NIST Special Publication 800-13

Telecommunications Security Guidelines for Telecommunications Management Network

John Kimmins, Charles Dinkel, and Dale Walters

U.S. DEPARTMENT OF COMMERCE

Technology Administration
National Institute of Standards and Technology

COMPUTER SECURITY

1.0 PREFACE

The Public Switched Network (PSN) provides critical commercial telecommunications services and National Security and Emergency Preparedness (NS/EP)[1] telecommunications. Service providers, equipment manufacturers, users, and the Federal Government are concerned that vulnerabilities in the PSN could be exploited and result in disruptions or degradation of service. To address these threats, the National Institute of Standards and Technology (NIST) is collaborating with Bellcore to investigate the vulnerabilities and related security issues that result from the use of open systems architectures in the telecommunications industry. Security features required to counter the threats are identified.

A series of Telecommunication Security Guidelines (TSGs) that address a hierarchy of telecommunication architectures of increasing complexity may be produced. This first guideline focuses on two specific components of a Telecommunications Management Network (TMN)[2] - Network Elements (NEs) and Mediation Devices (MDs) - with emphasis on the security features needed to protect the Operations, Administration, Maintenance, and Provisioning (OAM&P) of these components.

This TSG is intended to provide a security baseline for NEs and MDs that is based on commercial security needs. In addition, some NS/EP security requirements will be integrated into the baseline to address specific network security needs.

The guideline should assist telecommunications vendors in developing systems and service providers in implementing systems with appropriate security for integration into the PSN. It can also be used by a government agency or a commercial organization to formulate a specific security policy. It does not stipulate regulatory requirements or mandated standards of the National Institute of Standards and Technology.

1.1 INTRODUCTION

1.1.1 BACKGROUND

The Public Switched Network (PSN) provides services that are essential to U.S. citizens and government agencies alike. Disruption of telecommunications services would clearly represent a serious threat to public safety and security. A 1989 report of the National Research Council, "The Growing Vulnerability of the Public Switched Network," [1] outlined the concerns of the government for maintaining the integrity of the PSN against intruders. A report the following year by the President's National Security Telecommunications Advisory Committee (NSTAC) concluded that "until there is confidence that strong, comprehensive security programs are in place, the industry should assume that a motivated and resourceful adversary, in one concerted manipulation of the network software, could degrade at least portions of the PSN and monitor or disrupt the telecommunications serving [government] users" [2]. In addition, outages experienced by service providers in the recent past have focused the Federal Government's attention on the need to ensure that telecommunications services are available and reliable. More recent NSTAC studies have shown that the threat and vulnerabilities for public networks is still significant [18].

[1] "NS/EP telecommunications services are telecommunications services which are used to maintain a state of readiness or to respond to and manage any event or crisis (local, national, international) which causes or could cause injury or harm to the population, damage to or loss of property or degrades or threatens the NS/EP posture of the United States" [19]

[2] See the Appendix for a description of a TMN architecture

In the past, there were relatively few telecommunications providers, and the systems they used were built on proprietary platforms. The Federal Communication Commission's (FCC) Open Network Architecture (ONA) requirements specify unbundled and equal access to the PSN for Bell Operating Companies and their enhanced services competitors [3]. The environment is changing today to one where many service providers are using products and offering services that must work with products from many vendors [4], [5], [6]. This new open telecommunications environment has been characterized as one with: a large number of features; multi-media, multi-user services; incomplete knowledge of the feature set by service designers; lower skill and knowledge levels of some service creators; multiple execution environments from different vendors; and distributed intelligence [7]. A Network Operations Forum (NOF) report notes that:

> While the advent of open systems interfaces has assisted the acceptance and international deployment of networking technology, it has also seen a downside in that it has become easier to intrude on networks designed with such open features. ... Bellcore's security Subject Matter Experts have indicated that many of the intruders were assisted in their endeavors by the openness and standardization that the telecommunications industry has undergone during the last decade [8].

Fraudulent use of telecommunications resources is also on the increase. Intruders are taking advantage of different situations to commit fraud. Two situations are listed below:

1. Customers frequently fail to adequately protect their customer premises equipment (CPE) which allows intruders to steal service without modifying data, information, or software controlling Network Elements (NEs).

2. Customers have demanded and received greater access to data, information, and software controlling NEs to expand their capabilities to control and customize their service. Intruders gain unauthorized access to customers' capabilities and steal service by modifying data, information, or software controlling NEs.

The second situation is of greater concern, because in addition to simple theft of service, it creates the potential for intruders to cause denial of service that may affect a large number of users.

Safeguarding the security and integrity of the PSN in such an environment is a challenging task. In the current open environment, industry/government cooperation will help ensure that organizations implement the baseline security measures needed to protect their systems. This document provides baseline protection measures that government agencies or commercial organizations can use to safeguard Telecommunication Management Networks (TMN) resources and counter security threats.

1.1.2 SCOPE OF TSG EFFORT

Telecommunications networks offer a wide range of communication services (packet switching, data transfer, voice, video, etc.) to customers. These networks, which may be public or private, are populated by a large and increasing number of Operations Systems (OSs), Network Elements (NEs), Element Managers (EMs) and Mediation Devices (MDs) supplied by different vendors.

OSs tend to have centralized functionality, a span of control that covers a large portion of the network, and generally provide most of the operations functions. NEs are distributed components that provide telecommunications services, have a span of control generally limited to themselves, and have a relatively limited set of operations functionality. MDs act on the context of operations information passing between NEs and OSs. MDs may provide functions such as upper layer protocol internetworking, filtering, format conversion, storage, etc. The Appendix provides more detail on the differences among these components.

A TMN allows for the exchange of management information and offers communications between itself and the telecommunications networks. Management information about most aspects of network operations, including testing, maintenance, billing, and engineering is exchanged over TMN interfaces. TMNs provide the organized network structure that is needed to interconnect various types of OSs and telecommunications equipment using standardized protocols and interfaces.

The rapid growth in the number of telecommunications networks and the variety of services they offer have created a wide diversity of management and security needs to be satisfied. TMN interfaces, such as those between NEs and OSs, are vulnerable to a variety of threats. Adequate security measures must be provided to protect them. The connectivity provided by open systems accentuates the security risks of unauthorized access to the TMN environment and its software and databases.

The Telecommunication Security Guidelines (TSG) for TMN will define a framework and provide guidance for establishing a secure TMN. Security in a TMN refers to a set of procedural, logical, and physical measures that prevent, detect and correct certain types of actions or threats that may compromise the integrity, availability, timeliness, and confidentiality of information and services. Security mechanisms for the interfaces and communications required to manage the various Operations, Administration, Maintenance, and Provisioning (OAM&P) functions in a TMN are discussed.

Various levels of decomposition exist within a telecommunications network. The TMN architecture provides one such level. The first phase of this effort will address the network at a component level. Subsequent phases will address both component and global levels.

1.1.2.1 SCOPE OF SECURITY FEATURES

This first of a series of TSGs describes security features that are necessary to protect TMN components, specifically NEs and MDs, from various types of attacks leading to misuse and abuse of the software functions within the components. These security features address such areas as authentication, access control, audit, integrity, and administration. This document addresses both the global nature of the TMN and the interactions among TMN components.

Security features are not sufficient by themselves to provide a secure TMN. Security has to be considered throughout the entire development life cycle of the TMN and its components as part of quality assurance and system reliability. All security features need to be properly conceived, designed, implemented, tested, installed, documented, and maintained. Otherwise, a false sense of security may result. This TSG effort specifies appropriate security requirements to ensure that an acceptable security level is maintained throughout the system development life cycle and is also reflected in system documentation.

1.1.2.2 PERSPECTIVES

1.1.2.2.1 TELECOMMUNICATIONS SECURITY GUIDELINE

This Telecommunications Security Guideline adopts an OAM&P perspective rather than a user service perspective. This document describes security features needed by the network nodes and the network to protect themselves from various types of security threats and attacks. The focus is on the security of NE and MD operations, NE/MD interactions with other components, information resident in the NE, and fraud prevention.

The security features will not address security in the context of the inherent features in the network's call processing functions or how various network services will provide security within the framework of the service. The OAM&P of the information and software used by the network to process a call or a service request are within the purview of this effort.

Emphasis is placed on defining a minimum security baseline to protect the TMN components from various security threats. It is recognized that network environments and service needs will vary. This document will establish a security baseline that is applicable to a common commercial level of security. For some user environments, additional security features and stronger mechanisms may be needed to augment the specified baseline, depending on the organizational security policies.

1.1.2.2.2 MINIMUM SECURITY REQUIREMENTS/COMMON CRITERIA

NISTIR 5153, **Minimum Security Requirements for Multi-User Operating Systems (MSR)**, specifies computer-based protection mechanisms for the design, use, and management of information systems. These requirements include technical measures that can be incorporated into multi-user, remote access, resource sharing, and information-sharing computer systems. The MSR provides administrators of an MSR-conformant computer system with the tools to control the sharing of information and resources based primarily on the identity of users, but also on the time of day, terminal location, or type of access requested by users. The technical measures also provide tools to protect against common user actions that may compromise security and against deliberate penetration attempts by "crackers[3]". In addition, there are requirements that a conformant computer system provide a tailorable ability to log events that may impact the security of either the system or the information that it is processing.

The MSR provides basic commercial computer system security requirements applicable to both government and commercial organizations. The MSR document was written from the perspective of protecting the confidentiality and integrity of an organization's resources and promoting the continual availability of these resources. The MSR is being superseded by the draft Common Criteria.[4]

1.1.2.2.3 DIFFERENCES BETWEEN THE TSG AND MSR

In the past, differences between telecommunications systems and computer systems were readily apparent. Today that distinction is not so clear. For example, one type of NE, the software-controlled digital switch, has replaced much of the older mechanically switched telecommunications equipment. The newer digital systems are taking on the characteristics of special purpose computer systems processing a communication application. As such, they are subjected to many of the same threats that confront computer systems, while at the same time retaining much of the unique functionality associated with responding to customer demands for voice communications.

[3] A cracker is a computer hacker who specializes in overcoming software protection systems.

[4] The Common Criteria will allow for the creation of protection profiles for general purpose, multi-user operating systems, trusted components, and secure distributed systems. It is anticipated that these profiles, or a version thereof, will form the basis for mutual recognition of system evaluations among nations.

The TSG and the MSR/Common Criteria take different approaches to dealing with security. The latter can be used to specify a set of security requirements needed in a class of computer products often described as general purpose, multi-user operating systems. The Common Criteria is intended to broaden its scope to include requirements for trusted subsystems and distributed systems. Examples of such products from the TMN environment (architecture) include Operations Systems (OSs) and Workstations (WSs). The MSR is based on the TCSEC[5] C2 criteria class, with additions from current computer industry practice and commercial security requirements specifications.

In contrast, the focus of the TSG is on NEs and MDs - components that differ from the general purpose computers normally associated with OSs and WSs. Also, the full functionality of an NE can include call-handling OAM&P functions as well as a billing capability.

Security requirements for TMN components such as OSs and WSs are addressed by the MSR/Common Criteria. For that reason the TSG does not deal with such systems, but instead focuses on the remaining components of the TMN architecture. The Appendix provides a description of the TMN architecture.

1.1.2.3 ENVIRONMENTAL ASSUMPTIONS

The following specific environmental conditions have been assumed in specifying the security mechanisms required to protect TMNs:

1. Physical security - it is assumed that TMN components are in physically secure locations or that manual procedures and controls and other physical safeguards (e.g., locked equipment cabinet) can provide physical security for a given location.

2. Training and Awareness - these topics are viewed as part of the overall security strategy for a given environment. Management must make an informed decision regarding the adequacy of existing training and awareness efforts.

3. User Service Perspective - the security features of a given service or application are outside the scope of this effort. This includes service specific, and fraud detection and prevention requirements.

4. There will be one or more personnel assigned to manage the system, including the security of the information it contains.

5. If a network interface is supported, the attached networks will provide some facility to transport the identity of remote users.

1.1.3 DEFINITIONS

User

[5] The Department of Defense Trusted Computer System Evaluation Criteria (TCSEC) describes criteria for specifying and evaluating the trust of operating systems. It is widely known as the "Orange Book."

The term *user* refers to an individual, group, host, domain, trusted communication channel, network address/port, another network, a remote system (e.g., operations system), or a process (e.g., service or program) that accesses the network, or is accessed by it, including any entity that accesses a network support entity to perform OAM&P-related tasks. Regardless of their role, users must be required to successfully pass an identification and authentication (I&A) mechanism. For example, I&A would be required for a security or system administrator. For customers, I&A could be required for billing purposes.[6] See Figure 1.

Customer

The term *customer* applies to a person or organization who subscribes to a service offered by a telecommunications provider and is accountable for its use. A customer is permitted to use an NE to make calls and configure local line parameters (e.g., configure the numbers that should receive forwarded calls).[7]

Security Administrator

The term *security administrator* is used generically to mean the highly privileged role a person may have for performing security-related administrative tasks (e.g., customize the audit features for the system).

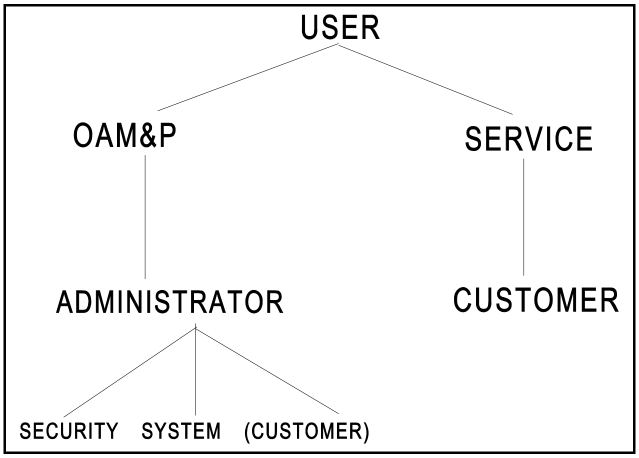

Figure 1 – User Roles.

Domain

The term *domain* refers to a part of the network that is administered by a single authority.

[6] For some services (e.g., Emergency Services) a customer may not need to be authenticated by the system.

[7] In some circumstances a customer can also play the role of administrator, for example, when the customer has access to operations information that would permit him to reconfigure his circuits. Some service providers offer this service, as well as other OAM&P features, to customers for a fee.

1.1.4 AUDIENCE

The TSG targets four distinct audiences: users, vendors, evaluators and service providers.

* The TSG addresses the security needs of telecommunications systems users. This includes application developers, customers, and private sector and government administrators. The requirements focus on the basic security requirements of commercial telecommunications systems.

* The TSG provides vendors with a single, well-defined set of security requirements that are applicable across their entire customer base. These requirements represent the integration of a number of security requirement specifications from various sources (see Section 1.1.2.2.2) into a single set that is expected to have wide acceptance. Vendors can more confidently use this set to develop a single system with features that meet the needs of a significant customer base. The level of detail provided by these requirements should help clarify what the vendor must do to comply.

* Product and system evaluators can apply the well-defined set of security requirements in the TSG to their work. The detailed level of the requirements significantly decrease the need for evaluator interpretation. A format similar to that used in the Common Criteria provides a basis for widespread acceptance of the requirements and mutual recognition of evaluations.

* Service providers are provided a clearly defined and widely accepted set of security requirements that are consistent with user expectations. It is anticipated that the TSG will result in a wider array of competitively priced products from which service providers can choose when responding to user solicitations and requirements.

1.1.5 TERMINOLOGY

The TSG project adopts the following terminology used in the MSR document:

* **Requirement** - A feature or function that is necessary to satisfy the security needs of a typical commercial or government organization. Failure to meet a Requirement may cause application restrictions, result in improper functioning of the system, or hinder operations. A Requirement contains the word shall and is identified by the letter "R."

* **Advisory** - A feature or function that may be desired by a typical commercial or government organization. An Advisory represents a goal to be achieved. An Advisory may be reclassified as a Requirement at some future date. An advisory contains the word should and is identified by the letter "A."

1.1.6 CONFORMANCE

Due to the hierarchical nature of the TMN architecture, different levels of conformance will be specified. At the network component level, for example, conformance can be linked to the detailed analysis and evaluation of a particular element.

In situations where control is less definitive, conformance may need to be demonstrated in less rigorous ways. This would be the case for network components that are controlled by an administrative entity that is distinct from the user environment, or where two TMNs need to be interconnected.

1.1.7 APPLYING THE TSG

It is not sufficient to specify requirements in terms of features and functions. A framework for applying the requirements is also included to provide additional guidance to users and vendors.

The TSG effort provides baseline criteria from which requirements specific to a particular TMN environment may be derived. In addition, this baseline can assist the user in formulating a specific security policy. The baseline is a benchmark with which formal security requirements for a specific TMN environment can be compared and exceptions justified on the basis of unique vulnerabilities, associated risks, and sound business decisions. For some specific TMN environments the baseline may have to be augmented with additional security features that are tied into the policy, as well as with the identified security needs of the environment.

1.1.8 AREA FOR FURTHER RESEARCH

There is one area, broadband network components, that needs to be further studied to determine whether the TSG applies to these components also and, if so, where they fit in the series of documents. The broadband network area is evolving and is in the early stages of network trials and product development. The initial versions of these broadband products may not accurately represent what a broadband network node will look like in the future. Some of these products, even though acting in the role of a NE, may be more closely aligned with data communication equipment in terms of functionality. More work is needed to determine if this is a new class of equipment that needs specific requirements or whether it fits into the existing categories of equipment (i.e., NEs and data communication network nodes). This document, which focuses on NEs, MDs, and EMs, is the initial phase of the TSG effort. The second phase will cover data communication network nodes.

2.0 SECURITY THREATS AND CONCERNS

2.1 INTRODUCTION

In the United States, government and industry have become dependent upon telecommunications networks to support commerce in all of the major economic sectors. At the same time, because of changes in technology, regulations, customer service demands, and accelerated technology deployments to address market pressures, the Public Switched Network (PSN) is becoming more vulnerable to security breaches.

Several reports have discussed recent intrusion experiences and potential threats to the PSN. The National Research Council report, "**Growing Vulnerability of the Public Switched Network: Implications for National Security Emergency Preparedness**" [1], and the "**Report of the Network Security Task Force**" [2], both address growing concern with possible network disruptions. A more recent study, "**The Electronic Intrusion Threat To National Security and Emergency Preparedness (NS/EP) Telecommunications**" [18] reports that the network intruder's knowledge and sophistication is increasing and the potential impact on the PSN is greater. Adequate protection of PSN resources is required to ensure: the availability of service during emergencies; the integrity of transmitted information; the non-disclosure of sensitive information; and the prevention of service fraud.

This chapter describes the scope of the threat, sources for these threats and characteristics associated with the major categories of threats.

2.2 SCOPE OF SECURITY THREATS

Changes in network architectures, technologies, interfaces, services, and operations may impact the ability of the PSN to provide the mix of functions and services to meet NS/EP and commercial needs. "*Threats*" are accidental or deliberate actions or events that compromise the quality, utility, or functionality of network services and operations. Threats can result in financial losses for the network and service providers and/or their users. A "security threat" is an intentional threat, whether mischievous or malicious, against network services and operations. The focus of this document is security threats.

Threats to the PSN could result in any of the following impacts:

1. Service denial or disruption - Typically, service disruptions caused by intruders have been brought about by accidental actions rather than malicious attempts.

2. Unauthorized monitoring and disclosure of sensitive information - The current approaches that intruders have used are eavesdropping techniques, network monitoring tools, and intrusions into network databases containing customer information.

3. Unauthorized modification of user or network information and network services - Intruders have changed user service profiles and affected billing and routing. This can result in unreliable service.

4. Fraud - The typical approach is to build upon the previous attacks and masquerade as a legitimate customer to commit fraud related to voice and data services.

2.3 SOURCES OF THREATS

Threats[8] to the PSN arise from several different sources:

Source	Likelihood	Principal Impact on Network
Employees/Insiders	65%	Availability, integrity, privacy
Natural disasters	20%	Availability
Hackers	15%	Availability, integrity, privacy

2.3.1 EMPLOYEES/INSIDERS

Intentional and accidental errors, omissions, and malicious acts by employees cause the majority of the damages and losses experienced in the telecommunications industry. This is partly attributable to changes in the definition of "*employee*." Previously, an employee was usually considered a full-time member of an organization. From a security perspective, it generally equated to an insider with high privilege. Today, insiders also include contractors who have administrative roles with respect to network service and may perform other job functions as well. This broader definition of an employee increases the potential of insider attacks that can severely impact the security of the PSN.

2.3.2 NATURAL DISASTERS

Natural disasters and accidents resulting from man-made causes can impact the availability of the PSN. Disasters such as hurricanes, floods, fire, etc., impact the timeliness and quality of the delivered services. In addition to the basic security concerns, NS/EP related capabilities can also be affected. Methods of dealing with threats from natural and man-made disasters include the use of redundant networks, reliable components, disaster recovery plans, and priority restoration of services (e.g., The Telecommunications Service Priority (TSP) System provides for priority provisioning and restoration of NS/EP telecommunications services). A complete discussion of this topic is beyond the scope of this document.

2.3.3 MALICIOUS HACKERS

The PSN is becoming increasingly controlled and dependent on software and operations networks that may offer customer access to network functions, user-configured databases, and special features. The potential for intruders to access network management and operations functions is growing because customers now have greater access to functions that were previously restricted to telecommunications employees. This increases threats caused by viruses, worms, and other malicious software. Dial-in access to PSN components is a prime point of malicious intrusions into software-based telecommunications systems.

The FCC-mandated ONA is designed to provide equal, user-transparent access via the PSN to network services provided by network-based and non-network enhanced service providers. ONA has the potential to create network vulnerabilities because it greatly increases the number of users (some of whom may be hostile) who have awareness of the network architecture. See NIST Special Publication 800-11 [22] for more information on the impact of ONA. In addition, as users learn more about the operation of network software, those with hostile intent will acquire knowledge that could assist them in misusing resources.

[8] Statistics - Datapro Research Corporation - figure in Security Overview 1, 14th NCSC, 1991; Wall Street Journal, Aug 15, 1990

2.4 THREAT CATEGORIES

Threats are circumstances or events with the potential to cause harm to a system in the form of destruction, disclosure, or modification of data and/or denial of service. They have the potential to compromise the security of software applications providing OAM&P functionality as well as network services. They may be deliberate, e.g., hacking, or accidental, e.g. procedural errors. The following is a list of categories of threats to software applications residing on NE platforms:

1. Masquerade - an attempt to gain unauthorized access to, or greater privilege to a system, by posing as an authorized user (e.g., using stolen logon ids and passwords). This may be done by replaying data or inserting false data that appears genuine into a communications path. System software and data may be deleted, disclosed, or corrupted. An example is the re-programming of NE software to insert malicious code to steal passwords. This threat can occur from:

   a. Outside users accessing the NE from the public network;
   b Locally connected users;
   c. Compromised administrator accounts that are configured for direct and remote access;
   d. Administrators dialing into dial-in modems connected to the NE.

2. Disclosure of information - data disclosed without authorization, either by deliberate action or by accident. Examples include:

   a. Eavesdropping on phone conversations or on data transmissions;
   b. Unauthorized disclosure of routing, address or other customer or service related information;
   c. Deliberate misrouting data to enable an unauthorized entity to access information.

3. Message stream or data modification - data altered in some meaningful way by reordering, deleting or modifying it. Examples include:

   a. Accessing and changing billing information;
   b. Unauthorized modification of NE software or databases;
   c. Rerouting calls.

4. Denial of service - actions that prevent the NE from functioning in accordance with its intended purpose. A piece of equipment or entity may be rendered inoperable or forced to operate in a degraded state; operations that depend on timeliness may be delayed. Examples include:

   a. Unauthorized destruction of existing NE resources including hardware, software, and databases;
   b. Degraded NE service processing caused by a large volume of service requests;
   c. Putting a NE in an "out-of-service" state.

5. Traffic analysis - a form of passive attack in which an intruder observes information being transmitted and makes inferences from the calling and called numbers, and the frequency and length of the calls. Examples are:

a. An intruder concludes that a high volume of communications between a company and the Patent Office indicates that a patent is being filed;

b. A corporate merger is deduced from the amount of traffic between two companies.

3.0 REQUIREMENTS FRAMEWORK

This document specifies the generic security requirements for switching, access, and transport NEs. It applies to all new NEs, as well as supporting entities called Element Managers (EMs) or Mediation Devices (MDs). Depending on local policy decisions, existing systems (NEs, MDs, etc.) should be upgraded to meet these requirements. Although the term NE is used exclusively in the following paragraphs, the requirements also apply to MDs and EMs. In addition, the document pertains to software and data and is applicable through all phases of the product life cycle.

Future NEs must follow these requirements throughout their life cycle. Existing NEs, when major modification occurs, must incorporate these life cycle requirements which will remain throughout the rest of their life cycle.

3.1 REQUIREMENTS APPLICABILITY

3.1.1 MEDIATION DEVICES AND ELEMENT MANAGERS

MDs and EMs manage network resources and provide a wide range of functions in support of the NE using different interfaces. These devices may control various types of network services, provide for information conversion and storage, perform protocol interworking, and manage network resources individually or in aggregation as a subnetwork. They may perform operations-related functions for network resources, and/or may assist in handling calls. This is consistent with the TMN architecture described in the Appendix.

The placement of functions into a physical system is an implementation decision made by the vendor. Consequently, the security requirements for a particular implementation of a mediation device or element manager depend on the functionality of the resident applications, and the associated risks. A risk analysis has to be performed to determine the specific NE security requirements that apply. However, the High Level Security Requirements defined in Section 3.2 must be followed.

3.1.2 COMPONENT VIEW

This document addresses NE security. In a TMN environment there are security dependencies that must be considered. TMN components interface with other components within the context of defined trust relationships. When securing a NE or its interfaces, these dependencies need to be recognized.

3.1.3 SECURITY POLICY

A commercial unclassified security baseline (Section 4) is defined in this document. Additional security may be needed to meet specific application and service needs. Senior level management must establish a security policy and define mission critical requirements for a NE and its associated operating environment.

3.1.4 USER ACCESS

New interfaces and user groups may require access to NEs. In particular, unbundling the PSN as defined by the ONA, and emerging customer network management services will affect NE security. The defined baseline requirements can be used to derive specific policies, requirements, mechanisms and procedures to accommodate the increased diversity in user access.

3.1.5 FRAUD

Fraud is a critical concern when providing user services. This document addresses fraud as viewed from the standpoint of applying security requirements in an operations setting. The generic security requirements of this guideline protect OAM&P functions that may be used to commit fraud. Fraud of billable service capabilities is not addressed. The requirements are not specific to particular billable services that could be susceptible to various types of attack (e.g., masquerade and unauthorized access).

3.1.6 NEW TECHNOLOGIES

New technologies and services, e.g., broadband, have resulted in various types of equipment being classified as NEs. Besides the traditional large NEs residing in central office environments, smaller NEs can be located at the edges of the PSN in various locations such as in private networks and user locations. A risk analysis will help identify security threats as well as the vulnerabilities of the interfaces in such equipment. Although the High Level Security Requirements defined in the next section are applicable, the detailed requirements in Chapter 4 may need to be modified to accommodate the identified risks and vulnerabilities.

3.2 HIGH LEVEL SECURITY REQUIREMENTS

This section provides High Level Security Requirements for NEs. The statements (S) describe basic high level security features. Each is followed by an appropriate high level policy guideline (P).

S1. IDENTIFICATION

Identification is the process whereby the NE recognizes a user's unique and auditable identity such as the User-ID. The User-ID is the name by which a valid user is recognized by the NE. This item of information is generally not considered confidential.

P1. All authorized users of the NE shall be uniquely identified to support individual accountability.

S2. AUTHENTICATION

Authentication is the process of verifying the claimed identity of the NE user. Passwords and smart cards can be used to provide this verification. Authentication information, especially when it is transmitted between a user and a remote NE, must be kept confidential.

P2. The NE shall authenticate all users prior to initially allowing access.

S3. SYSTEM ACCESS CONTROL

NE access control authorizes establishment, continuation, and completion of a session that is responsible for processing, storing, or transmitting information. NE access is allowed only to those users that are identified and authenticated.

P3. The NE shall not allow access to users, processes, or other systems unless they are properly identified and authenticated.

S4. RESOURCE ACCESS CONTROL

Resource access control provides the capability of denying access to NE resources in the absence of proper authorization. Users may be restricted from executing unauthorized commands, or from accessing information in certain records and fields. For the NE, security-critical functions must be restricted to users with special privileges. This is recommended to control the extent of damage that can be caused by mistakes or malicious actions. Users should possess no more privilege than necessary to perform their job function. This enforces the principle of least privilege.

P4. The NE shall assign and enforce levels of privilege to users, processes and other systems for restricting the use of resources.

S5. DATA AND SYSTEM INTEGRITY

Data and system integrity deals with consistency and reliability issues associated with the NE and its data and software resources.

P5. The NE shall support mechanisms that ensure the integrity of the system and information stored, processed and transmitted by the system.

S6. AUDIT

An audit trail, which supports accountability, is required for a NE. Users should be prevented from modifying audit information.

P6. The NE shall provide an audit log for investigating security relevant events.

S7. SECURITY ADMINISTRATION

Security administration consists of secure management and management of security including proper activation, maintenance, and use of NE security features. It entails tasks such as managing the security database, replacing vendor-supplied default passwords, and customizing the security audit features for OAM&P systems.

P7. The NE shall provide tools for managing security tasks for OAM&P systems by an authorized administrator.

S8. DATA CONFIDENTIALITY

Data Confidentiality deals with protecting against the disclosure of information by ensuring that the data is limited to those authorized or by representing the data in such a way that its semantics remain accessible only to those who possess some critical information (e.g., a key for decrypting the enciphered data).

P8. The NE shall support mechanisms that ensure the confidentiality of sensitive information stored, processed and transmitted by the system.

4.0 DETAILED GUIDELINE

Mechanisms that enforce telecommunications security policies and guard against security intrusions are required. Proper controls will reduce security breaches and financial losses.

This section of the TSG provides baseline security requirements for the NE portion of TMN. Requirements are listed for Identification, Authentication, System Access Control, Resource Access Control, Data and System Integrity, Audit, Data Confidentiality, and Security Administration. The requirements do not address unique security risks and vulnerabilities of specific NE configurations, or particular network environments. The following terminology is used:

* Requirement (R) - A security feature that is *necessary* to ensure the correct functioning of an NE.

* Advisory (A) - A security feature that is *desirable* to ensure the correct functioning of an NE.

4.1 IDENTIFICATION

All authorized users must be uniquely identified to support individual accountability. A user may be a person, a process, or some other system (e.g., an OS, another NE) that accesses or attempts to access the NE to perform tasks or process a call. A user identification code (User-ID) is a non-confidential, unambiguous, and auditable representation of a user.

The requirements for Identification are:

R1. Within a specific NE, the NE shall enforce unambiguous User-IDs to identify its users.[9]

R2. All NE interfaces and ports that accept user command inputs shall require unambiguous User-IDs before performing any actions.

R3. The NE shall internally maintain the identity of all current active users.

R4. The NE shall restrict a User-ID to only one active session.

R5. All operations-related processes running on the NE shall be associated with the User-ID of the invoking user.

R6. If a user-ID has not been used for a specified time interval, the NE shall be capable of disabling that User-ID. In addition, the security administrator shall have a choice of automatic or manual disabling of these User-IDs.

4.2 AUTHENTICATION

[9] The user may be a person, a system, another process, etc. When a process is invoked by another process, the invoked process shall be associated with the ID of the invoking process. Autonomous processes shall have an associated identification code. The use of aliases is permitted only after a user has been properly identified and authenticated.

Authentication is the process of verifying the claimed identity of a session requestor. The confidential authenticator that provides the verification can be based on a password, Personal Identification Number (PIN), token, smart card, biometrics, exchange of keys, etc.

The requirements for Authentication are:

R7. The NE shall verify the identity of all users prior to allowing access.

R8. All NE interfaces and ports that accept user command inputs shall require user authentication before performing any actions.

R9. The NE shall ensure the confidentiality of all internally stored authentication data and protect it from access by unauthorized users.

R10. Reusable passwords transmitted across networks, including wireless or other unprotected channels, shall be encrypted.

R11. The NE shall preserve the confidentiality and integrity of stored authentication information such as passwords, PINs, and authentication tokens.

R12. Authentication information entered during login shall be immediately overwritten within the NE.

R13. The NE shall not permit users to bypass the authentication mechanism.

R14. Only designated security administrators shall be able to access protected authentication information.

R15. The NE shall prohibit the outputting or writing of a clear text representation of authentication information to any printer, terminal, or data entry device.

R16. The NE shall perform the entire authentication procedure even if an invalid User-ID is entered. The NE shall not disclose which part of the authentication is incorrect and shall provide no information to the user other than "invalid attempt."

R17. If reusable passwords are used as the authentication mechanism, then:

a. Users shall not be notified if they select a password already associated with another user.

b. The NE shall permit users to change their passwords only if they have been properly authenticated to the system at the time they make the request.

c. After a password is assigned to a user, the user shall be required to immediately change the password the first time the user establishes a session. Users that do not comply will not be allowed to continue the session.

d. If passwords are used for authentication, the NE shall require a user selected password to have a minimum password length of 6 characters, use both alpha and numeric characters, and use both upper and lower case characters. (See FIPS 112 and FIPS 181 for additional guidance on the selection of passwords).

e. The NE shall require users to change passwords after a specified period of time. Users shall be prevented from choosing a password that they have previously used until a specified period of time elapses.

f. The security administrator shall have the capability of setting the password aging interval and reuse period.

g. The NE shall notify users a specified period of time prior to expiration of their password.

h. The security administrator shall have the capability of setting this time period.

i. Passwords shall not be transmitted in clear text.

A1. The NE should require those users who access the system remotely to use an authentication mechanism stronger than a password.

A2. Users who perform critical administrative and other OAM&P functions should be authenticated by means of a procedure that is stronger than passwords; for example, a biometrics, token-based, or cryptographic technique.

A3. A NE should be able to incorporate and support authentication schemes including those based on trusted third-party servers that provide common dedicated services.

If the authentication mechanism uses public-key encryption technology based on third party servers, then:

a. Users' public keys should be certified by a trusted certification authority (CA) that protects the association of users with their public keys.

b. Users' private keys should not be known by a CA. When a pair of keys are generated for a user, only the public key needs to be shared with the CA.

c. The server should maintain a certificate revocation list (CRL) of all invalid/compromised keys, and prevent the use of such keys.

If the authentication mechanism uses private-key technology based on third party servers, then:

a. The server should support secure registration and timely revocation procedures for user ID/key pairs.

b. The NE should support a secure repository of shared keys for users and services.

4.3 SYSTEM ACCESS CONTROL

The NE must identify and authenticate the session requestor before granting permission to use the system. NE access control mechanisms must provide the security features required for establishing and continuing a session.

The requirements for System Access Control are:

R18. The NE shall not allow access to any user unless identified and authenticated. Only authorized users, processes or remote systems shall be allowed access.

R19. All ports and interfaces of the NE that accept operations-related command inputs shall exercise access control. This includes ports that provide direct, dial-up, and data communications network access.

R20. The NE shall not allow any session to be established via a port that is not designed to accept operations-related command inputs.

R21. The NE shall not provide any default User-IDs that can permit unauthenticated system access.

R22. The NE log-in procedure shall exit and end the session if the user authentication procedure is incorrectly performed a specified number of times. This value shall be set by the security administrator.

R23. Exceeding the threshold for incorrectly performing the user authentication procedure shall be considered a security relevant event. The NE shall notify the security administrator in real time of this occurrence.

R24. When the threshold for incorrectly performing the user identification procedure has been exceeded, the NE shall lock out that log-in port for a specified interval of time.

R25. To prevent unauthorized users from purposely locking out all input ports by performing incorrect user authentications, the default lock-out period shall not exceed 60 seconds. Only the security administrator shall be able to modify that value.

R26. When the threshold for incorrectly performing the user authentication procedure has been exceeded, the NE shall not suspend the associated User-ID. Suspension could allow an unauthorized user to disable all accounts.

R27. When a logical connection is established, but before access, the NE shall provide an advisory warning message regarding unauthorized entry/use and its possible consequences. The message shall comply with applicable local, state, and federal laws.

R28. Upon successful access to the NE, the system shall display for the user the date and time of the user's last successful access to the NE and the number of unsuccessful attempts.

R29. The NE shall automatically disconnect a user and require reauthentication after a specified period of inactivity. The time-out interval shall be set by the security administrator.

R30. The NE shall end a session by means of a secure log-off procedure. The port shall be dropped immediately if the session is interrupted due to causes such as time-out, power failure, link disconnection, etc.

R31. The NE shall be able to incorporate and support mechanisms to grant or deny access to any user based on time-of-day, day-of-week, and calendar date.

4.4 RESOURCE ACCESS CONTROL

The resource access control mechanism limits the use of NE resources, such as processes and databases, based on the principle of "minimum privilege"; i.e., access is granted to only those resources that are needed to perform the job function. Levels of access permission may be assigned to users, data entry devices, and NE ports for restricting the use of NE resources.

The requirements for Resource Access Control are:

R32. The NE shall provide a level of granularity such that for each user allowed access to resources it shall be possible to grant access rights to specific software, processes, databases, data, etc.

R33. Only authorized users shall be allowed access to software in the NE. Software shall be access controlled for overwrite and update, as well as execution rights.

R34. Control of access to resources shall be based on authenticated user identification.

R35. The NE shall provide a level of granularity such that for each resource controlled by the NE it shall be possible to:

1. Grant access rights to a single user, group of users, or a port.

2. Deny access rights to a single user, group of users, or a port.

R36. The NE shall have the capability to screen access to specified resources and restrict a user's ability to perform certain designated operations on the basis of originating address/port. Unauthorized addresses/ports shall be denied access.

R37. Modification of the access rights to a resource shall be allowed only by the owner of that resource or by an appropriate security administrator.

R38. The NE shall provide a mechanism to remove access rights to all resources for a user or a group of users.

R39. The NE shall protect the data files and tables associated with the access control mechanisms from unauthorized access.

R40. Users having predefined roles shall not have default rights to modify their roles and associated rights.

4.5 DATA AND SYSTEM INTEGRITY

Integrity of both the NE system and its data must be ensured. System integrity is concerned with issues related to providing an acceptable level of service. If service interruptions and degradation are not minimized, customers will lose confidence in the system and supplier. Data integrity must be ensured during transmission/reception, processing, and storage of data.

The requirements for Data and System Integrity are:

R41. The NE shall have the capability to identify the original creator of any named or user-accessible NE resources such as data and processes.

R42. The NE shall have the capability to identify the originator of any operations information received via communications networks.

R43. The NE shall provide mechanisms that allow it to periodically validate its correct operation.

R44. The NE shall have the capability to protect the integrity of stored data by performing cryptographically-based integrity checks (e.g., message authentication code) and/or data updates.

R45. The NE shall be designed and developed to protect data integrity by checking inputs for reasonable values.

R46. Documentation for the NE shall contain recommendations for running, on a regular basis, integrity checking utilities for file systems and disks.

R47. A non-privileged user action, either deliberate or accidental, that requests NE resources shall not cause denial of service of the NE to other users.

R48. Mechanisms shall be provided to allow the NE to recover from a failure or discontinuity without risk of compromising security.[10]

R49. To facilitate recovery, and to reduce the potential impact of a security compromise, check points shall be included in the software.

R50. The NE shall provide mechanisms to preserve the integrity of data stored internally to the NE.

R51. The NE shall have the capability to verify the integrity of new software releases and subsequent patches.

R52. The NE shall process security alarms in real-time based on indicated severity levels.

4.6 AUDIT

The audit log provides the capability to investigate unauthorized activities after they occur so that proper remedial action can be taken. The requirements for Audit are:

R53. The NE shall generate logs that contain information about security relevant events. Items selected for recording shall be defined and selected by the security administrator. The logs shall enable security administrators to investigate losses and improper actions on the part of users, legitimate and otherwise, and to seek legal remedies.

[10] For example, if the system is halted to download new or modified software, or a system restart is required.

R54. The NE shall provide audit capabilities with user accountability for all significant events. The user-identification associated with any request or activity shall be maintained and passed on to any other connected systems so that the initiating user can be traceable for the lifetime of the request or activity.

R55. The audit log shall be protected from unauthorized access or destruction by means of access controls based on user and channel privileges.

R56. The audit log and audit control mechanisms shall be protected from modification or destruction.

R57. The audit log and audit control mechanisms shall survive system restarts by being maintained throughout a system restart.

R58. Subject to selections made by the security administrator, the audit log shall minimally record information on the following events:

1. Changes to the NE security configuration.
2. Modifications of NE software.
3. Invalid user authentication attempts.
4. Unauthorized attempts to access resources such as data, the password file, and transactions.
5. Changes to a user's security profile and attributes.

R59. For each recorded event, the audit log shall record the following:

1. Type of event.
2. Date and time of event.
3. User identification including associated terminal, port, network address, or communication device.
4. Names of the resources accessed.
5. Success or failure of the event.

R60. The security administrator shall be immediately notified if the audit log fails to record the events that are required to be recorded.

R61. It shall not be possible to disable the audit log of actions taken by a security administrator.

R62. Authentication information such as passwords, PINs, and cryptographic keys shall not be recorded in the security log.

R63. In order to prevent overwriting any information, the NE shall be capable of automatically forwarding the audit log to a storage device or authorized management system. Any transmission of audit information shall be done securely.

R64. When the audit log is copied to other media or locations, the copy shall start at the oldest record and copy sequentially without deleting any records.

R65. The NE shall support audit analysis tools that can produce exception reports, summary reports, and detailed reports on specific data items, users, or communication facilities.

4.7 SECURITY ADMINISTRATION

Security administration mechanisms enable a human administrator to control the security of an NE. This administrator must have proper authorization to perform security administration functions such as setting security parameters, removing default values, and updating security features.

The requirements for Security Administration are:

R66. The NE shall separate administrator functions from other user functions. Only authorized security administrators shall be allowed to execute these functions.

R67. The security functions performed by authorized administrators shall be identified and documented.

R68. The NE shall provide a mechanism for an authorized administrator to display all currently active users or software processes. These processes include both OAM&P and telecommunications service applications.

R69. The NE shall provide a mechanism for an authorized administrator to be able to independently and selectively review the action of any one or more users, including privileged users, based on individual user identity. Note: due to privacy considerations, users must be aware that this capability exists. (See CSL Bulletin, "Guidance on the Legality of Keystroke Monitoring," March 1993.)

R70. The NE shall provide a mechanism that permits an authorized administrator to monitor the activities of a specific terminal, port or network address in real time. (See note in R69)

R71. The NE shall provide a mechanism to allow an authorized administrator to lock out a specific port or channel.

R72. The NE shall provide a mechanism to allow an authorized administrator to authorize or revoke users.

R73. The NE shall provide a mechanism to allow an authorized administrator to identify all resources owned by or accessible to any specific user along with the associated access privileges.

R74. The NE shall provide a mechanism to allow an authorized administrator to create a unique User-ID for a particular user.

R75. The NE shall provide a mechanism to allow an authorized administrator to disable User-IDs after a specified period of time during which the user-ID has not been used.

R76. The NE shall provide a mechanism to allow an authorized administrator to reinstate or delete a disabled User-ID.

R77. The NE shall provide a mechanism to allow an authorized administrator to enter, reset, or delete passwords for users.

R78. An authorized administrator shall not be able to retrieve any password in clear text.

R79. The NE shall provide the capability to generate alarms for specifiable security events. The alarms shall be prioritized based on pre-determined criteria and routed to the security administrator. Only an authorized security administrator can deactivate an alarm.

R80. The following security parameters shall be specifiable and adjustable by an authorized security administrator:

1. The period after which a password must be changed.

2. The interval during which an expired password shall be unselectable as a new password by the same user.

3. The threshold on the number of incorrect login attempts which, when exceeded, would cause immediate notification.

4. The duration of channel lock-out that occurs when the threshold on the number of incorrect logins is exceeded.

5. A customized advisory warning banner that is displayed upon system entry regarding unauthorized use, and the possible consequences of violating the warning.

6. The duration of the inactivity time-out interval for an established session.

7. The access rights of a user to a resource.

8. The events that may trigger alarms (e.g., failed login attempts), the levels of alarms (e.g., critical, major, minor, etc.), the type of notification (e.g., bell and/or message), and the routing of the alarm (e.g., specific port).

9. Parameters for the mechanism that notifies users of the need to change passwords shall be specifiable and adjustable by an authorized administrator. This includes how far in advance users shall be notified, and the grace period for using an expired password.

R81. The NE shall provide a mechanism to allow an authorized administrator to periodically validate the correct operation of the NE with respect to the supported applications.

4.8 DATA CONFIDENTIALITY

There are conditions where the confidentiality of data must be ensured. Data Confidentiality should be ensured during transmission/reception, processing, and storage of data.

The requirements for Data Confidentiality are:

R82. The type of data items and structures whose confidentiality is protected shall be identified. For example, if data is transmitted, some identifier might accompany the transaction which would identify the key and related attributes needed by the receiving system.

R83. The system shall have the capability of protecting the confidentiality of each individual message or selective fields of each message.

R84. The NE shall support mechanisms that ensure the confidentiality of communication information by encryption if the communication media cannot be protected by physical and administrative means.

5.0 DEVELOPMENT LIFE CYCLE REQUIREMENTS

NE security features are not sufficient by themselves to provide a secure NE. Security has to be considered throughout the life cycle of the NE. Security features and mechanisms need to be properly conceived, designed, implemented, tested, installed, documented, and maintained.

This section describes generic security requirements for the various phases of the NE development life cycle. The purpose is to ensure the development of NE security features with reliability, integrity and robustness. In addition, vendor support is necessary to ensure NE security.

5.1 SECURITY POLICY

R85. The NE vendor shall have a security policy that governs software development, integrity, and maintenance throughout the life cycle of the NE product.

5.2 REQUIREMENTS ANALYSIS

R86. Security requirements shall consist of the baseline security features described in Section 4.

R87. For specific applications, it may be necessary to perform a risk analysis to determine if additional measures commensurate with the relative threats, vulnerabilities, and values of the resources (application) being protected are needed. This risk analysis shall include:

a. Nature of NE data, software, and functions used by the application.

b. Potential risk if the security baseline is not followed.

c. Impact on NE data, software, and functions if they are compromised on the NE or associated systems and networks.

5.3 SYSTEM DESIGN

R88. The design shall not allow for a mode of entry that is not a documented feature.

R89. The functional requirements shall be based on the application requirements defined during the requirements analysis phase.

R90. The functional requirements shall be documented.

R91. The design shall accommodate the various roles that a user may take on when accessing the NE.

R92. The security functions available to be performed by an appropriate administrator shall be identified and documented.

R93. If there is a feature to support the enabling and disabling of a privileged account, the software functions shall not allow a user with limited privilege to become a highly privileged user in any context, except with administrator intervention.

R94 Limited-privilege users shall not be able to access the underlying software operating environment unless that environment can support the defined access control policies and the user is given the higher privilege by administrator action.

5.4 DETAILED SYSTEM DESIGN

R95. The design shall specify security mechanisms, based on the target operating environment and supported applications, to satisfy the functional requirements.

R96. The specified security mechanisms shall be documented.

R97. The design review process shall address the functional requirements as well as the potential for unintended security flaws and malicious attacks.

5.5 IMPLEMENTATION

R98. Security mechanisms defined in the detailed design shall be implemented.

R99. No method of NE access, including access for software debugging, shall be provided other than what was designed and documented.

R100. Passwords used during the design and implementation phases shall not be stored in cleartext in unprotected databases or files.

R101. If a password is used in cleartext form in an executing process, the password shall be overwritten immediately after use within the NE.

R102. NE software shall be treated as proprietary and labeled with appropriate markings. These markings shall reside with the software when it is in the NE and when the software is listed in any documentation.

5.6 DEVELOPMENT ENVIRONMENT

R103. NE vendors shall have documented security policies that address the secure use and maintenance of the computer systems and software used in the development of the NE.

R104. All systems and software used in developing the NE shall be subject to periodic security audits.

R105. Passwords, and other forms of personal authentication, used by key software developers and other privileged users, shall be protected and subject to appropriate complexity requirements.

R106. Passwords used during the development phase shall not be stored in clear text in unprotected databases, workstations, or networks.

R107. Third party (e.g., commercial software vendor) software used in NE development shall be obtained in an authorized manner with appropriate approvals.

R108. Public domain and other types of commonly available software (free-ware, share-ware etc.) shall not be used in NE development unless the software has been inspected, in source form, by an approved authority.

R109. Software that is developed internally by a vendor for use in NE development shall be approved by an appropriate authority within the development environment.

5.7 SYSTEM TEST

R110. All security features shall be tested for flaws by the vendor. The tests shall be conducted under conditions that simulate normal use as well as emphasizing penetration attacks that target the software security features.

R111. Security flaws detected during testing shall be corrected, removed, or neutralized and the software retested to demonstrate that the flaws have been eliminated and that no new flaws have been introduced.

R112. The vendor's test plan, procedures, suites, and results shall be verified and documented by an independent vendor testing group.

5.8 PACKAGING AND DELIVERY

R113. Only authorized software and software modifications shall be added to the software baseline to form the product baseline.

R114. All software changes shall be tested, verified, documented and reviewed to determine that NE security has not been compromised.

R115. There shall be tools and procedures to generate a new version of the NE software from backup media or source code.

R116. There shall be tools and procedures for verifying that a software release contains all of the appropriate component modules.

R117. There shall be tools and procedures for protecting the backup media and source code from unauthorized modification.

R118. The master copy of all routines used to generate the NE software shall be logically, physically, and procedurally protected from unauthorized modification and destruction.

R119. The vendor shall maintain a master database of all delivered software releases by release number.

R120. All NE software shall be delivered with secure installation defaults.[11]

R121. Passwords associated with default User-IDs delivered with a NE software release shall be modifiable by the administrator during the installation process.

[11] For example, audit features should be enabled, default accounts should be password protected, etc.

R122. The NE vendor shall provide procedures that enable the user to conduct a site security acceptance test that demonstrates conformance to the security requirements.

R123. The user shall be provided with tools and procedures to verify, at any time, that the currently installed software has remained consistent with the delivered software, i.e., no unauthorized modifications.

R124. Vendor documentation shall be delivered with the distributed software.

5.9 DOCUMENTATION

R125. Instructions for and descriptions of security features and items for consideration shall be provided for all of the NE users, including administrators and operators.

R126. The documentation shall have the appropriate proprietary markings.

R127. General user documentation shall not contain any information that could compromise NE security if publicly disclosed. Actual passwords shall not be listed in the documents.

R128. A User Guide that describes all security features, and provides guidelines on their use, shall be provided.

R129. There shall be a System Administration Guide that contains:

1. Description of security features and protection considerations for securing the NE;
2. Description of security tools used to examine the security of the NE and guidelines on the use of these tools;
3. Recommendations for configuring the security related parameters of the NE software;
4. Guidelines on the administrator functions and activities needed to secure the NE;
5. Guidelines on security self-assessment techniques to assess and maintain NE security.
6. Guidelines on monitoring and maintaining the availability of the NE and its resources to detect and prevent denial of service attacks and to maintain the integrity of security features (e.g., log space to record system activity).

R130. The System Operations Guide shall describe procedures to initially start the NE in a secure manner and to restart and recover the NE after various system events.

R131. Documentation shall be distributed through authorized channels.

5.10 SUPPORT

R132. The vendor shall identify a primary and secondary point of contact for addressing and resolving issues related to the security of the NE.

R133. The vendor shall have a documented method for notifying users of new or recurring security problems.

R134. All problems that pose a security threat to the NE shall be prioritized and addressed in the order of highest threat to the NE.

R135. If security problems are identified by the vendor in a supported release, the vendor shall make that information available to authorized user representatives in a protected fashion.

R136. If possible, security fixes to identified security problems shall not require the installation of the next release of the NE software.

R137. All user login information and access configurations shall be protected by the vendor and treated in a restricted manner.

R138. Vendor personnel shall not access the NE, either remotely or on the user's site, without prior authorization from the user.

R139. Vendor personnel accessing an NE shall not bypass user security procedures.

R140. All new software features and patches shall be tested first on a development system and approved by an appropriate testing organization, prior to installation on an operational system.

R141. Tests that modify live data shall not be performed.

R142. A risk analysis shall be conducted of proposed software changes to determine their impact on NE security.

R143. Any changes to security features or security defaults shall be documented and made available to the user before the software is distributed.

R144. All maintenance and feature releases shall be subject to the entire set of development life cycle requirements.

R145. Documentation shall be provided that describes the secure administration, operation and use of new software features and fixes.

LIST OF ACRONYMS

CA	Certification Authority
CCITT	Comite Consultatif International Telegraphique et Telephonique
CPE	Customer Premise Equipment
CRL	Certificate Revocation List
DCN	Data Communications Network
EM	Element Manager
FCC	Federal Communications Commission
I&A	Identification and Authentication
ISDN	Integrated Service Digital Network
MD	Mediation Device
NE	Network Element
NIST	National Institute of Standards and Technology
NOF	Network Operations Forum
NS/EP	National Security and Emergency Preparedness
NSTAC	National Security Telecommunications Advisory Committee
OAM&P	Operations, Administration, Maintenance, and Provisioning
ONA	Open Network Architecture
OS	Operations System
PBX	Private Branch Exchange
PIN	Personal Identification Number
PSN	Public Switched Network
SONET	Synchronous Optical Network
STP	Signal Transfer Point
TCSEC	Trusted Computer System Evaluation Criteria
TMN	Telecommunications Management Network
TSG	Telecommunications Security Guideline
WS	Workstation

REFERENCES

[1] National Research Council. Growing Vulnerability of the Public Switched Networks. National Academy Press, 1989.

[2] National Security Telecommunications Advisory Committee. Report of the Network Security Task Force. National Security Telecommunications Advisory Committee, 1990.

[3] Federal Communications Commission. Computer Inquiry III, FCC, June 1986.

[4] S.E. Dolan. Open Network Architecture from an Operational Perspective. In IEEE Globecom. IEEE, 1988.

[5] L. Simpson. Open Network Architecture: OAM Perspective, an RBOC's View. In IEEE Globecom. IEEE, 1988.

[6] G. Giridharagopal S. Homayoon. ONA: Demands on Provisioning and Performance. In IEEE Globecom. IEEE, 1988.

[7] F.S. Dworak. Approaches to Detecting and Resolving Feature Interactions. In Proceedings, IEEE Globecom. IEEE, 1991.

[8] Installation and Maintenance Responsibilities - SS7 Link and Trunk Installation and Maintenance Access Services; Network Operations Forum Reference Document, Issue 3, Jan 1993.

[9] Generic Requirements for Network Element Security, Technical Report TR-NWT-000815, Issue 2, Bellcore, 1992.

[10] Bellcore Operations System Security Requirements, Technical Report TA-STS-001194, Bellcore, 1991.

[11] Bellcore Standard Operating Environment Security Requirements, Technical Report TA-STS-001080, Bellcore, 1990.

[12] NISTIR 5153, Minimum Security Requirements for Multi-User Operating Systems, March 1993.

[13] CSL Bulletin, Guidance on the Legality of Keystroke Monitoring, March 1993

[14] Bellcore Technical Advisory, TA-NWT-001469, Issue 1, September 1993, Generic Requirements on Security for OSI-Based Telecommunications Management Network Interfaces.

[15] Bellcore Technical Reference, TR-NWT-000815, Issue 2, December 1992, Network Element (NE) Memory Administration - Network Element and Network System Security.

[16] CCITT Recommendation M.3010, Principles for a Telecommunications Management Network.

[17] American National Standard for Telecommunications; Operations, Administration, Maintenance, and Provisioning (OAM&P) - Principles of Functions, Architectures and Protocols for Telecommunications Management Network (TMN) Interfaces ANSI T1.210,1993.

[18] Office of the Manager, National Communications Systems, The Electronic Intrusion Threat to National Security and Emergency Preparedness (NS/EP) Telecommunications: An Awareness Document, Second Edition, December 5, 1994.

[19] NCS Manual 3-1-1, Telecommunications Service Priority (TSP) System for National Security Emergency Preparedness (NS/EP) Service User Manual, July 9, 1990.

[20] American National Standard for Telecommunications; Operations, Administration, Maintenance, and Provisioning (OAM&P) - Baseline Security Requirements for Telecommunications Management Network (TMN), ANSI T1.243,1995.

[21] American National Standard for Telecommunications, Security Framework for Telecommunications Management Network (TMN), ANSI T1.233-1993.

[22] NIST SP 800-11, The Impact of the FCC's Open Network Architecture on NS/NP Telecommunications Security, February, 1995.

[23] CCITT Recommendation X.700, Management Framework Definition for Open Systems Interconnection (OSI) for CCITT Applications.

APPENDIX

1.0 GUIDING NETWORK ARCHITECTURE

The Telecommunication Security Guideline (TSG) effort is guided by the Telecommunication Management Network (TMN) architecture as specified in CCITT and ANSI documents (See Figure 2, TMN Logical Network)

TMNs provide an organized architecture to interconnect various types of operations oriented application systems and/or telecommunications network equipment. The architecture permits information exchange by means of standardized interfaces, protocols and messages.

A TMN exchanges management information among the various TMN components. Within the context of the TMN, *management* refers to a set of capabilities to allow for the exchange and processing of management information to assist administrators in conducting their business efficiently.

A TMN can vary in complexity from a simple connection between an Operations System (OS) and a single piece of telecommunications equipment to a complex network interconnecting many different types of OSs and telecommunications equipment. The component parts of a TMN include:

* Operations Systems (OS) - Systems that perform operations functions, i.e., activities required to provide the services of a telecommunications system to users/subscribers. The OS supports the processing of information related to operations, administration, maintenance, and provisioning (OAM&P) for telecommunications networks.

* Network Elements (NE) - Analog and digital devices and supporting equipment that provide communication services such as switching, multiplexing, and transport services to subscribers. NEs also support network maintenance, billing and administration functions.

* Data Communication Networks (DCN) - Communication networks within TMNs that transport information related to telecommunication management between function blocks. These function blocks, in various TMN components, provide the general functions to perform OAM&P (See Figure 2). In its simplest form, a DCN may be a point-to-point connection.

* Mediation Devices (MD) - Devices that act on the content of information passing between network elements and operations systems. MDs may provide any of the following: upper layer protocol internetworking, adaptation, filtering, format conversion, storage, thresholding, condensing information, and decision making.

* Workstations (WS) - Collections of hardware and software that perform workstation functions, i.e., provide a human user with entry into or exit from a TMN component such as a NE or OS. A personal computer (PC) or computer terminal can function as a workstation.

* Q Adapters (QA) - Devices that act on the content of information passing between TMN function blocks and non-TMN function blocks. Protocols carrying the information may be converted. QAs also support interfaces between TMN components and OSs and NEs that belong to the same jurisdiction as the TMN but do not conform to TMN standards.

1.1 DISTINCTION BETWEEN OSs AND NEs

Traditionally the major distinction between OSs and NEs has been that NEs forward switch and transport information between subscribers of the network while OSs do not perform any activities on a per call basis. This distinction is fading with the emergence of network systems that assist in call handling; for example, 800 number translation databases that do not carry any user information.

NEs interact essentially through signaling for call setup and disconnect. In this situation there is no direct exchange of management information between NEs (though NEs participate in the transport of such information between OSs and NEs). Future developments may result in NEs, such as Synchronous Optical Network (SONET) digital cross connects, that exchange management information (not related to any specific call) to execute circuit rearrangements.

Different performance requirements for NEs and OSs generally exist. Communications involving NEs are usually more time critical since they involve the allocation and availability of network resources and hence the quality of service as seen by the end users. By contrast, the exchange of management information by an OS is usually less time critical.

OSs perform functions such as surveillance, testing, performance monitoring, provisioning, and traffic management. The OSs and NEs interface with people through end-user systems such as terminals and workstations (WS). The OSs and NEs may also interface with external entities (OSs and WSs that are outside the TMN). Such interfaces, as well as some interfaces that are internal to the TMN, may go through a Mediation Device (MD) or an NE acting in the role of a gateway.

1.2 DATA COMMUNICATIONS NETWORK (DCN)

The OSs and NEs, as well as the workstations, are interconnected via a Data Communications Network (DCN). The DCN provides information transport mechanisms, including routing functions based on layers 1 through 3 of the OSI Reference Model (i.e., physical, data link, and network layers).

Figure 2 illustrates the general relationship between a TMN and a telecommunications network that it manages. A TMN is conceptually a separate network that interfaces a telecommunications network at several different points to send/receive information to/from it and to control its operations. The telecommunications network consists primarily of NEs that are organized to support services invoked by telecommunications-enabled user devices (e.g., telephones). A TMN may use parts of the telecommunications network to provide its communications and to enable management of the TMN.

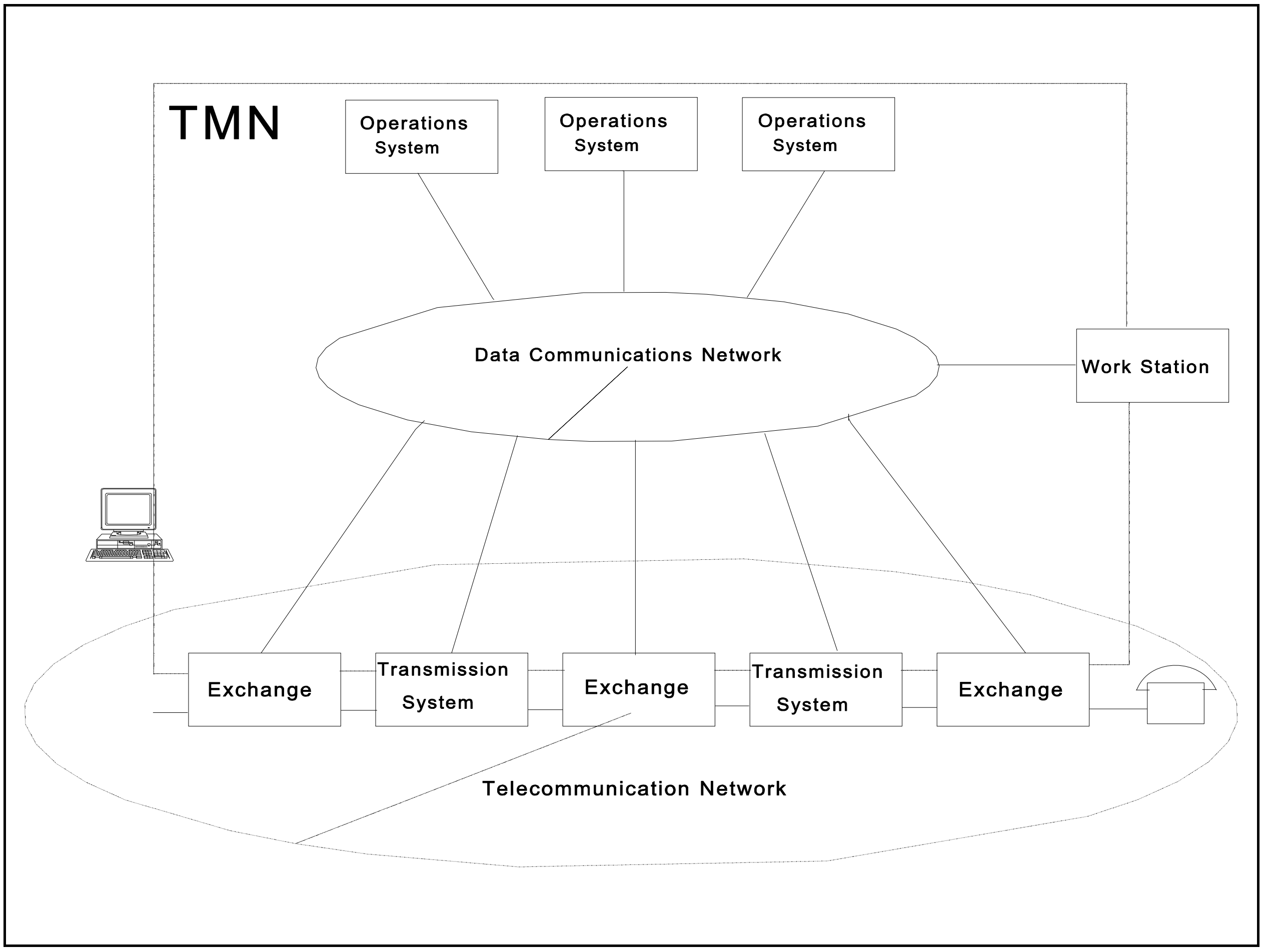

Figure 2 – TMN Logical Network (General Relationship of a TMN to a Telecommunications Network).

It is important to realize that a TMN only depicts a network environment that is under the control of one administrative domain. Later phases of the TSG effort will embrace the security issues that arise when TMNs are interconnected.

1.3 FIELD OF APPLICATION

The following are examples of the networks, telecommunications services and major types of equipment that may be managed by the TMN:

* Public and private networks, including ISDNs, mobile networks, private voice networks, private virtual networks and advanced intelligent networks;

* TMN itself;

- Transmission terminals (multiplexers, cross connects, channel translation equipment, etc.);
- Digital and analog transmission systems (cable, fiber, radio, satellite, etc.);
- Operations systems and their peripherals;
- Mainframes, front-end processors, cluster controllers, file servers, etc.;
- Digital and analog exchanges;
- Area networks (WAN, MAN, LAN);
- Circuit and packet switched networks;
- Signaling terminals and systems including signal transfer points (STPs) and real time data bases;
- Bearer services and teleservices;
- PBXs, PBX accesses and user (customer) terminals;
- ISDN user terminals in accordance with relevant maintenance procedures for public networks;
- Software provided by or associated with telecommunications services, e.g., switching software, directories, message data bases, etc.;
- Software applications running within mainframes, etc. (including applications supporting TMN);
- Associated support systems (test modules, power systems, air conditioning units, building alarms systems, etc.).

In addition, a TMN may be used to manage distributed entities and services offered by grouping items in the above list.

1.4 BASIC OBJECTIVES FOR THE TMN

The objective for the TMN specifications is to provide a framework for telecommunications management. By introducing the concept of generic network models for management, it is possible to perform general management of diverse equipment using generic information models and standard interfaces.

The principle of keeping the TMN logically distinct from the networks and services being managed introduces the prospect of distributing the TMN functionality for centralized or decentralized management implementations. This means that operators can perform management of a wide range of distributed equipment, networks and services from a number of management systems.

Security and distributed data integrity are recognized as fundamental requirements for the definition of a generic architecture. A TMN may allow access and control from sources considered outside the TMN (e.g., inter-TMN cooperation and network user access). Security mechanisms may be needed at various levels (managing systems, communications functions, etc.)

1.5 FUNCTIONS ASSOCIATED WITH A TMN

A TMN is intended to support a wide variety of management areas that cover the planning, installation, operations, administration, maintenance and provisioning of telecommunications networks and services.

The specification and development of the required range and functionality of applications to support the above management areas is a local matter. Some guidance, however, is provided by CCITT which has categorized management into five broad management functional areas (Recommendation X.700[23]). These areas provide a framework within which the appropriate applications can be determined with respect to support for the administration's business needs. The management functional areas are:

* Performance Management;

* Fault Management;

* Configuration Management;

* Accounting Management;

* Security Management.

Some of the information that is exchanged within the TMN may be used in support of more than one management area. The classification of the information exchange within the TMN is independent of the use that will be made of the information.

Overall the functionality of the TMN consists of the ability to:

* Exchange management information across the boundary between the telecommunications environment and TMN environment;

* Convert management information from one format to another so that management information flowing within the TMN environment has a consistent nature;

* Transfer management information between locations within the TMN environment;

* Analyze and react appropriately to management information;

* Manipulate management information into a form that is useful and/or meaningful to the management information user;

* Deliver management information to the management information user and to present it with the appropriate representation;

* Ensure secure access to management information by authorized management information users.

1.6 ARCHITECTURAL REQUIREMENTS

TELECOMMUNICATION SECURITY GUIDELINE FOR TMN

The TMN needs to be aware of telecommunications networks and services as collections of cooperating systems. The architecture is concerned with orchestrating the management of individual systems to have a coordinated effect upon the network. Introduction of TMNs gives administration the possibility to achieve a range of management objectives, including the ability to:

- Minimize management reaction times to network events;
- Minimize load caused by management traffic where the telecommunications network is used to carry it;
- Allow for geographic dispersion of control over aspects of the network operation;
- Provide control mechanisms to minimize security risks;
- Provide control mechanisms to locate and contain network faults;
- Improve service assistance and interaction with customers.

To take into account at least the above objectives, the TMN architecture should:

- Make various implementation strategies and degree of distribution of management functionality possible;
- Allow for management of heterogeneous networks, equipment and services within a telecommunications environment;
- Allow for compartmented structure, where management functions may operate autonomously within the compartment;
- Allow for technological and functional changes;
- Include migration capabilities to enhance early implementation and allow future refinement;
- Provide a certain degree of reliability and security in the support of management functions;
- Make it possible for customers, value added service providers, and other domain administrations to access management functions;
- Make it possible to have different, or the same, management applications at different locations, even if they access the same NE;
- Address the requirements of small and large numbers of managed objects;
- Make the interworking between separately managed networks possible, so that inter-network services can be provided between domains;
- Provide for management of hybrid networks consisting of mixed network equipment;
- Allow flexibility in the degree of reliability/cost trade-off in all the network management components.