acceptable losses, and define the window of time available to resume operations. The analysis will then define the restoration timeline and the possible need to use alternate facilities in different scenarios.

- List resources required to restore those critical functions identified in the BIA. This should include the hardware, software, documentation, facilities, personnel, and outside support needed for recovery. Different strategies could be formed for short-term, intermediate-term, and long-term outages.

Mitigation of Risks—Mitigate risks identified in the risk assessment by implementing new procedures and providing redundancy wherever possible. This includes cross-training personnel on other job duties as well as making plans for extra hardware and backup software.

Store electronic media in protective jackets or media boxes. Consider purchasing data safes (fire-resistant safes, specially designed to protect magnetic media from damage caused by magnetism, fire, heat, water, and airborne contaminants, such as smoke and dust). A water vacuum or roll of plastic can be extremely useful with a water leak or malfunctioning sprinkler system.

Power is critical to computing and wireless environments. It is common to provide protection of computing equipment through UPS systems, battery systems, connection to two different power grids, and the use of backup generators.

Hardware Redundancy—The following techniques are used to provide hardware redundancy:

- **Disk Mirroring**—Disk mirroring is the duplication of data from one hard disk to another. Mirrored drives operate in tandem, constantly storing and updating the same files on each hard disk. Should one disk fail, the file server issues an alert and continues operating. Should the controller fail, access to either disk may be denied.

- **Disk Duplexing**—This is similar to disk mirroring except each drive has its own controller circuitry. Should one disk or controller fail, the file server issues an alert and continues operating.

- **Disk Arrays**—These enable the administrator to replace a failed drive while the server is still running, and users can continue operating. The system automatically copies redundant data on the file server to the new disk.

- **Hot Backup**—Two file servers operate in tandem, and data is duplicated on the hard disks of the two servers. This is like disk mirroring but is across two servers instead of one. If one server fails, the other automatically assumes all operations without any outage.

- **Cold Site**—A cold site is an emergency facility containing a heating, ventilating, and air conditioning (HVAC) system and cabling, but not computers. When outsourcing, evaluate providers on high availability and disaster tolerance. Such arrangements may be informal (as a reciprocal agreement) or formal (a separate recovery site or a contract with a third-party provider). Cold sites are generally cheaper than hot sites. They should be a reasonable distance away from the main facility to prevent the same disaster from destroying its capabilities as well as the primary facility. Also, they should not be overextended in the number of organizations for which they provide this service. In a massive disaster, all of the organizations will want the facility at the same time.

- **Hot Site**—A hot site is an off-site facility contracted to have compatible systems ready to restore an organization's backups and run them as if in their own facility. Hot sites contain computers, backup data, and communication equipment. Written agreements should be signed if contracting with another unit for alternate processing of critical systems in the event of a disaster. Again, they should be a reasonable distance away from the main facility to prevent the same disaster from destroying its capabilities as well as those of the primary facility. They should not be overextended in the number of organizations for which they provide this service.

Software Redundancy—There are several different types of data backups. Determine the level and frequency of backups (e.g., daily incremental backups with weekly full backups). Consideration should be given to using more than one technique to better ensure the information gets backed up promptly.

- **Full Backups**—All files on a hard disk should be copied to a tape or other storage medium. These are used for total system recovery and are often done once a week.

- **Differential Backups**—These are done only for the files that have been changed or added since the last full backup. Earlier versions of these files will be replaced in differential backups and are often done nightly.

- **Incremental Backups**—These are completed only for the files that have changed or been added to a system since the last backup and are often done whenever work is finished on the computer. These backups use less storage space and are faster to run. They are generally used to aid in the recovery of old versions of files and the restoration of file integrity when files become corrupted.

- **Off-site Storage**—At least two copies of server backups should be made. One copy is kept on-site to restore files. The second backup should be stored off-site, or an electronic tape vaulting service should be used. A mutual agreement should be signed with the off-site facility to ensure that it provides the security needed to protect the information at the same level as that provided by the primary facility. Fire protection, air conditioning, heating, moisture control, availability, and other security factors should be considered. Regularly scheduled delivery of the backup media will help ensure the backups are available when needed. Backup and recovery functions should be limited to the administrator and alternate.

Plan Development—Procedures should be documented for various types of disasters, such as fire, flood, extended power outages, bomb threats, chemical spills, and loss of personnel. This phase also includes the implementation of changes to current procedures to help prevent disasters and to support recovery strategies and vendor negotiations with recovery services or off-site storage. Individual responsibilities for members of the Disaster Recovery Team should be defined, and recovery standards are also developed at this stage.

Planning should include specific procedures to restore wireless mobile data systems. Lack of power is the leading cause of failure of wireless systems, both private and commercial in a disaster. Wide area hot spot IEEE 802.11 type systems will need special attention in the plan. It is unlikely that the access points will have extended backup power available. Plans should address the loss of these systems in an extended power outage.

The first priority should always be the safety of personnel. Escape routes and evacuation procedures should be documented and made clear to all personnel, and the availability of adequate medical and first-aid supplies should be ensured.

Testing the Plan—Practice and test the plan. Set up a mock disaster, and work through the plan to discover its weaknesses and make necessary changes. Routinely perform restorations from the various kinds of backups (full, incremental, or differential) to ensure they will work when needed. Plans tested less than once a year will probably not support critical business requirements.

Plan Maintenance—Regularly review the plan once it is complete. The information within the plan constantly changes. Critical functions, telephone numbers, and job duties change. Even organizational priorities and goals may change.

References

- National Institute of Standards and Technology, *Domestic Disaster Recovery Plan for PCs, OIS, and Small VS Systems*, Gaithersburg, MD: U.S. Department of State, Washington, DC, <http://www.ntis.gov/search/product.asp?ABBR=PB90265240&starDB=GRAHIST>.

- Federal Emergency Management Agency, *Emergency Management Guide for Business and Industry: A Step-by-Step Approach to Emergency Planning, Response, and Recovery for Companies of All Sizes*, Washington, DC: FEMA, 1993. Order from: Publications Distribution Center, Post Office Box 2012, Jessup, MD 20794. Telephone: (800) 480-2520.

- National Archives and Records Administration, Office of Records Administration, *Vital Records and Records Disaster Mitigation and Recovery,* College Park, MD: NARA, 1996. Available from: Publications and Distribution Staff (NECD) RM. G-9, National Archives, Washington, DC.

Appendix A: Glossary of Security Acronyms and Terminology

AAMVA	American Association of Motor Vehicle Administrators
Acceptable Risk	A concern that is acceptable to responsible management, due to the cost and magnitude of implementing controls.
Access Control	Procedures and controls that limit or detect access to critical information resources. This can be accomplished through software, biometrics devices, or physical access to a controlled space. The ability of a system to grant, limit, or deny access to specific data, applications, or resources for specific users, devices, or systems.
Access Control Policy	The set of rules that define the conditions under which an access may take place.
Access Level	The hierarchical security level used to identify the sensitivity of data and the clearance or authorization of users.
Accountability	The security objective that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports nonrepudiation, deterrence, fault isolation, intrusion detection, and after-action recovery and legal action.
ACL	Access Control List
ACLU	American Civil Liberties Union
AEA	Advanced Encryption Algorithm
AES	Advanced Encryption Standard
AFIS	Automated Fingerprint Identification System

AIS	Automated Information System
Algorithms	Complex mathematical formulae that are one component of encryption.
Analog	A signal that may vary continuously over a specific range of values.
Antenna	A device (usually metallic) for radiating or receiving radio waves.
Anonymizer	Anonymizer is a gateway to keep Web surfing anonymous and preserve privacy online when surfing the Web, sending e-mail, or posting to a newsgroup. By using the anonymizer, any information and IP addresses that are collected will be false information. By hiding an IP address, one can eliminate the possibility of a DoS attack. See <http://www.anonymizer.com>.
ANSI	American National Standards Institute
Armored Virus	An armored virus tries to prevent analysts from examining its code. The virus may use methods to make tracing, disassembling, and reverse engineering its code more difficult.
APB	Advisory Policy Board
ASCII	American Standard Code for Information Interchange
Assurance	The grounds for confidence that an entity meets its security objectives.
Attack Detection and Prevention	The communications networks must be resistant to jamming; they must be capable of passive/active attack monitoring and defense deployment; they must be able to geolocate the source of an attack; and they must be capable of monitoring all functional aspects by authorized users/devices.
Audit	The independent examination of records and activities to ensure compliance with established controls, policy, and operational procedures and to recommend any indicated changes in controls, policy, or procedures.

Audit Trail	A chronological record of system activities that is sufficient to enable the reconstruction and examination of the sequence of environments and activities surrounding or leading to an operation, procedure, or event in a security-relevant transaction from inception to results.
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in a system.
Authorization	The granting or denying of access rights to a user, program, or process.
Authorized	A system entity or actor is granted the right, permission, or capability to access a system resource. See Authorization.
Availability	Timely, reliable access to data and information services for authorized users; protection against intentional or accidental attempts to perform unauthorized deletion of data or otherwise cause a denial-of-service on data.
Back Door	A feature built into a program by its designer which allows the designer special privileges that are denied to the normal users of the program. A back door in an EXE or COM program, for instance, could enable the designer to access special setup functions.
Backup	A duplicate copy of data made for archiving purposes or for protecting against data loss. A backup is considered secure only if it is stored away from the original.
Band	A well-defined range of wavelengths or frequencies.
Bandwidth	The range within a band of frequencies. A measure of the amount of information that can flow through a given point at any given time.
BIA	Business Impact Analysis
Binary	A numbering system based on twos (2s) rather than tens (10s). Each element has a digit value of either one (1) or zero (0) and is known as a bit.
Biometrics	Biometrics is the science and technology of measuring and statistically analyzing biological data. In information technology, biometrics usually refers to automated technologies for authenticating and verifying human body characteristics, such as fingerprints, eye retinas and irises, voice patterns, facial patterns, and hand measurements.

Bit	See Binary.
Brute Force Attack	An attack in which each possible key or password is attempted until the correct one is found.
C&A	Certification and Accreditation
CA	Certification Authority—an authority that issues and manages security credentials for a PKI.
CA Privacy Root Key	Cryptographic key known only to the CA. It is used to verify user or server certificate requests (digitally signed certificates).
CAPI	Cryptographic Application Programming Interface
Carnivore	The Internet surveillance system developed by the Federal Bureau of Investigation to monitor the electronic transmissions of criminal suspects.
CCITSE	Common Criteria for Information Technology Security Evaluation
CDL	Commercial Driver's License
CERT®	Computer Emergency Response Team—(1) The people who are responsible for coordinating the response to computer security incidents in an organization. (2) CERT® is one of the main agencies for Internet security formed by the Defense Advanced Research Projects Agency (DARPA) in 1988 to aid the Internet community in responding to computer security events, raise awareness of computer security issues, and conduct research aimed at improving security systems. See <http://www .cert.org> for more information.
CERT®/CC	CERT® Coordination Center
Certificate	In cryptography, an electronic document binding some pieces of information together, such as a user's identity and public key. Certifying Authorities (CAs) provide certificates.
Certificate Owner	The person that has access to use the certificate. This access could be protected by a password, a smart card, or other device.
CFR	Code of Federal Regulations

Channel	A band of frequencies of sufficient width to support a single radio communications path.
CHRI	Criminal History Record Information
CIO	Chief Information Officer—the highest-level person responsible for policy concerning information systems and telecommunications systems.
CIP	Critical Infrastructure Protection
Cipher	An alternative term for an encryption algorithm.
Ciphertext	Encrypted data
CIR	Centralized Information Repository
CIS	Center for Internet Security
CJIS	Criminal Justice Information Services
CKMS	Centralized Key Management System
Compromise	To access or disclose information without authorization
Confidentiality	Assurance that information is not disclosed to unauthorized persons, processes, or devices. Confidentiality covers data in storage, during processing, and while in transit.
Contingency Plan	A plan maintained for emergency response, backup operations, and post-disaster recovery for an AIS, to ensure availability of critical resources and to facilitate the continuity of operations in an emergency.
Cookies	Blocks of text placed in a file on a computer's hard disk. Web sites use cookies to identify users who revisit the site.
COTS	Commercial Off-the-Shelf
Countermeasure	Any action, device, procedure, technique, or other measure that reduces a system's vulnerability to a threat.
Coverage	The amount or percentage of area reached by a communications medium.
CPO	Chief Privacy Officer

Cracker	One who breaks security on an automated system.
CRL	Certificate Revocation List
CRT	Central Response Team
Cryptography	The art and science of using mathematics to secure information and create a high degree of trust in the electronic realm.
CSA	Computer Security Act of 1987
CSD	Computer Security Division
CSIRC	Computer Security Incident Response Capability—a set of policies and procedures defining security incidents and governing the actions to be taken when they occur.
CSIRTs	Computer Security Incident Response Teams
CSMA/CD	Carrier Sense Multiple Access/Collision Detect
CSO	Central Security Officer
CSPs	Critical Security Perimeters—security-related information (e.g., cryptographic keys, authentication data such as passwords and PINs) appearing in plaintext or an otherwise unprotected form and whose disclosure or modification can compromise the security of a cryptographic module or the security of the information protected by the module.
CSRC	Computer Security Resource Center
CSS	Card Scanning Service
CTA	Control Terminal Agency
CTO	Control Terminal Officer
DAC	Discretionary Access Control
DAC	Data Authentication Code—also known as a Message Authentication Code (MAC) in ANSI standards

Data Security	The communication networks must not allow unauthorized interception of communications or information; they must not allow communications replay attacks; and they must have nonrepudiation capabilities to ensure evidence in the event of a dispute.
DBMS	Database Management System
DDoS	Distributed Denial-of-Service—hackers launch attacks by using several smaller network connections, making it harder to detect. DDoS can inundate the largest ISPs and consume all their bandwidth.
Decryption	The process of changing ciphertext into plaintext.
Denial-of-Service (DoS)	This is an indirect attack to a site. Hackers are not trying to get into the site itself, but they are trying to keep everyone else from getting into the site.
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol—a protocol used to dynamically assign IP addresses to mobile devices.
Dictionary Attack	A password-cracking technique that uses words in a dictionary to crack passwords.
DID	Distributed Intrusion Detection
Digital	Information that can be represented by two discrete states (either 0 or 1). Most information in the speaking/seeing world is not digital but must be converted into this form to be used by computers.
Digital Fingerprint	A number that is unique to a digital certificate, used to verify if a signature is valid.
Digital Signature Standard	The digital signature algorithm (DSA) developed by the U.S. National Security Agency to generate a digital signature for the authentication of electronic documents.
Digital Timestamp	A record mathematically linking a document to a time and a date.
Distributed Denial-of-Service (DDoS) Attacks	Hackers launch attacks by using several smaller network connections, making it harder to detect. DDoS can inundate the largest ISPs and consume all their bandwidth.

DMS	Defense Messaging System
DMZ	Demilitarized Zone—a network inserted as a "buffer zone" between a company's private, or trusted, network and the outside, nontrusted network.
DoS	Denial-of-Service—this is an indirect attack to a site. Hackers are not trying to get into the site itself, but they are trying to keep everyone else from getting into the site.
DSA	Digital Signature Algorithm—used by a signatory to generate a digital signature on data and by a verifier to verify the authenticity of the signature.
DSO	District Security Officer
DSS	Digital Signature Standard
DSSV	Digital Signature Storage and Verification
EAL	Evaluation Assurance Level 4 as defined by the Common Criteria for Information Technology Security Evaluation (CCITSE). EALs provide a uniformly increasing scale which balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. There are seven hierarchically ordered EALs. The higher the EAL, the greater the degree of assurance.
EAM	Extranet Access Management
EAN	Extended Area Network—Jurisdiction Area Networks that are linked with county, regional, state, and national systems or extended area networks.
EAP	Extensible Authentication Protocol
ECC	Elliptic Curve Cryptosystem
EDI	Electronic Data Interchange
E-Mail Bombing	Flooding a site with enough mail to overwhelm its e-mail system. Used to hide or prevent receipt of e-mail during an attack or as retaliation against a site.

Emergency Medical Services Event Management System	A database containing information on the real-time status of emergency medical personnel, resources, hospitals, and patients that is accessible by command personnel, authorized responders, health care facilities, and so on.
Encryption	The process of cryptographically converting plaintext electronic data to a form unintelligible to anyone except the intended recipient.
EPIC	Electronic Privacy Information Center
ERB	Engineering Review Board
EvDO	Evolution Data Optimized
Expiration Date IEEE	All digital certificates should have an expiration date (Institute of Electrical and Electronics Engineers). A body that creates some cryptographic standards.
FAR	False Acceptance Rate
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
File Viruses	Usually replace or attach themselves to COM and EXE files. They can also be files with the extensions SYS, DRV, BIN, OVL, DOC, VBS, SCR, and OVY.
FIPs	Fair Information Practices
FIPS	Federal Information Processing Standard
FIPS PUB	Federal Information Processing Standard Publication
Firewall	A system designed to prevent unauthorized accesses to or from a private network. Often used to prevent Internet users from accessing private networks connected to the Internet.
Firewall Boundary	A commonly used term referring to a security perimeter that is largely defined by the presence of one or more firewalls.
FIRST	Forum of Incident Response and Security Teams. See <http://www.first.org>.
Footprinting	Also known as profiling, the process of obtaining data about a particular individual or company.

Frequency	The number of repetitions of a periodic process in a unit of time.
FRR	False Rejection Rate
FTC	Federal Trade Commission
FTP	File Transfer Protocol—a means to exchange files across a network.
GASSP	Generally Accepted System Security Principles
GPRS	General Packet Radio Service—one of the network protocols which are used by commercial mobile data network providers in the United States.
Gopher Protocol	Designed to allow a user to transfer text or binary files among computer hosts across networks.
Hacking	Unauthorized use or attempts to circumvent or bypass the security mechanisms of an information system or network.
"Hactivism"	Politically motivated attacks on publicly accessible Web pages or e-mail servers.
HIDS	Host computer Intrusion Detection Systems
HTML	HyperText Markup Language—the mechanism used to create Web pages.
I&A	Identification and Authentication
IAFIS	Integrated Automated Fingerprint Identification System
IAN	Incident Area Network—a network created for a specific incident. This network is temporary in nature.
ICDAG	Interagency Confidentiality and Data Access Group
ICMP	Internet Control Message Protocol
IDIP	Intruder Detection and Isolation Protocol

IDS	Intrusion Detection Systems—techniques that try to detect intrusion or unauthorized entry into a computer or network by observation of actions, security logs, or audit data. Intrusion detection is the discovery of break-ins or attempted break-ins, either manually or via specific software systems that operate on logs or other information available on the network.
IDWG	Intrusion Detection Working Group
IDXP	Intrusion Detection Exchange Protocol
IEEE 802.11	Wi-Fi
IEEE 802.11i	WPA2, an amendment to the 802.11 standard specifying security mechanisms for wireless networks.
IEEE 802.16	WiMAX
IEEE 802.20	Mobile Broadband Wireless Access
IEEE 1451.5	Wireless Sensor Standards
IETF	Internet Engineering Task Force
III	Interstate Identification Index
IJIS Institute	Integrated Justice Information System Institute See <http://www.ijis.org>.
IMAP	Internet Message Access Protocol
Infrastructure	The underlying permanent installations required for radio communications. Infrastructure includes antennas, base/repeater stations, consoles, links (fiber, microwave, radio, and wire), towers, and support structures (such as buildings and towers).
Insider Threat	A disgruntled insider with knowledge of the victim's system.
Integrity	Preservation of the original quality and accuracy of data in written or electronic form.
Interference	Confusion of received radio signals due to strays or undesired signals.

Intermediary	A program or set of programs that in some way evaluate, filter, modify, or otherwise interject some function between two end users or end-use programs such as a client/server. An example is the proxy server that most companies place between their internal Web users and the public Internet.
IP	Internet Protocol—a network protocol that facilitates the routing of data across a set of networks connected by routers (an Internet). IP addresses are used to identify the locations within the networks.
IP Spoofing	An attack where a hacker outside the network attempts to impersonate a computer from the trusted network.
IPsec	IP Security—adds security features to the standard IP protocol to provide confidentiality and integrity services.
ISDN	Integrated Services Digital Network
ISO	Information Security Officer
ISO	International Standards Organization
ISPs	Internet Service Providers
IT	Information Technology
ITMS	Information Technology Management Section
ITN	Identification Tasking and Networking
IWG	IJIS Industry Working Group. See <http://www.ijis.org>.
JAN	Jurisdiction Area Network—the main communications network for first responders. It is responsible for all non-JAN voice and data traffic. It handles any JAN traffic that needs access to the general network, as well as providing the connectivity to the EAN.
JISN	Justice Interconnection Services Network
JTF	Joint Task Force
KEA	Key Exchange Algorithm
KEK	Key Encrypting Key—a cryptographic key that is used for the encryption or decryption of other keys.

Key	A series of numbers used by an encryption algorithm to transform plaintext data into encrypted data.
Key Escrow	The system of giving a piece of a key to each of a certain number of trustees such that the key can be recovered with the collaboration of all the trustees.
Key Recovery	A secure means for backup and recovery of encryption key pairs.
Key Serial Number	A 128-bit number associated with a certificate.
Keyring File	A file that can house the certificate.
Killer Packets	A method of disabling a system by sending Ethernet or IP packets that exploit bugs in the networking code to crash the system. See SYN Floods.
KMF	Key Management Facility
KTC	Key Translation Center
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol—a standardized way to connect with a directory that might hold passwords, addresses, public encryption keys, and other exchange-facilitating data.
LEIF	Law Enforcement Interconnecting Facilities
LRA	Local Registration Authority—a person who evaluates and approves or rejects certificate applications on behalf of a Certification Authority.
MAC	Mandatory Access Control or Message Authentication Code
MANET	Mobile Ad-hoc NETwork—a collection of mobile nodes which communicate over radio and do not need any preinstalled communication infrastructure. Communication can be performed if two nodes are close enough to exchange packets. Mobile ad hoc networks are envisioned to be self-forming, self-maintained, and self-healing and will not require any existing infrastructure.
MIME	Multipurpose Internet Mail Extensions

MISPC	Minimum Interoperability Specification for PKI Components
Misuse	Illicit activity that exploits system vulnerabilities or file access privileges.
MIT	Massachusetts Institution of Technology
Mobile IP	Mobile Internet Protocol—the current standard for supporting mobility in IP networks.
Modem	An acronym for modulator/demodulator, which is a device that translates digital signals coming from your computer or other digital device into analog signals that can be transmitted over standard telephone lines or radio circuits. The modem also translates the analog signal back into a digital signal.
Multicast	Occurs when one device sends data across the network to multiple devices; however, depending on the multicast protocol, only nodes that are on the path from the originating device to the receiving device receive and forward the data.
Mutual Aid	This mode describes those major events with large numbers of agencies involved, including agencies from remote locations. Their communications are not usually well planned or rehearsed. The communications must allow the individual agencies to carry out their missions at the event but follow the command and control structure appropriate to coordinate the many agencies involved with the event.
NAPs	Network Access Points
NASCIO	National Association of State Chief Information Officers
NAT	Network Address Translation
NCIC	National Crime Information Center
NCS	Network Control Software
NCSC	National Center for State Courts
NIAP	National Information Assurance Partnership
NIDS	Network Intrusion Detection System

NIPC	National Infrastructure Protection Center
NIST	National Institute of Standards and Technology. See <http://www.nist.gov>.
Nlets	The International Justice and Public Safety Information Sharing Network
NNTP	Network News Transfer Protocol—protocol for Usenet news distribution.
Noise	An unwanted signal or disturbance (e.g., static) in a radio communications system.
Noninteractive Data Communications	A one-way stream of data, such as the monitoring of firefighter biometrics and location, which greatly increases the safety of the practitioners. This form of communications also makes the command and control requirements easier when the commander is aware of the condition and location of the on-scene personnel.
Noninteractive Voice Communications	These communications occur when a dispatcher or supervisor alerts members of a group about emergency situations and/or to share information. In many cases, the noninteractive voice communications have the same mission-critical needs as the interactive service.
Nonrepudiation	The cryptographic assurance that a message sender cannot later deny sending a message or that the recipient cannot deny receipt.
NSA	National Security Agency. See <http://www.nsa.gov>.
NTIS	National Technical Information Service
OECD	Organization for Economic Cooperation and Development
OMB	Office of Management and Budget
ORI	Originating Agency Identifier
OSCA	Office of State Court Administrators

OSI	Open Systems Interconnection—also known as the OSI reference model. This describes a standard for how messages should be transmitted between any two points in a network. The reference model defines seven layers that take place at each end of a communication.
P3P	Platform for Privacy Preferences
Packet	A unit of data that is routed between an origin and a destination on the Internet.
PAN	Personal Area Network—a collection of fixed, portable, or moving components, which form a network through local interfaces, with a typical radius of about 10 meters. These can include components that are carried, worn, or located near the body, such as wireless devices used to monitor the first responder's physical location, pulse rate, breathing rate, oxygen tank status, as well as devices for hazardous gases detection and voice communications.
Password	A string of characters used to authenticate an identity or to verify access authorization.
PCS	Personal Communications Services
PDP	Privacy Design Principle
Personal/Person-Identifiable Information	Information about the characteristics or activities of an identifiable natural person, including information about individuals who may not be explicitly identified but whose identity could be inferred from elements of the data. Sensitive data elements in existing databases can include name, address, social security number, ID numbers, and birth date.
PGP	Pretty Good Privacy—this set of standardized security procedures and algorithms provides authentication and privacy services and is most frequently used for secure e-mail. More information about PGP is available at <http://www.pgp.com>.
Physical Security Policy	A document specifying the steps to take to protect the actual machines used to store and process sensitive or valuable data.
PIA	Privacy Impact Assessment

PIN	Personal Identification Number
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure—an architecture which is used to bind public keys to entities, enable other entities to verify public key bindings, revoke such bindings, and provide other services critical to managing public keys.
Plaintext	Unencrypted (unenciphered) data
POC	Point-of-Contact
PP	Protection Profile
PPP	Point-to-Point Protocol
PPTP	Point-to-Point Tunneling Protocol
Privacy	The right of an individual to control his/her personal information and not to have it divulged or used without permission. In the context of information sharing, privacy is the right of an individual to have their personal information accessed only by authorized and intended individuals. Rules governing these privacy rights are subject to national and state policies and regulations. Security safeguards and mechanisms are used to enforce privacy through the protection of integrity, availability, and confidentiality of information. These mechanisms should not be confused with privacy.
Privacy Seals	The seals of approval granted by organizations such as TRUSTe, BBBOnline, and WebTrust. The seals intend to demonstrate that a Web site has adopted appropriate policies to protect personal information and to assure individuals that they are visiting a Web site they can trust. Disclaimer—keep in mind that these seals are not monitored, and anyone can "stick" a seal on their Web site.
Private Key	The key of the public key pair that is not shared by its owner.
PRNG	Pseudorandom Number Generator
Protected Resource	A target, access to which is restricted by an access control policy.

Protocol	A set of rules (i.e., formats and procedures) for communications that computers use when sending signals between themselves.
Public Key	The key of the public key pair that is widely shared, generally through a digital certificate.
Public Key Cryptography	Cryptography based on methods involving a public key and a private key.
PSAP	Public Safety Answering Point—the answering center for 9-1-1 calls.
PSTN	Public Switched Telephone Network—the public telephone system.
PVC	Permanent Virtual Circuits
QoS	Quality of Service
RACF	Resource Access Control Facility
RBAC	Role-Based Access Control
RC2, RC4	Specific standardized block ciphers algorithms (Rivest Cipher or Ron's Code).
"Recreational Hackers"	Persons who crack into networks for the thrill of the challenge or for bragging rights in the hacker community.
Refarming	An administrative process being conducted by the FCC to reduce channel bandwidths and, as a result, promote spectrum efficiency.
Registration Authority	A mechanism or person that, as part of a PKI, is involved in verifying and enrolling users.
Release	Disclosure of documents (records) containing personal information to a third-party requester.
Remote Access	Potential entry point for an attack that uses a war dialer and a password hacking tool to make login attempts.
RFC	Request for Comments

Risk	An expectation of loss or threat that can be expressed as the probability that a particular threat (or set of threats) will exploit a particular vulnerability with particularly harmful results.
Risk Analysis/Risk Assessment	The process of examining all risks, then ranking those risks by level of severity. Risk analysis involves determining what you need to protect, what you need to protect it from, and how to protect it.
Risk Management	The total process of identifying, controlling, and mitigating information technology-related risks; cost-benefit analysis; and the selection, implementation, testing, and security evaluation of safeguards. This overall system security review considers both effectiveness and efficiency, including impact on the mission/business and constraints due to policy, regulations, and laws.
RISS	Regional Information Sharing Systems®.
Router	A device or, in some cases, software in a computer that determines the next network point to which a packet should be forwarded toward its destination.
RSA	Rivest-Shamir-Adelman public key encryption algorithm.
Rules of Behavior	The rules that have been established and implemented concerning use of, security in, and acceptable level of risk for the system. Rules will clearly delineate responsibilities and expected behavior of all individuals with access to the system. Rules should cover such matters as work at home, dial-in access, connection to the Internet, use of copyrighted works, unofficial use of federal government equipment, assignment and limitation of system privileges, and individual accountability.
S-HTTP	Secure HyperText Transfer Protocol
S/MIME	Secure Multipurpose Internet Mail Extensions
S/WAN	Secure Wide Area Network
SAML	Security Assertion Markup Language—an XML security standard for exchanging authentication and authorization information.

Secret Key	In secret-key cryptography, this is the key used both for encryption and decryption.
Security Discipline	A set of subjects, their information objects, and a common security policy.
Security Goal	To enable an organization to meet all mission/business objectives by implementing systems with due care and consideration of information technology-related risks to the organization, its partners, and its customers.
Security Objectives	The five security objectives are integrity, availability, confidentiality, accountability, and assurance.
Security Policy	The statement of required protection of the information objects.
Sensitive Information	Information whose loss, misuse, or unauthorized access to or modification of could adversely affect the national interest or the conduct of federal programs or the privacy to which individuals are entitled.
SHA-1	Cryptographic hash algorithm that is optimized for high-end processors and produces a 160-bit digest.
Shoulder Surfing	Stealing passwords or PINs by looking over someone's shoulder.
SLA	Service Level Agreement
Smart Card	A small plastic card with a microprocessor that can store information.
SMTP	Simple Mail Transfer Protocol
Smurfing	The attacking of a network by exploiting Internet Protocol broadcast addressing and certain other aspects of Internet operations. Smurfing uses a program called Smurf and similar programs to cause the attacked part of a network to become inoperable.
SNA	Systems Network Architecture

Sniffer	A program to capture data across a computer network. Used by hackers to capture user names and passwords. Software tool that audits and identifies network traffic packets. It is also used legitimately by network operations and maintenance personnel to troubleshoot network problems.
Social Engineering	Subverting information system security by using nontechnical, social means.
Spamming	Sending unsolicited e-mail.
Spectrum	The region of the electromagnetic spectrum in which radio transmission and detection techniques may be used.
Spectrum Frequency	Optimizing the amount of information sent over a given amount of bandwidth.
SSID	Service Set Identifier is the default wireless network name.
SSL	Secure Socket Layer Protocol—invented by Netscape Communications, Inc. This protocol provides end-to-end encryption of application layer network traffic.
Standards	Conditions and protocols set forth to allow uniformity within communications and virtually all computer activity.
SYN Floods	A method of disabling a system by sending more TCP SYN packets than its networking code can handle. See Killer Packets.
Target of Evaluation	An information technology (IT) product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol and Internet Protocol
Telnet Protocol	A communication protocol used to (possibly remote) log on to a computer host.

Temporary Network	JANs and EANs are networks that exist at all times, whereas the JANs are created on a temporary basis to serve a particular purpose, such as an incident and then are dissolved. The nature of the JAN is such that it may not reach all areas of an incident. In such cases, the user would either connect to the JAN or create a temporary network to extend the JAN to the area not covered.
Threat	An event or activity, deliberate or unintentional, with the potential for causing harm to an information technology (IT) system or activity.
TIA CDMA2000 1x	1xRTT
TIA CDMA2000 1xED-VO	Evolution Data Only
TLS	Transport Layer Security
TOC	Technical and Operations Committee
Tokens	Something that the claimant possesses and controls that may be used to authenticate the claimant's identity.
TRB	Technical Review Board
Trinoo	A Trojan horse used by hackers to launch a Distributed Denial-of-Service (DDoS) attack.
Triple DES	A technique used to make Data Encryption Standard encryption stronger by applying the algorithm three times.
Tripwires	A mechanism or tool that detects hack attacks and alerts someone, such as an administrator, about the attack.
Trojan Horse	A computer program that appears to have a useful function but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program.
UPS	Uninterruptible Power Source
USENET	An e-mail-based discussion system, originally supported by dial-up connections, now usually accessed via TCP/IP.
VAN	Value-Added Network

VIN	Vehicle Identification Number
Virus	A small program that inserts itself into another program when executed and generally produces a detrimental result.
VPN	Virtual Private Network—a collection of technologies that creates secure connections via nonsecure networks (such as the Internet).
Vulnerability	A weakness in system security procedures, hardware, design, implementation, internal controls, technical controls, physical controls, or other controls that could be accidentally triggered or intentionally exploited and result in a violation of the system's security policy.
WAN	Wide Area Network
WAP	Wired Access Protocol—a specification for a set of communication protocols to standardize the way that wireless devices, such as cellular telephones and radio transceivers, can be used for Internet access, including e-mail, the World Wide Web, newsgroups, and Internet Relay Chat (IRC). For more information on the following terms, see the links provided. Protocol: <http://searchNetworking.techtarget.com/sDefinition/0,,sid7_gci212839,00.html> Wireless: <http://searchNetworking.techtarget.com/sDefinition/0,,sid7_gci213380,00.html> Internet Relay Chat: <http://searchWin2000.techtarget.com/sDefinition/0,,sid1_gci214040,00.html>
War Dialer	A simple database and an automated modem script that dials every phone number in a group designated by the user. After it successfully connects with a modem tone, the war dialer will record the phone number in a database. The hacker can then review the database and select a likely target for a hack attempt.
Wave	A disturbance or variation that transfers energy progressively from point to point in a medium and that may take the form of a variation in electric or magnetic intensity or electric potential.

Wavelength	The disturbance from one point along the progression of a wave to the next point on the wave of corresponding amplitude and phase.
WEP	Wired Equivalent Privacy—a combined access control, link privacy, and message integrity system for WLANs.
WLAN	Wireless Local Area Network—a network of computers or terminals connected by radio frequencies. Wireless LANs were conceived to complement fixed wired networks. Wireless access points (similar to traditional Ethernet hubs) provide access to devices that have wireless network interface cards.
Worm	A program that copies itself from system to system via the network.
WPA2	Wi-Fi Protected Access 2. See IEEE 802.11i.
WPA/RSN	Wi-Fi Protected Access/Robust Security Networks
XML	Extensible Markup Language
Zeroization	A method of erasing electronically stored data by altering the contents of the data storage in order to prevent the recovery of the data.

Appendix B: Bibliography

- Allen, Julia, and Stoner, Ed, *Detecting Signs of Intrusion*. (CMU/SEI-SIM-009). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2000, <http://www.cert.org/security-improvement/modules/m09.html>.
- *The Biometric Consortium,* <http://www.biometrics.org/html/standards.html>.
- *Biometrics Standards and Current Standard-Related Activities*, The Biometrics Resource Center Web site, National Institute of Standards and Technology, <http://www.itl.nist.gov/div895/biometrics/standards.html>.
- *Center for Internet Security (CIS)*, Hershey, PA, <http://www.cisecurity.org/>.
- *CERT® Coordination Center (CERT/CC)*, Carnegie Mellon Software Engineering Institute, <http://www.cert.org>.
- *The Computer Security Act of 1987*, Title 40, Section 1441, Responsibilities Regarding Efficiency, Security, and Privacy of Federal Computer Systems, <http://uscode.house.gov/usc.htm>.
- *Computer Security Resource Center (CSRC)*, National Institute of Standards and Technology (NIST), Computer Security Division (CSD), compilation of computer-related security best practices, <http://csrc.nist.gov/>.
- *Confidential Information*, United States Code, Title XI, Rule 81: Papers Filed Conformity, Section (h), <http://www4.law.cornell.edu/uscode/28/appendix-rule81PapersFiledConformity.html>.
- *Criminal Justice Information Systems*, U.S. Code of Federal Regulations (CFR), 28 CFR 20.1, Judiciary and Judicial Procedure, U.S. Department of Justice.
- *Data Encryption Standard* (DES) was, until recently, used by the United States government for protecting sensitive but unclassified data. This standard has since been superseded by Triple DES due to increases in computer power, which have allowed DES encryption to be broken. Advanced Encryption Standard (AES) has now become recognized by the National Institute of Standards and Technology (NIST), Computer Security Division (CSD), Computer Security Resource Center (CSRC), and has been officially approved for use by the United States government under Federal Information Processing Standard (FIPS) 197.

- *Data Security and Classification Guidelines*, Section IX: Data and Computing Policy Guidelines, The University of Massachusetts, <http://www.umassp.edu/policy/data/itcdatasec.html>.
- *Directive 96/46/EC on Data Protection* (the Directive), European Union (EU), <http://www.privacyinternational.org/agreements.html>.
- *Domestic Disaster Recovery Plan for PCs, OIS, and Small VS Systems*, National Institute of Standards and Technology (NIST), Gaithersburg, MD, U.S. Department of State, Washington, DC, National Technical Information Service (NTIS), U.S. Department of Commerce, <http://www.ntis.gov/search/product.asp?ABBR=PB90265240&starDB=GRAHIST>.
- *The Electronic Communications Privacy Act of 1986 (ECPA),* United States Code, Title 18, Part 1, Chapter 119, Section 2511: Interception and disclosure of wire, oral, or electronic communications prohibited, <http://www4.law.cornell.edu/uscode/18/2511.html>.
- *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)*, NIST Special Publication 800-27, June 2001, <http://csrc.nist.gov/publications/nistpubs/800-27/sp800-27.pdf>.
- *Evaluation Assurance Level 4 (EAL4), Common Criteria for Information Technology Security Evaluation (CCITSE)*, the Trust Technology Assessment Program (TTAP), National Security Agency (NSA), and National Institute of Standards and Technology (NIST), Radium Customer Information Provider—EALs provide a uniformly increasing scale which balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. There are seven hierarchically ordered EALs. The higher the EAL, the greater the degree of assurance, <http://www.radium.ncsc.mil/tpep/process/faq-sect3.html>.
- *Federal Agency Security Practices*, National Institute of Standards and Technology (NIST), <http://csrc.nist.gov/fasp/>.
- *Federal Information Security Management Act of 2002 (FISMA),* Public Law 107-347, December 17, 2002.
- Ford, Gary, et al., *Securing Network Servers*. (CMU/SEI-SIM-007). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 1999, <http://www.cert.org/security-improvement/modules/m10.html>.
- *The Freedom of Information Reform Act* (1986), United States Code, Title 5, Part I, Chapter 5, Subchapter II, Section 552: Public information; agency rules, opinions, orders, records, and proceedings, <http://www4.law.cornell.edu/uscode/5/552.html>.
- *F-Secure, Symantec, and McAfee* (antivirus software providers), <http://www.fsecure.com>, <http://www.symantec.com>, and <http://www.mcafee.com>.
- *Generally Accepted System Security Principles (GASSP)* as defined by the International Information Security Foundation, <http://web.mit.edu/security/www/GASSP/gassp11.html>.
- *Global Security Working Group* (authentication policy samples), Global Justice Information Sharing Initiative, <http://www.it.ojp.gov/topic.jsp?topic_id=58>.

- *Government Information Technology Agency* (sample working, multiagency program, with Central Response Team membership application), <http://gita.state.az.us/policies_procedures/p800_s855_incident_resp.htm>.
- *Guide for the Security Certification and Accreditation of Federal Information Systems*, NIST Special Publication 800-37, June 2003 (second public draft), <http://csrs.nist.gov/sec-cert/>.
- *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,* Organization for Economic Cooperation and Development (OECD), <http://oecdpublications.gfi-nb.com/cgi-bin/OECDBookShop.storefront/EN/product/932002011P1>.
- *Health Insurance Portability and Accountability Act (HIPAA) of 1996*, Centers for Medicare and Medicaid Services, <http://www.cms.gov/hipaa/>.
- *Health Insurance Portability and Accountability Act (HIPAA) of 1996*, Fact Sheet, Administrative Simplification Under HIPAA: National Standards for Transactions, Security, and Privacy, U.S. Department of Health and Human Services, <http://www.hhs.gov/news/press/2002pres/hipaa.html>.
- *IEEE/EIA STD 12207*. Software Life Cycle Processes, <http://standards.ieee.org/reading/ieee/std_public/description/se/12207.0-1996_desc.html>, <http://standards.ieee.org/reading/ieee/std_public/description/se/12207.1-1997_desc.html>, and <http://standards.ieee.org/reading/ieee/std_public/description/se/12207.2-1997_desc.html>.
- *Industry Working Group (IWG)*, Integrated Justice Information Systems (IJIS), <http://www.ijis.org>.
- *Information Technology Security Training Requirements: A Role and Performance-Based Model*, NIST Special Publication 800-16, April 1998, <http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf>.
- The Internet Engineering Task Force, four documents under current review:
  - Curry, David, and Debar, Hervé, *Intrusion Detection Message Exchange Format Data Model and Extensible Markup Language (XML) Document Type Definition*, January 31, 2003.
  - Feinstein, Benjamin, Matthews, Gregory, and White, John, *The Intrusion Detection Exchange Protocol (IDXP),* October 23, 2002.
  - New, Darren, *The TUNNEL Profile*, December 6, 2002.
  - Wood, Mark, and Erlinger, Michael, *Intrusion Detection Message Exchange Requirements*, October 23, 2002, <www.ietf.org/ids.by.wg/idwg.html>.
- *Internet Storm Center,* (DID) Systems, <http://www.incidents.org/isw/iswp.php>.
- *IP Security Protocol (IPsec),* Internet Engineering Task Force (IETF), <http://www.ietf.org/html.charters/ipsec-charter.html>.
- *The ISO 17799 Service and Software Directory,* International Organization for Standardization (ISO 17799 is a comprehensive set of controls comprising best practices in information security. It is essentially an internationally recognized generic information security standard.), <http://www.iso17799software.com/>.

- *Justice Information Privacy Guideline—Developing, Drafting, and Assessing Privacy Policy for Justice Information Systems,* National Criminal Justice Association, September 2002, <http://www.ncja.org/publications.html#>.
- Kossakowski, Klaus-Peter, et al., *Responding to Intrusions*. (CMU/SEI-SIM-006). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 1999, <http://www.cert.org/security-improvement/modules/m06.html>.
- *Lightweight Directory Access Protocol (LDAP),* The Internet Engineering Task Force, Network Working Group, <http://www.ietf.org/rfc/rfc1777.txt>.
- *MIT Business Continuity Plan,* Massachusetts Institute of Technology (MIT), 1995, <http://web.mit.edu/security/www/pubplan.htm>.
- *MIT Emergency Response System*, Massachusetts Institute of Technology (MIT), <http://web.mit.edu/emergency/ers/index.html>.
- *National Association of State Chief Information Officers (NASCIO)*, Lexington, KY, <http://www.nascio.org>.
- *Omnibus Crime Control and Safe Streets Act of 1968*, Pub. L. No. 90-351, 82 Stat. 197, 1968 U.S.C.C.A.N. 237, as amended.
- *Personnel Security Standard*, Treasury Board of Canada, <http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/CHAPT2-4_e.asp>.
- *Preservation and Exchange of Identification Records and Information*, U.S. Code of Federal Regulations, Title 28, Part II, Chapter 33, Section 534, Judiciary and Judicial Procedure, U.S. Department of Justice, Federal Bureau of Investigation, Acquisition, <http://www.access.gpo.gov/uscode/uscmain.html>.
- *Privacy Act of 1974,* United States Code, Title 5, Part 1, Chapter 5, Subchapter 11, Section 552a, <http://www.4.law.cornell.edu./uscode/5/pich5schll.html>.
- *Recommendation for Electronic Authentication*, NIST Special Publication 800-63, <http://fasp.nist.gov/publications/drafts.html#draft-sp80063>.
- *Safe Harbor Act*, U.S. Department of Commerce, Export Portal, <http://www.export.gov/safeharbor/>.
- *Sample Operating Policies and Procedures*, Institute for Intergovernmental Research® (IIR), <http://www.iir.com/28cfr/sample_operating_Policies_procedures.htm>.
- *The SANS Security Policy Project*, The SANS Institute, <http://www.sans.org/resources/policies/>.
- *Security Assertion Markup Language (SAML),* Organization for the Advancement of Structured Information Standards (OASIS), Security Services Technical Committee, <http://www.oasis-open.org/committees/security/>.
- *Security Classification of Information*, Classification Levels, Chapter 7, Vol. 2, Principles for Classification of Information, Oak Ridge National Laboratory, U.S. Department of Energy,

Department of Energy Federation of American Scientists Web site, <http://www.fas.org/sgp/library/quist2/chap_7.html>.

- *Secure Hash Standard*, Federal Information Processing Standard Publication 180-1, April 17, 1995, <http://www.itl.nist.gov/fipspubs/fip180-1.htm>.
- *Summary of the Intrusion Detection and Isolation Protocol (IDIP) Project*, Intrusion Detection and Isolation Protocol, University of California, Davis, <http://seclab.cs.ucdavis.edu/projects/idip.html>.
- Swanson, Marianne, *Security Self-Assessment Guide for Information Technology Systems*, National Institute of Standards and Technology, Publication 800-26, <http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf>.
- *Underlying Technical Models for Information Security*, Stoneburner, G., NIST Special Publication 800-33. December 2001, <http://csrc.nist.gov/>.
- *Washington State Information Technology Security Policy Audit Standards*, Washington State Auditor's Office, September 2001, <http://www.sao.wa.gov/StateGovernment/ITSecurity/ITStandards.htm>.
- *Washington State Privacy Policy*, Access Washington, Department of Information Services, <http://www.wa.gov/dis/aboutdis/pdpnotice.htm>.
- *<http://www.leo.gov/lesig/cjis/cjis_pub/information/poly2002_feb/POLY2002_Feb.htm>.
  *Note: Only LEO members may access the www.leo.gov Web site.

Note: Those who are interested in computer and information systems security are encouraged to consult the Web site of the National Institute for Standards and Technology (NIST) at <http://csrc.nist.gov/index.html>. At this site, the Computer Security Resource Center (CSRC) at NIST offers a series of publications on security terminology, issues, and policies for justice information specialists to use as guidance.

www.it.ojp.gov

About Global

The U.S. Department of Justice's Global Justice Information Sharing Initiative (Global) serves as a Federal Advisory Committee to the U.S. Attorney General on critical justice information sharing initiatives. Global promotes standards-based electronic information exchange to provide justice and public safety communities with timely, accurate, complete, and accessible information in a secure and trusted environment. Global is administered by the U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance.

Applying Wireless Security Practices to Justice Information Sharing