1

INTRODUCTION

At the very outset of this book, questions worth asking are:

- What is the author referring to by the word "security?"
- What is the author referring to by the words "security management?"
- What are next-generation networks and services?

Security is a word whose meaning seems to change depending on the context where it is used and by the "mindset" or background of the individual. Some people think security is solely about "chain-link" fences, security guards, burglar alarms/video cameras, etc. Other people think security is about the use of encryption, login passwords, "firewalls," etc. Then there are those who believe security is only an issue for military-intelligence type organizations and of no importance, or a hindrance, to commercial and other enterprises, as allegedly overheard at a meeting of security people (Kaufman et al., 2002):

Speaker: Isn't it terrifying that on the Internet we have no privacy?
Heckler 1: You mean confidentiality. Get your terms straight.
Heckler 2: Why do security types insist on inventing their own language?
Heckler 3: It's a denial of service attack.

Security Management of Next Generation Telecommunications Networks and Services,
First Edition. Stuart Jacobs.

The aforementioned simply exemplifies how words become confused, misused, or ambiguous, when talking about security.

This problem just grows when the phrase "security management" appears. Does security management refer to:

- the management of technology related to security?
- the management of security activities?
- security for information processing management activities?
- security of organizational management activity?

or

- all of the above?

Again it depends on the individual as to which of the aforementioned is germane.

Then there is the term "Next-Generation Network," usually abbreviated as NGN. What is an NGN? What technologies are used by an NGN? How does an NGN differ from today's Internet Protocol (IP)-based networks and the existing Public Switched Telephone Networks (PSTNs)? A wide number of subjects need to be considered to answer the previous questions and should be addressed in an order that builds upon a number of foundation concepts.

The goal of this book is to provide an answer to these questions.
This chapter discusses:

- How the very concept of networking has evolved over time;
- The evolution of network security concepts from a standards perspective;
- Network and security management systems;
- The evolution of network and security management concepts;
- How the management of information security needs have changed over time.

Chapter 2 discusses:

- How modern networks have evolved over time;
- Common network organizations including: wired, wireless, metropolitan area, wide area, Supervisory Control and Data Acquisition (SCADA), sensor networks, and clouds;
- Next-Generation Network framework and architecture concepts;
- The evolving IP Multimedia Subsystem (IMS) organization of services.

Chapter 3 discusses:

- How cybercrime has become a significant information security driver;
- The evolution of information security governance into a core organizational management component;

- The primary information security management frameworks and the relative advantages/disadvantages to each framework;
- A holistic information security management approach leveraging the strengths of existing frameworks.

Chapter 4 discusses:

- Asset identification and developing an inventory of organizational assets;
- Analyzing the impact when organizational assets are damaged, lost, or made unavailable due to accidental or malicious human activities;
- Procedural risk mitigation controls;
- Technical risk mitigation controls acquisition or development;
- Risk mitigation controls deployment testing.

Chapter 5 discusses:

- Security within Element and Network Management Systems (EMS/NMS);
- Telecommunications Management Network (TMN) Security;
- Operations Support Systems (OSSs) Security Needs;
- A Security Management Framework as defined by ITU-T Recommendation M.3410;
- Operational Security Compliance Programs;
- Security Operations Reviews and Audits;
- Security Event Response and Incident Management;
- Penetration Testing;
- Common Criteria Evaluated Systems;
- Accreditation and Certification;
- Withdrawal from service.

Also included are a wide variety of appendices including:

Appendix	Presents
A	Provides a synopsis of basic cryptography concepts; Explores major aspects of crypto-analysis and key management; and Describes the primary approaches for cryptographically based authentication.
B	Describes the Kerberos and Public Key Infrastructure (PKI) authentication systems; Reviews issues associated with human authentication; Describes the capabilities of RADIUS-, LDAP- and Diameter-based authentication.
C	The Data Link Layer Security Mechanisms IEEE 802.1q, IEEE 802.1x, IEEE 802.11i; The IP Security (IPsec) inter-networking Security Mechanism; Network Authorization and Access Control mechanisms for: Firewalls, Application-level Gateways and IPS/IDS; Transport protocol security mechanisms: TLS, DTLS, SSL and Secure Shell (SSH); Application Security Mechanisms; The Web application Security Mechanisms: XML, SOA, SOAP and SAML; and

(*continued*)

Appendix	Presents
	Anti-Malware Applications for malware and spyware Scanning, Host Based Firewalls, Modification Scanners and Host Based IPS/IDS.
D	An example Organization security policy document based on the ISO/IEC 27002 standard that can serve as a starting point for developing customized policy documents.
E	An example decomposition of the example security policy document in Appendix D into detailed enterprise security functional requirements that can serve as a starting point for developing customized policy documents.
F	An overview of commonly used networking protocols in the data link, internetworking, transport, and application layers along with know attacks that leverage vulnerabilities within different protocols.
G	A comparison of security functionality covered by ITU-T Recommendations M.3400 and M.3050.
H	The state level personally identifiable information privacy—breach notification laws enacted within the United States as of 2010.
I	An example set of detailed information security related functional requirements that can be used in Requests for Proposals (RFPs).
J	An example Microsoft Excel spreadsheet that can be used for evaluating supplier proposals based on the requirements found on Appendix I.
K	An example Security Statement of Work (SOW) that can be used in contract negotiations.
L	An example set of Solaris Operating System security audit procedures.
M	An example set of Microsoft XP Operating System security hardening procedures.
N	An example set of network security audit procedures.
O	An example set of generic Unix Operating System security audit procedures.

1.1 EVOLUTION OF NETWORKING CONCEPTS

Through the 1960s and 1970s, there were two approaches to networking:

- the Public Switched Telephone Network (PSTN), commonly referred to as telephony, and
- computer/data communications networks.

Each approach evolved independently of the other and represented very different views regarding how devices should communicate and who should control the technology.

1.1.1 The Public Switched Telephone Network

The Public Switched Telephone Network (PSTN) was a government-sanctioned and regulated monopoly of "telephone companies" with about 65% owned and operated by AT&T,[1] about 30% owned and operated by GTE,[2] with the remaining 5% by some 20 very small independent owners/operators. As AT&T represented the largest PSTN

[1] American Telephone & Telegraph Corporation (AT&T), also referred to as the Bell System.

[2] General Telephone & Electronics (GTE).

operator, its Bell Laboratories was the driving force for the development of most PSTN technologies (especially network interfaces and protocols), since the other much smaller operators all had to interconnect with AT&T's infrastructure. Only following the 1968 U.S. Supreme Court "Carterphone" decision (and FCC ruling 13 F.C.C.2d 420), regarding modems,[3] were devices not supplied by the telephone company allowed to be interconnected to telephone networks. Even after the "Carterphone" decision, up through the 1990s, PSTN technology evolution was primarily controlled by PSTN operating companies and their equipment suppliers. Starting in the 1990s, Standards Development Organizations (SDOs) and industry forums began to have a major impact on PSTN technology. The major SDOs and forums impacting PSTN technology development have been the:

- International Telecommunication Union-Telecommunications (ITU-T) Standardization Sector whose predecessor was the International Telegraph and Telephone Consultative Committee (CCITT);
- Telecommunications Industry Association (TIA);
- Alliance for Telecommunications Industry Solutions (ATIS);
- European Telecommunications Standards Institute (ETSI);
- International Standards Organization (ISO); and
- 3rd Generation Partnership Project (3GPP).

Presently, these and numerous other organizations have assumed a significant role in defining how telephony-related technology should evolve.

1.1.2 Computer/Data Communications Networks

Computer/data communications network technology through the 1960s and 1970s was predominately controlled by computer manufacturers who developed network capabilities specifically to support their proprietary product lines. During this era, IBM[4] represented over 70% of all computers sold; consequently, other computer manufacturers routinely provided some degree of interoperability with IBM's networking technology. Virtually all of these proprietary computer networking capabilities were based on bit synchronous link protocols and used of an end-to-end connection approach between end computer systems. Each computer manufacturer developed their unique networking capabilities according to a proprietary network architecture[5] that was not subject to non-company external review or approval. In the 1980s, work on the concept of connectionless packet networking, independent of any single computer manufacturer, started to mature with the publication of the U.S. Government Defense Advanced Research Projects Agency sponsored, and in many cases Internet

[3] A modem (modulator-demodulator) is a device used for converting digital signals into, and recovering them from, quasi-analog signals suitable for transmission over analog communications channels such as the PSTN.

[4] IBM was the common abbreviation for the International Business Machine Corporation.

[5] A network architecture specifies the design of a communications network via a framework for the specification of a network's physical components, functional organization, protocols, data/message formats, and operational principles and procedures.

Engineering Task Force published, Request for Comments (RFCs) 791,[6] 792,[7] and 793[8] (defining IPv4, ICMPv4, and TCPv4) that are the foundation protocols for the modern Internet Suite of protocols and defined basic packet internetworking and end-to-end transport capabilities for generalized connectionless networking. By the early 1990s, IPv4 and TCPv4 had become de facto standards for computer-to-computer communications with the responsibility for these, and many other protocols, under the control of the Internet Engineering Task Force (IETF). Virtually all computers now include native Internet Protocol (IP-) and Transmission Control Protocol (TCP)-based communications capabilities. It must be noted that IETF protocol development does not follow any formalized network architecture beyond relying on the use of IP, TCP, and User Datagram Protocol (UDP).

1.1.3 Network Architectures

The first approach to developing a non-proprietary network architecture resulted in the publication by the ISO of document ISO/IEC 7498-1[9] in 1984, known as the Open System Interconnect (OSI) model.[10] It was quickly followed by three other standards, ISO/IEC 7498–2,[11] ISO/IEC 7498–3,[12] and ISO/IEC 7498-4.[13] The major contributions of these standards have been:

- Formal introduction of the concept of layering protocols, that operate on an end-to-end basis upon other protocols that provide interconnection/forwarding capabilities that provide basic communications link functions;
- The concept that a protocol should only utilize information about another protocol (either above it or below it) that is available via a well-defined interface, thereby allowing the internal structure or operation of a protocol to be changed without negatively impacting other protocols; and

[6] RFC 791, INTERNET PROTOCOL DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION, September 1981.

[7] RFC 792 INTERNET CONTROL MESSAGE PROTOCOL DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION, September 1981

[8] RFC 793, TRANSMISSION CONTROL PROTOCOL DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION, September 1981

[9] ISO/IEC 7498–1:1984, "Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model" International Standards Organization (ISO), 1984. A revised version was published by ISO as 7498–1:1994 and by ITU-T as X.200 in 1994.

[10] The OSI model goal was to get industry participants to agree on common network standards to provide multi-vendor interoperability.

[11] ISO/IEC 7498–2:1989, "Information technology – Open Systems Interconnection – Basic Reference Model: Part 2: Security Architecture" International Standards Organization (ISO), 1989 and published by the ITU-T as X.800 in 1994.

[12] ISO/IEC 7498–3:1989, "Information technology – Open Systems Interconnection – Basic Reference Model: Naming and addressing" International Standards Organization (ISO), 1989.

[13] ISO/IEC 7498–4:1989, "Information technology – Open Systems Interconnection – Basic Reference Model – Part 4: Management Framework" International Standards Organization (ISO), 1989 and published by the ITU-T as X.700 in 1992.

- Recognition that more than just protocols are necessary for a network architecture, namely, it:
  - provided formalized descriptions of protocol concepts for multiple protocol layers (ISO/IEC 7498–1);
  - introduced a standardized approach for the consideration of communications security capabilities (ISO/IEC 7498–2);
  - recognized the need for standardized naming, addressing, and directory capabilities (ISO/IEC 7498–3); and
  - presented a framework and basic concepts for the management of communications components, features, and services (ISO/IEC 7498–4).

Although the seven protocol layers and specific protocols specified within these ISO standards have not been widely adopted, the general concepts from:

- ISO/IEC 7498–1 (aka ITU-T X.200) of protocol layering and well-defined interprotocol interfaces are widely accepted;
- ISO/IEC 7498–2 (aka ITU-T X.800) for communications security services, security mechanisms, and the management of security mechanisms are considered the de jure definitions for security; and
- ISO/IEC 7498–4 (aka ITU-T X.700) for the management of communications devices, in the form of Fault, Configuration, Accounting, Performance, and Security Management (the "FCAPS" of management), are considered the de jure areas that network management focuses upon.

Figure 1.1 highlights the relationship of protocol layer within the OSI protocol model versus the Internet Suite of protocols. Some consider Internet Suite application protocols to constitute layer 5 protocols.

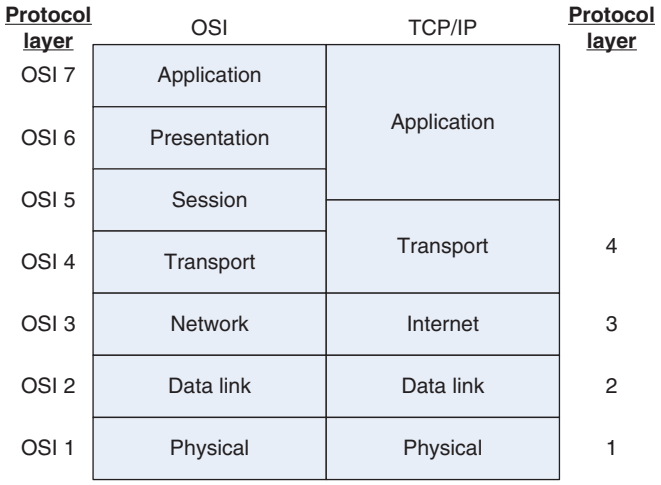

Figure 1.1. OSI Model and Internet Suite Protocol Layers.

1.1.4 Data Network Complexity

Since the aforementioned ISO standards were published, the complexity of deployed networks has vastly grown. Chapter 2 will explore this increasing complexity in more detail. Up through the 1980s, computer-oriented networks were primarily single facility/location oriented with computers either directly interconnected or connected to a local area network (LAN) that may have included a number of segments interconnected by bridging devices (e.g., Ethernet layer 2 bridges). Interfacility/location interconnection of computers or LANs relied on the use of modems to attach the local network to the PSTN via a modem and dial-up lines/services or a channel service unit to a PSTN-operator-supplied leased line.[14]

A "sea change" occurred in computer-data-networking with the concept of a router[15] which was under development through the 1970s and 1980s based on the use of minicomputers. These minicomputer router capabilities were, in this time frame, primarily limited to academic, government, and industrial research networks, given their expense and complexity. In the late 1980s, stand-alone multi-protocol connectionless routers became commercially available. These routing devices radically altered how computer networks were structured. From the late 1980s up to the present, router-based networks frequently utilize multiple routers to structure facility/location networks into logically separate subnets and tie multiple facility/location networks into enterprise networks that span geographic regions. High capacity versions of these routers have been instrumental to the evolution and growth of the Internet, which is really the router-based interconnection of a number of very large corporate or other enterprise-operated router networks. Figure 1.2 depicts the concept of a number of core (backbone) networks operated by AT&T, Verizon Business (formally MCI), Quest, Sprint, Level 3 Communications (L3), NTT Communications (NTTC) and Global Crossing (GBLX), "Tier 1" Internet Service Providers (ISPs), and an example set of commercial/residential access ISPs (the terms "alpha," "bravo," "delta," "echo," "tango," and "zulu" are used rather than actual company names for these example commercial/residential access ISPs). The term wide area network (WAN) represents Tier 1 ISP-routed networks that span wide geographic regions, and the term "IP Metro Network" represents access ISP-routed networks that span metropolitan-size geographic areas. As shown in Figure 1.1, the "Internet" is not a single network but many interconnected networks used to interconnect millions of other networks and computers.

Another area of complexity not considered by the ISO standards is at layer 2 of the OSI model. At the time when the ISO standards were published, the OSI layer 2 for local networks was considered to be a simple ability to interconnect two devices in either:

- a point-to-point manner (also called direct connection) as shown in Figure 1.3;

[14] A PSTN-operator-supplied leased line is a dedicated circuit between two different facilities at the link layer providing 56Kbps, 1.544 Mbps or sometimes 45 Mbps of bandwidth.

[15] A router is a networking device tailored to the tasks of routing and forwarding information between two or more networks based on layer 3 protocol information unlike a bridge or layer 2 switch that forwards information between two or more network segments based on layer 2 protocol information.

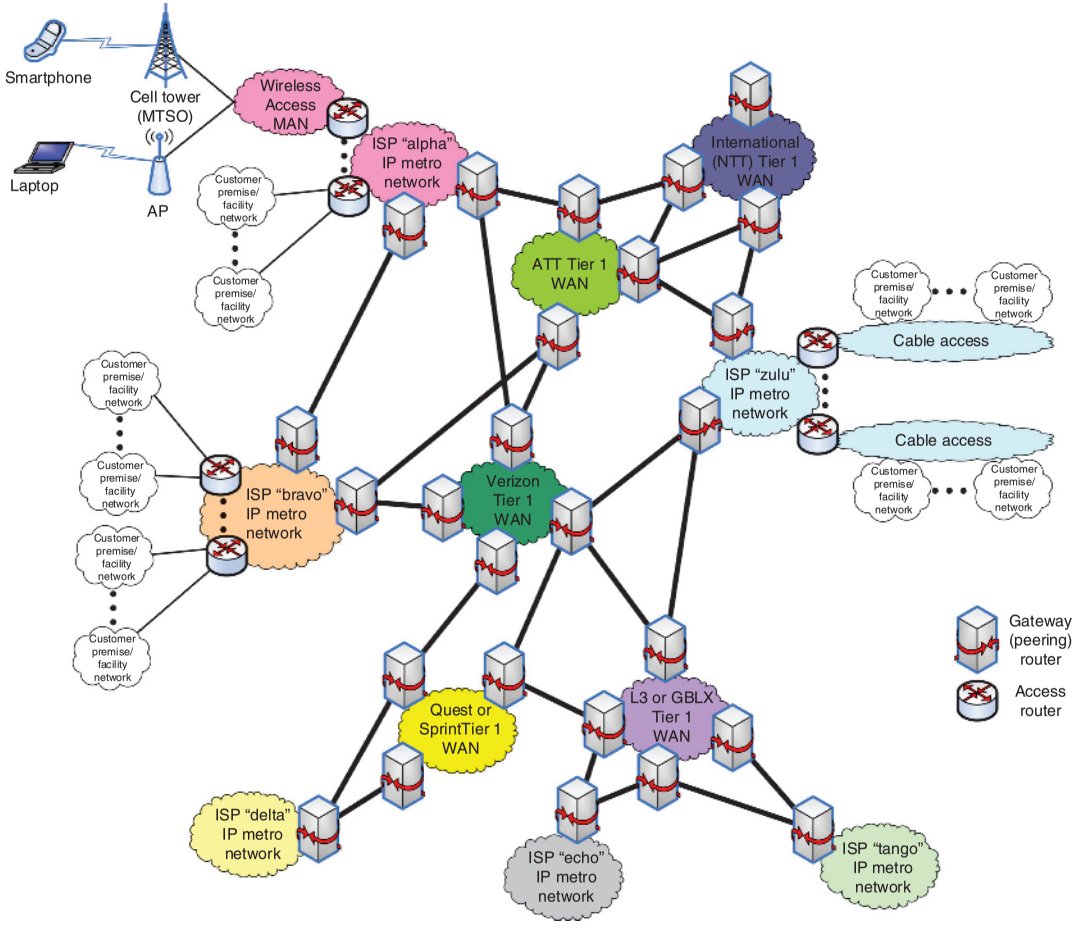

Figure 1.2. The Internet Concept of Core and Access ISP Networks.

- a multi-drop manner where a number of devices are interconnected to a common physical medium such as with the early versions of Ethernet (i.e., 10base5 "thick-wire" and 10base2 "thin-wire" coaxial cabled Ethernet) as shown in Figure 1.4; or
- a "star" manner where a number of devices are interconnected to a common device such as with hubbed or switched versions of Ethernet (i.e., 10baseT over-twisted pair cabling) as shown in Figure 1.5.

Interconnection of LANs was expected to rely on some form of intermediate packet switching network, such as a commercially available X.25 network. During the 1990s timeframe, significant layer 2 technological developments resulted in the availability of Synchronous Optical Network (SONET) and Asynchronous Transfer Mode (ATM) layer 2 networking along with continued use of X.25 and its commercial successor Frame Relay networking. These developments resulted in interfacility interconnection of facility/location LANs often using two or three protocols below the layer 3 protocol (routinely IPv4). For example, an organization interconnecting routed subnets at three

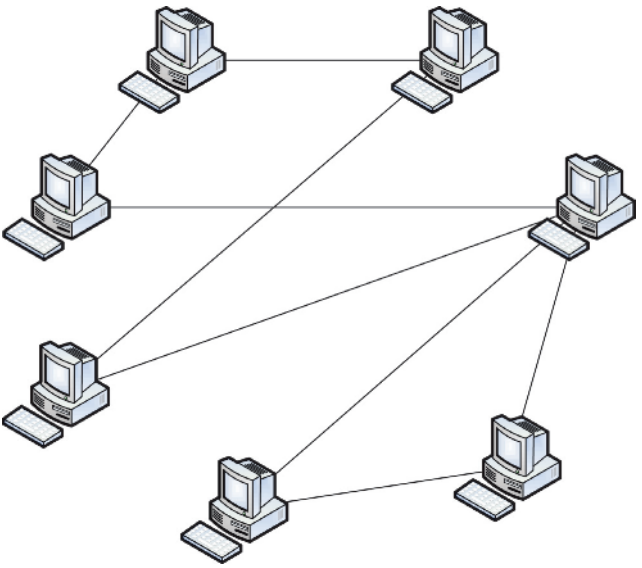

Figure 1.3. Direct Interconnection of Computers.

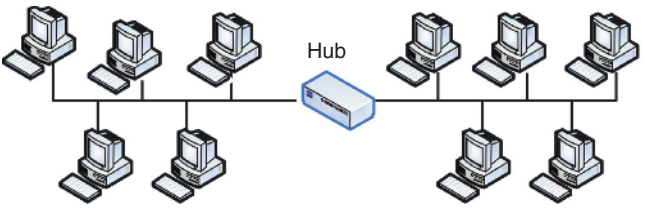

Figure 1.4. Multi-drop Interconnection of Computers.

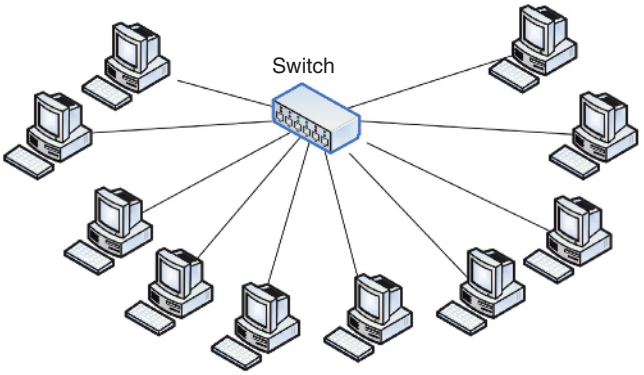

Figure 1.5. "Star" Interconnection of Computers.

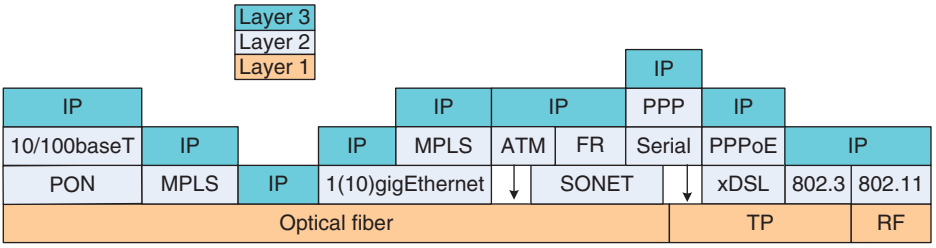

Figure 1.6. Current Complexity of Protocols in Layer 2.

locations would configure their routers to use SONET links over which ATM would be used to transport Ethernet frames that carried IP packets. Figure 1.6 depicts various arrangements for layering protocols within layer 2.

In Figure1.6:

- PON represents Passive Optical Networking
- MPLS represents Multi-protocol Label Switching
- xDLS represents various forms of Digital Subscriber Line technologies
- FR represents Frame Relay
- Serial represents asynchronous dial-up PSTN access
- 802.3 represents Ethernet
- 802.11 represents Wireless Ethernet (aka "WiFi")
- PPP represents Point-to-Point Protocol
- PPPoE represents Point-to-Point Protocol over Ethernet.

What needs to be pointed out is that:

- SONET technology is not a simple direct-connect, multi-drop, or star technology but actually provides the ability to interconnect many devices in what are called

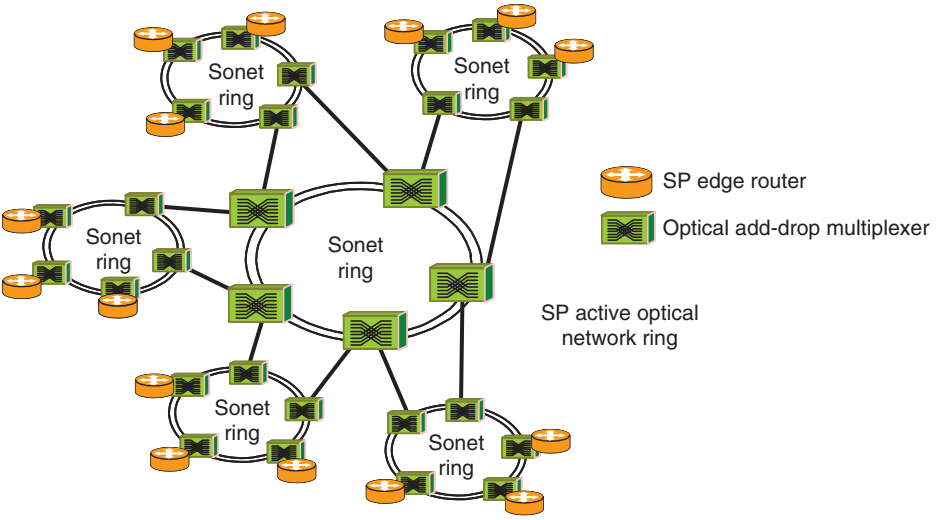

Figure 1.7. Example Sonet Rings.

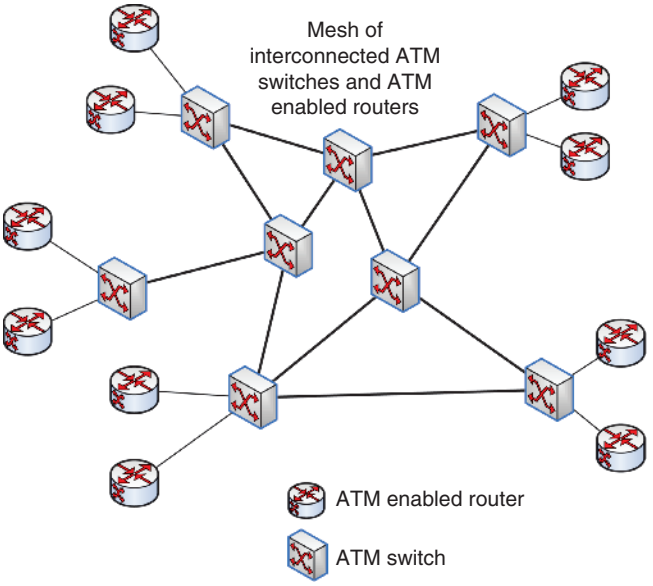

Figure 1.8. Example ATM Network.

rings and even interconnect these rings into more complex organizations as shown in Figure 1.7; and

- ATM technology is also not a simple direct-connect, multi-drop, or star technology but actually provides the ability to interconnect many devices in a meshed manner, with multiple links exiting/entering each ATM switch allowing the construction of complex ATM interconnections as shown in Figure 1.8.

ATM switches are routinely interconnected over SONET infrastructures, thus resulting in a complex organization of interconnected devices layered on top of another complex organization of interconnected devices.

As can be seen from the proceeding discussion, the standards describing network architectures have not kept pace with the various technologies deployed and the corresponding complexity of modern networks. For this reason, we start our discussion by considering how security, and its management, has been viewed from a standards perspective. We will also discuss some of the typical security technologies deployed in today's network infrastructures.[16]

1.2 A NETWORK SECURITY HISTORICAL PERSPECTIVE

To properly discuss what security management focuses on, it is helpful to understand where the very concept of network management began and how the issue of managing security has evolved over the decades. The first effort to formalize network management concepts resulted in the development and publication of ISO/IEC 7498–4. Prior to the publication of ISO/IEC 7598–1, network management (and security) were proprietary capabilities of both the PSTN and computer manufacturer products and services. However, during the 1980s, many in telecommunications-related industries began to recognize that network management activities could be grouped into the five areas of:

- **F**ault management;
- **C**onfiguration management;
- **A**ccounting management;
- **P**erformance management; and
- **S**ecurity management.

As organized in ISO/IEC 7498–4, these areas are typically referred to collectively as FCAPS (an acronym based on the first letter of each area). The subject of security management was further expanded upon in ISO/IEC 7498–2. When ISO published ISO/IEC 7498–4, the subject of security management was limited to simply noting that security management exists to support the application of security policies by functions concerned with:

- creation, deletion, and control of security services and mechanisms;
- distribution of security-relevant information; and
- reporting of security-relevant events,

and then directs the reader back to ISO/IEC 7498–2 for additional information on management functions within the ISO security architecture. Therefore, to understand the

[16] A network infrastructure is the basic physical (communications links/media), technical (hardware, software, and protocols), and organizational (policies, processes, and procedures) structures needed for the operation of an enterprise communications network that delivers services and facilities to the enterprise, its customers/users, and other interconnected networks.

roots of security management concepts, we need to further examine ISO/IEC 7498–1 and ISO/IEC 7498–2.

The aforementioned ISO standards ISO/IEC 7498–1, ISO/IEC 7498–2, and ISO/IEC 7498–4 have served as cornerstone documents and even adopted directly by the ITU-T as ITU-T X.200 (ISO/IEC 7498–1), ITU-T X.800 (ISO/IEC 7498–2), and ITU-T X.700 (ISO/IEC 7498–4). It is worth taking a look at these documents.

1.2.1 ISO/IEC 7498–1 (ITU-T X.200) Coverage of Management

ISO/IEC 7498–1 (X.200) focuses on the formal architecture of networks and the control of network components/devices (assets); however, only about 2 pages, out of some 60 plus pages, are devoted to the management of network assets. This document defines a number of concepts, specifically:

1. application management functions are concerned with managing application processes, and application management software provide application management functions;
2. systems management functions are concerned with the management of various network resources, and their status across all protocol layers of a network architecture, and system management software provide system management functions; and
3. protocol layer management functions reside within each layer for activities such as activation and error control and are partly performed as a subset of systems management.

ISO/IEC 7498–1 (X.200) then states that only management-related communication between management functions within networked devices is of concern within the network architecture, and that management activities local to specific networked devices are out of scope as the standard only considers network resources involved with data processing and data communication. Application management is discussed as the management of network application processes and includes activities such as:

a. initialization of parameters;
b. initiation, maintenance, and termination of applications;
c. allocation and de-allocation of network resources;
d. detection and prevention of network resource interference;
e. integrity and commitment controls;
f. security controls; and
g. application checkpoint and recovery control.

The activities of application security controls are not further explained or defined within the standard. Systems management is discussed as the management of network resources across all protocol layers, and such activities include:

a. activation/deactivation management, including activation, maintenance, and termination of network resources, program loading functions, control of connections between management entities, and parameter initialization/modification;
b. monitoring, including reporting status, status changes, and statistics; and
c. error control, including error detection, diagnostic functions, reconfiguration, and restart.

The protocols used for systems management are considered application layer protocols. Protocol layer management activities such as activation and error control are considered to occur within each protocol layer, whereas other layer management activities are viewed as part of systems management. ISO/IEC 7498-1's consideration of management and security subjects is so general as to be almost useless. Five years would pass before network management and security were given any serious consideration with the publication of ISO/IEC 7498–4 (X.700) and ISO/IEC 7498–2 (X.800).

1.2.2 ISO/IEC 7498–4 (ITU-T X.700) Coverage of Security Management

ISO/IEC 7498–4 (ITU-T X.700) devotes a single paragraph to the subject of security management which simply says that this area focuses on:

- creation, deletion, and control of security services and mechanisms;
- distribution of security-relevant information; and
- reporting of security-relevant events.

Nowhere in this document are these concepts further discussed other than to refer the reader to ISO/IEC 7498–2 (X.800).

1.2.3 ISO/IEC 7498–2 (ITU-T X.800) Coverage of Security and Management

For the sake of simplicity, and because the ITU-T published standards tend to be more frequently referenced than the ISO/IEC versions, we will hence forward reference X.200, X.700, and X.800 rather than the ISO/IEC versions.

Although frequently referred to as a "security architecture," the main value of ITU-T X.800 is the introduction and definition of:

- five primary network security services;
- a set of specific network security mechanisms;
- a number of non-specific (general) device resident security mechanisms; and
- a description of management mechanisms for controlling deployed security mechanisms.

ITU-T X.800 is concerned only with those visible aspects of communications that permit networked elements to achieve the secure transfer of information between them. It does not attempt to provide any kind of detailed descriptions or requirements, nor does it provide the means to assess conformance of any implementation to this or any other security standard. Additionally, it does not indicate, in any detail, the additional security mechanisms needed within networked elements to ensure reliable, secure computer operation.

1.2.3.1 X.800 Security Services. Security services are abstract functional capabilities which can counter security threats. In practice, these services are invoked at appropriate protocol layers and within computing elements, and in different combinations, to satisfy organizational security policies, requirements, and operational rules. Practical realizations of systems may implement particular combinations of the basic security services for direct invocation. Historically, there were considered to be five fundamental security services: Authentication (three variations), Access Control, Confidentiality (four variations), Integrity (five variations), and Non-repudiation (two variations). Standardized definitions of these historical security services were provided in ITU-T X.800-1991 and presented in Table 1.1.

X.800 then goes on to say that these security services would be instantiated via the deployment of security mechanisms, which are then discussed next as either specific security mechanisms or pervasive security mechanisms.

1.2.3.2 X.800 Specific Security Mechanisms. The specific security mechanisms X.800 considers appropriate for providing the aforementioned security services, which may be implemented (provided) within individual protocol layers, are presented in Table 1.2.

Appendix A of this book, "Role of Cryptography in Information Security," provides an overview of cryptographic hash algorithms and both symmetric and asymmetric cryptography along with how this technology may be used to provide:

- both Peer-entity and Data-origin authentication;
- different forms of confidentiality and integrity; and
- non-repudiation via digital signatures.

Appendix B of this book, "Authentication of Subjects," provides an overview of the different approaches for both cryptographic and non-cryptographic authentication of subjects (both human and machine).

1.2.3.3 X.800 General Security Mechanisms. ITU-T X.800 also describes a number of non-specific (general or pervasive) security mechanisms that all networked devices should include. These pervasive security mechanisms are expected to be independent of any network services, rather general capabilities of a network attached device, be it a router, switch server, workstation, etc. The intent of these mechanisms is to provide a secure execution environment for protocol-related security mechanisms.

TABLE 1.1. X.800 Security Services.

Service Group	Specific Service	Service Purpose or Capability
Authentication	**Peer-entity authentication**	A service for confirming the identities of subjects communicating with each other and provides confidence that a subject is not attempting to masquerade as some other subject.
	Data-origin authentication	A service for corroborating the source subject from which data are received and does not necessarily provide protection against duplication or modification of data.
	User authentication	A service for confirming/validating the identity of a human subject when the subject logs into a computer system and provides confidence that a human subject is not attempting a masquerade as a different human subject.
Access control		A service that provides protection against unauthorized use or access to communications resources (objects) and may be applied to various types of access to a resource.
Confidentiality	**Connection confidentiality**	A service that provides for the confidentiality of all data (objects) on a protocol connection being used by two communicating subjects.
	Connectionless confidentiality	A service that provides for the confidentiality of all data (objects) transferred by a protocol being used by two communicating subjects over a protocol exchange between the two subjects where the protocol uses a connectionless, or best effort/datagram, exchange method.
	Selective field confidentiality	A service that provides for the confidentiality of selected data (objects) transferred by a protocol regardless of whether the protocol operates in a connection-oriented or connectionless manner.
	Traffic flow confidentiality	A service that provides for the protection of information which might be derived from observation of the existence of communications activities between two subjects.
Integrity	**Connection integrity with recovery**	A service that provides the ability to detect the occurrence of unauthorized modification of all data (objects) on a protocol connection being used by two communicating subjects and should an unauthorized modification be detected, this service includes the ability to effect retransmission of the modified object(s).

(*continued*)

TABLE 1.1. (*cont'd*)

Service Group	Specific Service	Service Purpose or Capability
	Connection integrity without recovery	A service that provides the ability to detect the occurrence of unauthorized modification of all data (objects) on a protocol connection being used by two communicating subjects and does not include the ability to effect retransmission of the modified object(s).
	Selective field connection integrity	A service that provides the ability to detect the occurrence of unauthorized modification of selected data (objects) on a protocol connection being used by two communicating subjects and does not include the ability to effect retransmission of the modified object(s).
	Connectionless integrity	A service that provides the ability to detect the occurrence of unauthorized modification of all data (objects) on a protocol connection being used by two communicating subjects where the protocol uses a connectionless, or best effort/datagram, exchange method.
	Selective field connectionless integrity	A service that provides the ability to detect the occurrence of unauthorized modification of selected data (objects) on a protocol connection being used by two communicating subjects where the protocol uses a connectionless, or best effort/datagram, exchange method.
Non-repudiation	**Non-repudiation with proof of origin**	A service that provides a receiving subject of data with proof of the origin (sending subject) of data/object. This will protect against any attempt by the sender (sending subject) to falsely deny sending the object or its contents.
	Non-repudiation with proof of delivery	A service that provides a sender (sending subject) of data with proof of delivery of object to the receiving subject. This will protect against any subsequent attempt by the recipient to falsely deny receiving the data or its contents.

Unfortunately, ITU-T X.800 does not provide any in-depth discussion or description of these pervasive security mechanisms beyond a general definition of each (Table 1.3).

1.2.3.4 X.800 Security Management Mechanisms. ITU-T X.800 management of security focuses specifically on managing, controlling, configuring, and monitoring security services and mechanisms within network protocols and securing network management functionality; any consideration of managing general security capabilities within devices is considered out of scope of the document. A key concept introduced in X.800 is that of a "Security Domain" wherein all "subjects" are expected to adhere to

TABLE 1.2. X.800 Included Specific Security Mechanisms.

Security Mechanism	Mechanism Purpose or Capability
Encipherment	Encipherment mechanisms are based on encryption to provide confidentiality of either data or traffic flow information. Applicable encryption algorithms include symmetric (i.e., secret key) encryption and asymmetric (e.g., public key) encryption, and the use of an encryption mechanism implies the use of a key management mechanism.
Digital signatures	Digital signature mechanisms are based on asymmetric encryption and include procedures for signing data and verifying the signature of signed data. The basic characteristic of a digital signature mechanism is that the signature can only be produced using the signer's private information.
Access control mechanisms	Access control mechanisms rely on some combination of: • authenticated identity of an entity; • information about an entity; • capabilities of an entity; • time of attempted access; • route of attempted access; and • duration of access, in order to determine if access by the entity will be allowed to a resource.
Data integrity mechanisms	Data integrity mechanisms provide the ability to detect any accidental or intentional modifications. These mechanisms rely on the use of information (a secret key) shared by only the sending and receiving entities involved in an interaction.
Authentication exchange mechanisms	Authentication exchange mechanisms provide the ability to verify a claimed identity. These techniques may use cryptographic mechanisms, characteristics, or possessions of the requesting entity. These mechanisms may be combined with "handshaking" protocols.
Traffic padding mechanisms	Traffic padding can be used to provide some degree of protection against traffic analysis by obscuring the actual size of information being exchanged when used with encryption mechanisms.
Routing control mechanisms	Routing control mechanisms and systems are used to instruct a network SP to establish a connection via a specific route so as to bypass known/suspected malicious intermediate systems or to pass through certain sub-networks, relays, or links.
Notarization mechanisms	Notarization mechanisms are used to provide assurance of properties (such as data integrity, origin, time, and destination) about the data communicated between entities via a trusted third-party notary.

TABLE 1.3. X.800 Pervasive Security Mechanisms.

Trusted functionality	The intent of this mechanism is to ensure that security functions will perform as expected and not be affected by non-security-related functions within the device. However, the document does not provide any further elaboration on this subject.
Security labels	The intent of this mechanism is that software and data elements (resources) within a device may have a label associated with them such that the label indicates the "sensitivity" of the associated resource. These labels could be used to control access to a resource. The document does not provide any further elaboration on this subject.
Event detection	The intent of this mechanism is that apparent violations of security should be detectable and may also include detection of non-violation events, such as successful log-on or log-off. Events related to network activities and non-network activities should be detectable. This mechanism should also cover event reporting and event logging along with the syntactic and semantic definitions associated with these activities. The document does not provide any further elaboration on this subject.
Security audit trail	The intent of this mechanism is the ability to review security audit trails and provide a valuable capability to detect and investigate security breaches via subsequent security audits. Security audits require the recording of security relevant information in a security log file or equivalent form. Analysis and report generation from event and audit logs is considered a security management function. The document does not provide any further elaboration on this subject.
Security recovery	The intent of this mechanism is the ability to respond to requests from mechanisms such as event handling and management functions and either initiate or recommend recovery actions that isolate or mitigate the impact of security-violation-related events. The goal of this mechanism is the restoration of reliable normal functionality. The document does not provide any further elaboration on this subject.

a common set of security policy statements (requirements) as specified by a single "authority." The authority is the organization that controls or is responsible for network services and identifies who may interact with what services and functions via statements within the security policy. As stated in X.800, security management is concerned with the management of communications security services and mechanisms and spans both the configuration of these services and mechanisms and collection of information concerning the operation of these services and mechanisms. Some of the configuration control responsibilities of communications security management include:

- distribution of cryptographic keys ("Key management");
- the setting of security-related parameters ("Configuration management");
- monitoring of both normal and abnormal security-related events ("Event–Fault management");
- generation and processing of audit trails ("Audit management"); and
- both security service/mechanism activation and deactivation.

In X.800's view, security management does not address how security mechanisms in protocols actually provide specific security services. Another basic concept introduced by X.800 is that of a Security Management Information Base (SMIB), which serves as a repository for security-relevant information. No specific approach, or other details, for the storage of the information is discussed; yet each networked device is expected to maintain that local information necessary for the device to enforce applicable security policy statements. The SMIB is expected to be:

- essentially distributed across those devices within a "Security Domain," and
- likely included in any general Management Information Base (MIB) within and maintained by each device.

X.800 aggregates security management activities into three categories:

- network security management;
- network security service management;
- network security mechanism management.

Network security management functionality is expected to typically include:

- overall network security policy management;
- interaction with other network management functions;
- interaction with network security service management and network security mechanism management;
- network security event management spans those aspects of event handling and the remote reporting of apparent attempts to violate network security and the modification of thresholds used to trigger event reporting;
- network security audit management is responsible for:
  - the selection of events to be logged and/or remotely collected;
  - the enabling and disabling of audit trail logging of selected events;
  - the remote collection of selected audit records; and
  - the preparation of security audit reports;
- network security recovery management is responsible for:
  - maintenance of the rules used to react to real or suspected security violations;
  - the remote reporting of apparent violations of system security; and
  - security administrator interactions.

Network security service management focuses on specific network security services and is expected to typically (but not exhaustively) include the following activities on a per service basis:

- determination and assignment of the target security protection for the service;
- assignment and maintenance of rules for the selection (where alternatives exist) of the specific security mechanism to be employed to provide the requested security service;

- negotiation (locally and remotely) of available security mechanisms which require prior management agreement;
- invocation of specific security mechanisms via the appropriate security mechanism management function, for example, for the provision of administratively imposed security services; and
- interaction with other security service management functions and security mechanism management functions.

Network security mechanism management focuses on specific network security mechanisms and is expected to typically (but not exhaustively) include the following activities on a per mechanism basis:

- key management is responsible for:
  - generating keys;
  - deciding which entities should receive a copy of each key; and
  - making available, or distributing keys, in a secure manner.
    While noting that some key management functions, such as the physical distribution of keys, may occur outside of network security management functions, the exchange of session keys used during an association is a normal protocol layer function and utilize a key distribution center (KDC) or functions pre-distributed via management protocols.
- encipherment management is responsible for:
  - interaction with key management;
  - establishment of cryptographic parameters; and
  - cryptographic synchronization;
- digital signature management is responsible for:
  - interaction with key management;
  - establishment of cryptographic parameters and algorithms; and
  - use of protocols between communicating entities and possibly a third party;
- access control management is responsible for distribution of security attributes and parameters along with access control lists (ACLs) or capabilities lists;
- data integrity management is responsible for:
  - interaction with key management;
  - negotiation of cryptographic parameters and algorithms; and
  - use of protocol between communicating entities;
- authentication management is responsible for distribution of descriptive information, passwords, or keys to entities required to perform authentication;
- traffic padding management is responsible for maintenance of rules used for traffic padding, such as data rates, message characteristics (i.e., length), and variation of these rules based on attributes such as time of day or calendar;
- routing control management is responsible for definition of links or sub-networks considered to be either secured or trusted with respect to particular criteria; and

- notarization management is responsible for distribution of information about notaries and the protocols and interactions between notaries and a notary and other entities.

Although X.800 was developed specifically as a communications security architecture, the underlying concepts have broader applicability representing the first international consensus on the definitions of basic security services (Authentication, Access Control, Data Confidentiality, Data Integrity, and Non-repudiation) along with more general (pervasive) services such as Trusted Functionality, Event Detection, and Security Audit and Recovery.

Following the development of X.800, the need for additional related communications security standards was identified. As a result, work on a number of supporting standards and complementary architectural recommendations was initiated. Some of these recommendations are discussed next.

1.2.4 The Security Frameworks (ITU-T X.810–ITU-T X.816)

The security frameworks were developed to provide comprehensive and consistent descriptions of the security services defined in X.800. They were intended to address all aspects of how the X.800 security services could be applied in the context of a specific security architecture, including possible future security architectures. The frameworks focus on providing protection for systems, objects within systems, and interaction between systems. They do not address the methodology for constructing systems or security mechanisms.

The frameworks address both data elements and sequences of operations (excluding protocol elements) that are used to obtain specific security services. These services may apply to the communicating entities of systems as well as to data exchanged between, and managed by, systems.

1.2.4.1 The Security Framework Overview (X.810).[17] The Security Framework Overview introduces the other frameworks and describes common concepts, including security domains, security authorities, and security policies that are used in all the frameworks. It also describes a generic data format that can be used to convey both authentication and access control information securely.

1.2.4.2 The Authentication Framework (X.811).[18] The Authentication Framework occupies a position at the top of a hierarchy of authentication standards that provide concepts, nomenclature, and a classification for authentication methods. This framework defines the basic concepts of authentication, identifies possible classes of authentication mechanism, defines the services for these classes of mechanism, identifies functional requirements for protocols to support these classes of mechanism, and identifies the general management requirements for authentication.

[17] ITU-T Recommendation X.810, Information technology – Open Systems Interconnection – Security frameworks in open systems: OVERVIEW, 11/95

[18] ITU-T Recommendation X.811, Information technology – Open Systems Interconnection – Security frameworks in open systems: AUTHENTICATION Framework, 04/95

1.2.4.3 The Access Control Framework (X.812).[19] The Access Control Framework describes a model that includes all aspects of access control in Open Systems, the relationship to other security functions (such as Authentication and Audit), and the management requirements for Access Control.

1.2.4.4 The Non-repudiation Framework (X.813).[20] The Non-repudiation Framework extends the concepts of non-repudiation security services as described in X.800 and provides a framework for the development of these services. It also identifies possible mechanisms to support these services and general management requirements for non-repudiation.

1.2.4.5 The Confidentiality Framework (X.814).[21] The purpose of the confidentiality service is to protect information from unauthorized disclosure. The Confidentiality Framework addresses the confidentiality of information in retrieval, transfer, and management by defining the basic concepts of confidentiality, defining the possible classes of confidentiality and the facilities required for each class of confidentiality mechanism, identifying the management and supporting services required, and addressing the interaction with other security services and mechanisms.

1.2.4.6 The Integrity Framework (X.815).[22] The Integrity Framework addresses the integrity of data in information retrieval, transfer, and management. This recommendation defines the basic concepts of integrity, identifies possible classes of integrity mechanism and the facilities for each class of mechanism, identifies management required to support each class of mechanism, and addresses the interaction of the integrity mechanism and the supporting services with other security services and mechanisms.

1.2.4.7 The Audit and Alarms Framework (X.816).[23] The Audit and Alarms Framework defines the basic concepts and provides a general model of security audit and alarms, identifies the criteria for a security audit and for raising alarms, identifies possible classes of audit and alarm mechanisms, defines the services for these classes of mechanisms, identifies functional requirements to support these mechanisms, and identifies general management requirements for security audit and alarms.

1.2.4.8 Applicability of the ITU-T Security Frameworks. Unfortunately, these seven documents have received little attention since they were published. What has happened is that only the concepts directly contained within the original X.800 document have received general acceptance. In 2003, the ITU-T published X.805 as an updated

[19] ITU-T Recommendation X.812, Information technology – Open Systems Interconnection – Security frameworks in open systems: ACCESS CONTROL Framework, 11/95

[20] ITU-T Recommendation X.813, Information technology – Open Systems Interconnection – Security frameworks in open systems: NON-REPUDIATION Framework, 10/96

[21] ITU-T Recommendation X.814, Information technology – Open Systems Interconnection – Security frameworks in open systems: CONFIDENTIALITY Framework, 11/95

[22] ITU-T Recommendation X.815, Information technology – Open Systems Interconnection – Security frameworks in open systems: INTEGRITY Frameworks, 11/95

[23] ITU-T Recommendation X.816, Information technology – Open Systems Interconnection – Security frameworks in open systems: SECURITY AUDIT and ALARMS Framework, 11/95

security architecture meant to supersede X.800, and most standards developed after this document routinely reference and build upon X.805 rather than X.800 or the X.810 through X.816 framework documents. So we need to examine X.805.

1.2.5 The ITU-T X.805 Approach to Security

ITU-T X.805[24] attempts to define a security architecture for providing end-to-end network security by building on some of the concepts of X.800. The functionality of the basic security services of X.800 (Access Control, Authentication, Data Confidentiality, Data Integrity, and Non-repudiation) matches the functionality of what X.805 refers to as Security Dimensions. However, X.805 proceeds to introduce three new Communications Security, Availability, and Privacy Security Dimensions that are not consistent with X.800. Nor does X.805 build on, use, or even reference the security frameworks (X.810–X.816). X.805 relies on two major concepts: layers and planes.

The three layers are Infrastructure layer, Services layer, and Applications layer. The Infrastructure layer consists of the network transmission facilities as well as individual network elements (NEs). Examples of components that belong to the Infrastructure layer are individual routers, switches and servers, as well as the communication links between them. The Services layer addresses security of network services that are offered to customers. The Application layer addresses requirements of the network-based applications used by the customers.

X.805 also defines three Security planes to represent the three types of protected activities that take place on a network, namely, (i) the Management plane, (ii) the Control plane, and (iii) the End-User plane. These Security planes address specific security needs associated with network management activities, network control or signaling activities, and end-user activities correspondingly. The Management plane is concerned with Operations, Administration, Maintenance, and Provisioning (OAM&P) activities such as provisioning a user or a network, etc. The Control plane is associated with the signaling aspects for setting up (and modifying) the end-to-end communication through the network irrespective of the medium and technology used in the network. The End-User plane addresses security of access and use of the network by customers as well as protecting end-user data flows. However, X.805 cannot:

- be used as the basis of a security assessment as X.805 only talks about generic security objectives, not security requirements; nor does it provide any specific criteria for such an assessment;
- be used for maintaining, or reviewing, a security program over time as a specific security environment changes; also, it does not provide any specific criteria for security program review; and
- assist in the management of security policies and procedures, incident response and recovery plans, and technology architectures as it does not discuss security policy, operational procedures, business continuity, or technology architectures in a detailed manner.

[24] ITU-T Recommendation X.805, Security architecture for systems providing end-to-end communications, 10/2003

1.3 NETWORK AND SECURITY MANAGEMENT SYSTEMS

From the 1960s up to almost the end of the 1980s, data network and computer management was considered a local computer administrative activity with virtually no capabilities for remote administration. This was not an unreasonable view considering that commercial/business computer-oriented networking was primarily a computer-to-computer activity with little network-oriented equipment being used beyond modems throughout this period. However, by 1989, there were four commercial products that targeted the management of networks:

- International Business Machine's (IBM) Netview;
- Digital Equipment Corporation's (DEC) Enterprise Management Architecture (EMA);
- American Telephone & Telegraph (**AT&T**) Bell Laboratory's Unified Network Management Architecture (UNMA); and
- Hewlett Packard Corporation's (HP) OpenView.

Netview was primarily IBM System Network Architecture (SNA) network centric with meager management capabilities for non-SNA network technologies. DEC's EMA was primarily a Digital Networking (DECnet) tool along with providing a framework that could incorporate third-party management and interface functionality. AT&T's UNMA never progressed much beyond initial product introductions. HP's OpenView was based on the use of the IETF's Simple Network Management Protocol (SNMP) to make it vendor independent and has evolved into one of the more commercially successful heterogeneous management products available.

1.3.1 Element and Network Management Systems

During the 1990s, with the growth of LAN deployments, two categories of packet network applications evolved: the Element Management System (EMS) and the Network Management System (NMS). EMS products are typically developed by network equipment manufacturers for the remote administration of their own products and usually products with identical capabilities (as shown in Figure 1.9), whereas NMS products are intended

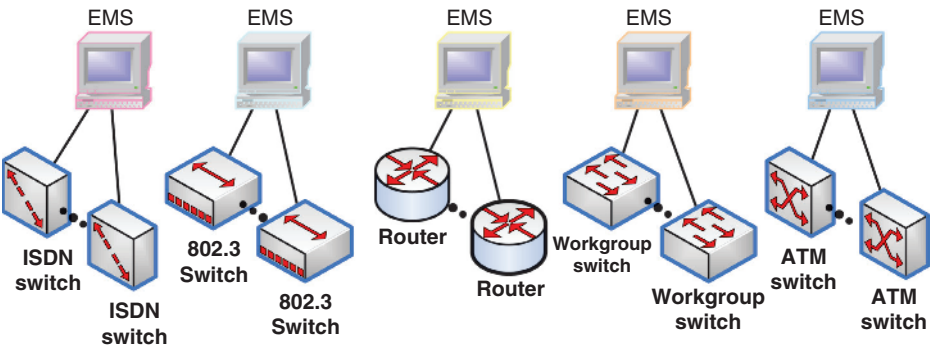

Figure 1.9. EMSs Dedicated to Specific Device Types.

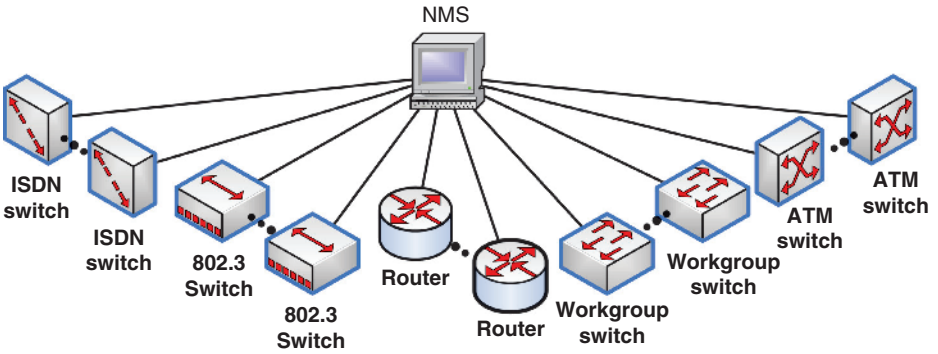

Figure 1.10. NMS Managing Different Types of Devices.

for the administration products from diverse manufacturers (as shown in Figure 1.10). These EMS and NMS applications were initially designed to execute on "minicomputers" and workstations and are now frequently found on personal computer systems.

1.3.2 Operations Support Systems

Within the PSTN world, administration was primarily a local telephone switch activity. Not until the late 1980s did telephone network operating companies begin to deploy intelligent networking equipment such as subscriber line/loop concentrators and remote switching units outside of the telephone central office (CO) where the main telephone switch was located. The major public telephone companies developed a number of mainframe-computer-based applications for managing their deployed telephone switch assets, access circuits, inter-CO links, directories, billing, and expansion planning. Some of these administrative applications included, just to name a few:

- TIRKS, LFACS, SWITCH for Inventory Control;
- SOAC for Service Request and Performance Administration; and
- LMOS and MLT for Trouble Resolution.

(Note that these are defined in Table 1.5.)

These administrative applications were routinely referred to as Operations Support Systems (OSSs) and provided multiple, and sometimes over-lapping, capabilities and complex interfaces, as depicted in Figure 1.11. Although a number of international standards documents have introduced the term Operations System (OS), many people use the term OSS, and this book follows the OSS convention, especially since the term OS is routinely associated with operating systems.

Many of these OSSs were created in the early to mid-1980s and continue as "cornerstone" management, administrative, and control systems.

Telecommunications Service Providers (SPs) developed a diverse suite of management systems (OSSs) over the last 25 plus years to support the major PSTN Operation, Administration, Maintenance and Provisioning (OAM&P) activities, where:

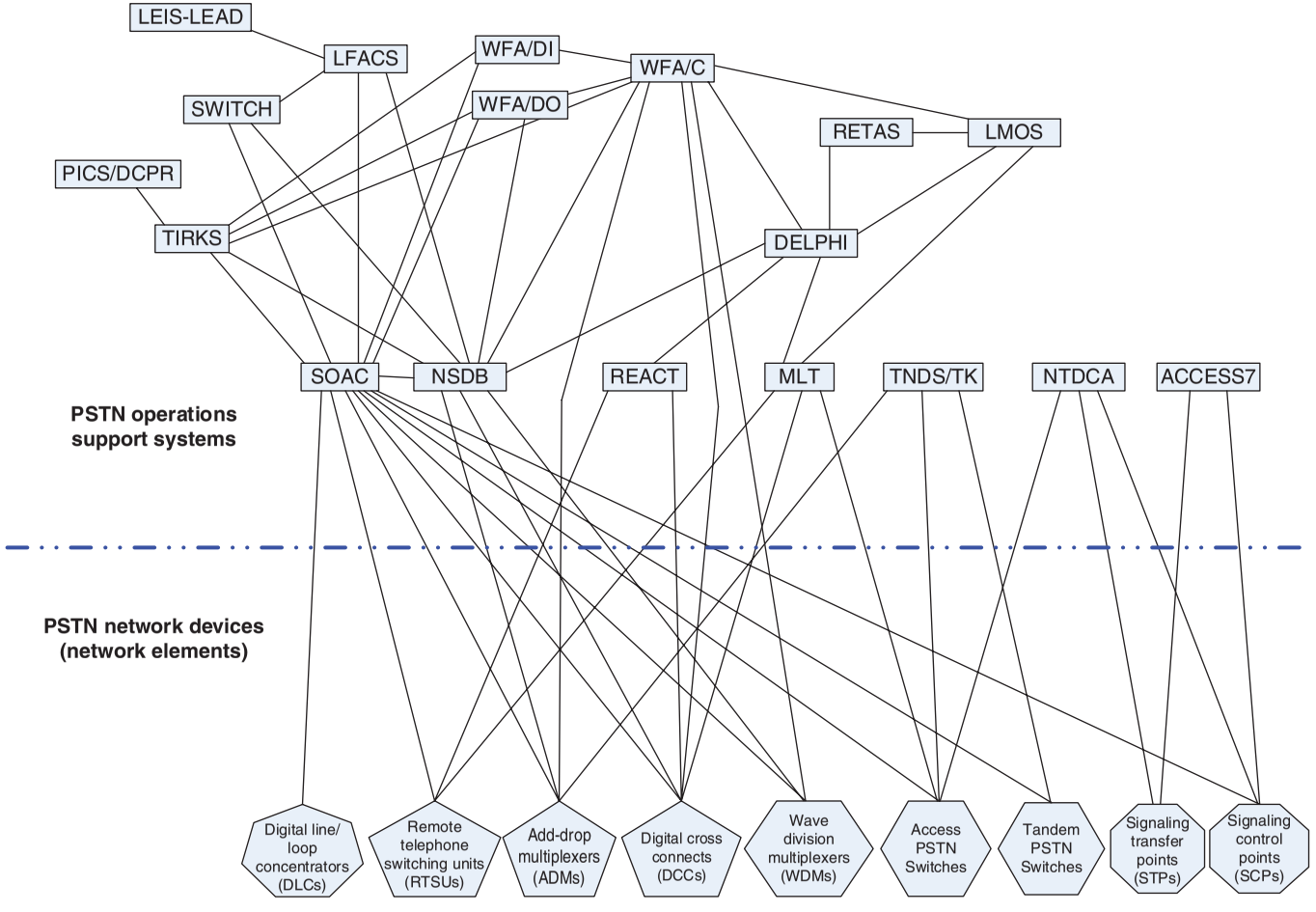

Figure 1.11. Example PSTN Operations Support Systems and Associated Network Elements.

Operations refers to the processes and procedures used to manage and control telecommunications network devices and telecommunications management network (TMN)-related devices;

A**dministration** refers to activities that ensure that the network resources are used efficiently and service-quality objectives met;

Maintenance refers to activities, such as tests, measurements, replacements, adjustments, and repairs, necessary to restore or maintain a network resource in a specified state so that the resource can perform its required functions; and

Provisioning refers to the process of preparing and equipping a network to allow it to provide services to its users.

In a traditional telecommunications network infrastructure, there is no distinction made between telecommunications transport services and "higher-level" application services, and therefore provisioning has spanned configuring systems, providing users with access to data and resources, and refers to all enterprise-level information resource management involved. Most PSTN SPs organize their OSSs as shown in Table 1.4.

As can quickly be seen in Table 1.4, many of these OSSs are involved in a number of different functional activities, such as TIRKS and SWITCH. Table 1.5 provides brief description of the more common OSSs used by PSTN Service Providers (SPs).

1.4 EVOLUTION OF NETWORK AND SECURITY MANAGEMENT CONCEPTS

How have management concepts evolved from those first presented in X.800. It was recognized that management systems need to be deployed in an organized manner. Figure 1.11 illustrates how the companies responsible for the PSTN had developed numerous management systems which frequently included proprietary functions and interfaces to the devices they were responsible for controlling and managing. This recognition was a driving factor for the development of ITU-T M.3010[25] in 1996 and ITU-T M.3400[26] in 1997 (both revised in 2000).

1.4.1 Telecommunications Management Network

ITU-T M.3010 introduced the concept that management of a telecommunications (PSTN) infrastructure is basically a distributed information processing application spread across a set of management OSSs that interact with a vastly larger set of communication devices within the PSTN, usually referred to as Network Elements (NEs) or Managed

[25] ITU-T M.3010, "SERIES M: TMN AND NETWORK MAINTENANCE: INTERNATIONAL TRANSMISSION SYSTEMS, TELEPHONE CIRCUITS, TELEGRAPHY, FACSIMILE AND LEASED CIRCUITS: Telecommunications management network: Principles For A Telecommunications management network", INTERNATIONAL TELECOMMUNICATION UNION TELECOMMUNICATION STANDARDIZATION SECTOR, 02/2000

[26] ITU-T M.3400, "SERIES M: TMN AND NETWORK MAINTENANCE: INTERNATIONAL TRANSMISSION SYSTEMS, TELEPHONE CIRCUITS, TELEGRAPHY, FACSIMILE AND LEASED CIRCUITS: Telecommunications management network: TMN management functions", INTERNATIONAL TELECOMMUNICATION UNION TELECOMMUNICATION STANDARDIZATION SECTOR, 02/2000

TABLE 1.4. Example Well-Known OSSs Used by Many SPs.

Functional Area	Functional Activities	Well-Known Example OSSs
Infrastructure Provisioning Systems	Forecasting	TNDS/TK
	Planning	LEIS–LEAD
	In-place Network Inventory	LEIS–LEAD and TIRKS
	Inventory Management	PICS/DCPR, TIRKS, CMA, CRIS
	Network Request Entry/ Management	CRIS
	Operations Performance Reporting	CRIS and LEIS–LEAD
	Design	CRIS
Service Provisioning Systems	TN/Address Inventory	FACS and SWITCH
	Operations Performance Reporting	Varies by SP
	Assignable Inventory	LFACS, SWITCH, and TIRKS
	Service Fallout & Resolution	Varies by SP
	Service/ Inventory Management	LFACS, SWITCH, and TIRKS
	Design & Assign	LFACS, SWITCH, and TIRKS
	Activation	Varies by SP
	Service Request & Performance Management	SOAC
Service Assurance Systems	Trouble Entry	RETAS
	Trouble Management	WFA/C and LMOS
	Operations Performance Reporting	Varies by SP
	Performance Monitoring & Trend Analysis	NTDCA
	Circuit Inventory	TIRKS, NSDB, LMOS
	Fault Location & Integrated Testing	DELPHI and MLT
	Proactive Fault Discovery	NFM and NMA
	Network Management & Reconfiguration	ACCESS7
	Traffic Data Collection	TNDS/TK, NDS–TIDE, and NTDCA
	Billing Data Collection	Varies by SP
Administration Systems	Billing	BOSS, CRIS, and CABS
	Field Access	Varies by SP
	Workforce Management	WFA/DI and FWA/DO

TABLE 1.5. Example OSS Brief Descriptions.

OSS	Description, Purpose, or Usage
ACCESS7	A distributed OSS that collects and analyzes messages from SS7 links. It is totally switch independent, providing a comprehensive, impartial view of what is happening on the network even during fault conditions.
BOSS	BOSS (Billing and Order Support System) allows access to and contains bill and credit information, equipment information, carrier billing information, customer contact notes, and payment history.
CABS	Carrier Access Billing System (CABS) is a system for billing interexchange carriers and other SPs for network access.
CRIS	Customer Record Information System (CRIS) contains the customer billing database and is used in the customer billing process.
DELPHI	The Delphi system provides connectivity to test systems.
EADAS/ EADAS/ NM	Engineering and Administrative Data Acquisition System (EADAS), used since the late 1970s, is the major data collecting system of TNDS and is used by network administrators to determine QoS and to identify switching problems. It also makes additional real-time information available to these administrators by providing traffic data history that covers up to 48 hours. EADAS/NM uses data directly from EADAS as well as receiving data from switching systems which do not interface with EADAS. It is used to analyze problems in near real time to determine their location and causes.
LEIS–LEAD	The Loop Engineering Information System (LEIS) is a family of applications that is made up of multiple modules that contain multiple databases. The Loop Engineering Assignment Data (LEAD) module of LEIS contains a separate database for each wire center.
LFACS	Loop Facilities Assignment and Control System (LFACS) maintains an inventory of local loop access facilities with automated assignment of customer access circuits and support of maintenance and engineering activities. LFACS also assigns outside loop plant facilities to requests received from SOAC as a result of customer service order activity.
LMOS	The Loop Maintenance Operations System (LMOS) is a trouble ticketing system that plays an essential part in the act of repairing local loops (telephone lines). LMOS is responsible for trouble reports, analysis, and similar related functions. LMOS started as a mainframe application in the 1970s and was one of the first telephone company operations support systems to be ported to the UNIX operating system.
MLT	Mechanized Loop Test (MLT) is a system that tests subscriber access lines (local loops), which is comprised of the wires and equipment used to provide dial tone/calling service to end users. MLT hardware is located in a repair service center, and test trunks connect MLT hardware to the telephone exchanges or wire centers, which in turn connect with subscriber loops.
NFM	Network force management (NFM) is a system that provides awareness screens that depict alarm condition descriptions for switch and facility alarms.
NMA	Network Monitoring and Analysis (NMA) is a system for monitoring all network facilities for abnormalities and provides transport of trouble alarm information.
NSDB	Network and service database (NSDB) is a repository for line record, customer, circuit, and call service data.

(*continued*)

TABLE 1.5. (*cont'd*)

OSS	Description, Purpose, or Usage
NTDCA	Network Traffic Data Collection & Analysis (NTDCA) is used to warehouse data collected by TDMS; NTDCA allows for long-term data storage of trunk capacity and overflow information.
PICS/DCPR	PICS is the mechanized operations system developed for the efficient management of large amounts of equipment inventories. It assists with both inventory and materials management and the introduction of new types of equipment while phasing out older types and sets utilization goals that balance service objectives and carrying charges on spare equipment. PICS/DCPR (PICS with Detailed Continuing Property Records) administers all types of PSTN Central Office (CO) equipment. The DCPR portion of PICS/DCPR serves as a detailed investment database supporting accounting records for all types of CO plug-in and "hardwired" equipment.
PREMIS	Premises Information System (PREMIS) is a geographical database that allows SP employees to perform customer lookups by telephone number (CNA), check for multiple subscribers at an address (upstairs/downstairs), and view account status. It has three mechanized databases: address data, a credit file, and a list of available telephone numbers.
RETAS	The Repair Trouble Administration System (RETAS) is a front-end tool that allows Competitive Local Exchange Carriers to interface with an SP's OSS maintenance and repair systems.
SOAC	Service Order Analysis and Control (SOAC) is an OSS for coordinating the provisioning order management process. SOAC schedules and manages tasks performed by provisioning systems such as facility assignment, circuit design, and network activation.
SWITCH	Switch/Frame Operations Management System (SWITCH) maintains the inventory of equipment inside PSTN switching COs.
TIRKS	Trunks Integrated Record Keeping System (TIRKS), used since the late 1970s, provides inventory and order control management of interoffice trunk circuits that interconnect telephone switches, supporting circuits from Plain Ordinary Telephone Service (POTS) and 150 baud modems up through T1, DS3, SONET, and DWDM. TIRKS consists of five major interacting component systems: Circuit Order Control system (COC), Equipment system (E1), Facility system (F1), Circuit system (C1), and Facility and Equipment Planning System (FEPS).
TNDS	TNDS is a set of coordinated systems which support a broad range of activities that depend on accurate traffic data. TNDS supports operations centers responsible for administration of the trunking network, network data collection, daily surveillance of the load on the switching network, the utilization of equipment by the switching network, and the design of local and CO switching equipment to meet future service needs.
WFA/C	Workforce Administration/Control (WFA/C) stores trouble tickets by circuit number and includes location, trouble history, and connections to other circuit details.
WFA/DI/DO	Workforce Administration/Dispatch In (WFA/DI) and Workforce Administration/Dispatch Out (WFA/DO) are OSSs supporting COs and field activities that include coordinating, assigning, dispatching, and tracking work requests.

Network Elements (MNEs). ITU-T M.3400 focuses on expanding the initial FCAPS management concept areas introduced in ITU-T X.700.

1.4.1.1 Basic TMN Concepts. M.3010 describes a Telecommunication Management Network (TMN) architecture to support the management needs of PSTN SPs in the planning, provisioning (configuring), installation, maintenance, operation, and administration of telecommunication networks and the services delivered over these networks. The basic concept of the TMN is to provide an organized approach for the interconnection between various types of OSSs and telecommunications equipment (devices) using an architecture with standardized interfaces defining protocols and messages. In defining the concept of the TMN, M.3010 was written to accommodate not just a complex infrastructure of OSSs, networks, and devices already deployed but also provide access to, and display of, management information contained within the TMN to service customers/users. Figure 1.12 shows the general relationship between a TMN and a telecommunications network which it manages. Most PSTN SPs implement their TMNs as a physically separate set of network links that interface telecommunications network devices at multiple points for information transfer and operational control. The parallel and separate TMN implementation is common to enhance TMN availability and ensure that the TMN is operational even when managed telecommunications network links and devices are experiencing congestion, overload, or even failures.

The goal of the TMN concept 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, networks, and services using generic information models and standard interfaces. A key component of the TMN concept is the ability to support a wide variety of management areas, such as infrastructure planning, equipment installation, ongoing operations and administration of devices and services, device maintenance, and service provisioning of telecommunications networks and services. The TMN functional architecture presented in ITU-T M.3010 provided a decomposition of management functionality into the following categories:

- Operations Systems functions;
- Management Application functions;
- Network Element to Management Application interaction functions;
- Transformation functions; and
- Workstation to Management Application interaction functions.

Another aspect of the TMN is the identification of reference points which delineate external views of management functionality. These TMN reference points can represent the interactions between a particular pair of management functions. The reference point concept is considered important as it represents the aggregate of all of the abilities that a particular management function seeks from another particular management function.

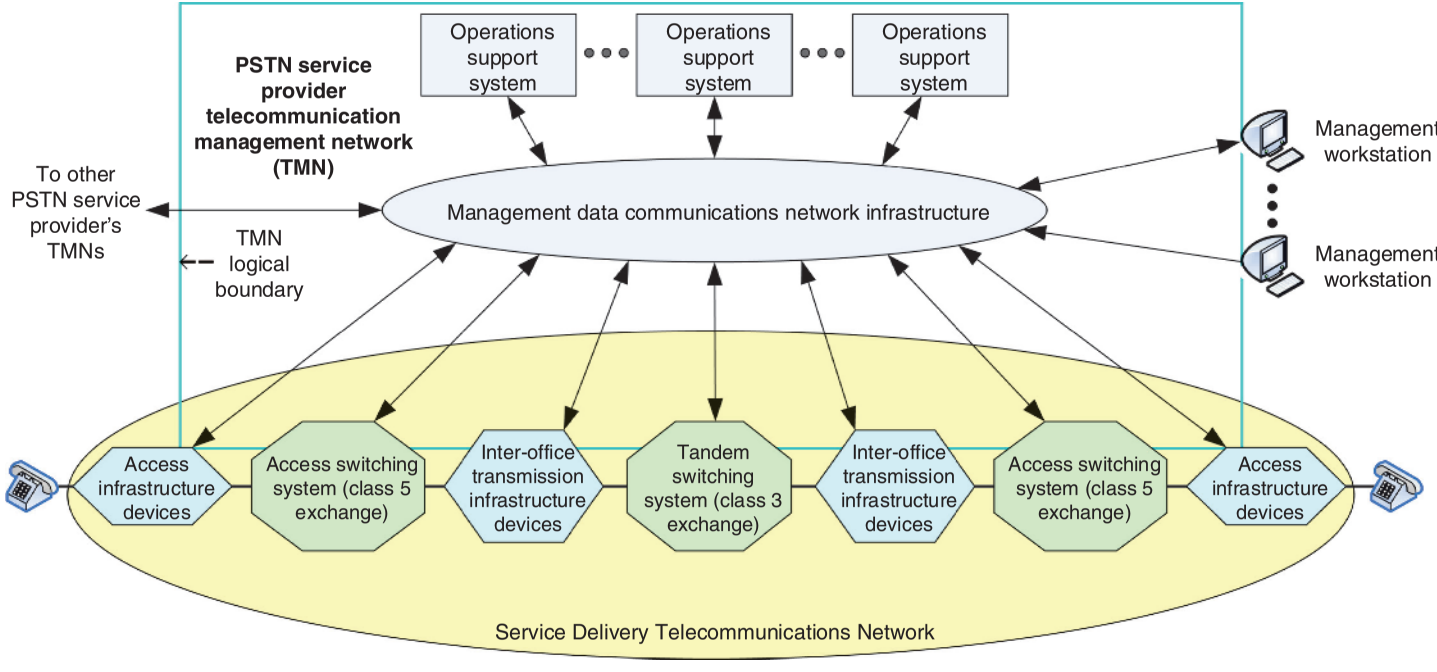

Figure 1.12. Major TMN Components.

It also represents the aggregate of all of the operations and/or notifications (such as alarms and alerts) that a management function can provide to a requesting management function. These TMN-specified reference points usually correspond to a physical interface if and only if the management functions are implemented in different devices.

The TMN concept deals with the complexity of telecommunications management, by partitioning management functionality into logical layers which organizes management functions into groups and describes the relationship between layers. A logical layer reflects particular aspects of management arranged by the following different levels of abstraction:

- business management;
- service management;
- network management;
- element management; and
- network elements.

Element Management Layer (EML) systems (EMSs) manage NEs on an individual or group basis. Within the EML, there may be one or more EMSs that are individually responsible for some subset of NEs.

According to the TMN, an EMS within the EML has the following three principal roles:

1. Control and coordination of a subset of NEs on an individual NE basis. In this role, an EMS is intended to support interaction between network management layer (NML) systems and NE layer devices by processing management information being exchanged between NML systems and individual NEs. EMSs are expected to provide full access to NE functionality.
2. An EMS may also control and coordinate a subset of NEs on a collective basis.
3. An EMS should maintain statistical, log, and other data about NEs within its scope of control.

The majority of commercially available EMS products provide extensive management capabilities over NEs but frequently are not designed to be subservient to NML systems beyond reporting log information, alarm notifications, and event forwarding to these NML systems. The primary management functionality of these EMSs focus on NE Fault, Configuration, and Performance management via the SNMP's[27] "set", "get", and "trap" commands. Rarely is security management available beyond what can be provided by Fault reporting and Configuration change. Another problem with today's EMS products is that these products are rarely designed to manage a heterogeneous collection of NEs. Routinely, a manufacturer will develop and sell an EMS that is only capable of working with that manufacturer's products and even limited to a subset of these products.

[27] RFC 1157, "A Simple Network Management Protocol (SNMP)," Internet Engineering Task Force, May 1990; RFC 1446, "Security Protocols for version 2 of the Simple Network Management Protocol (SNMPv2)," Internet Engineering Task Force, April 1993; RFC 3414, "User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)," Internet Engineering Task Force, December 2002.

Network Management Layer (**NML**) systems (NMSs) have the responsibility for the management of a variety of network devices. The TMN identifies an NMS as addressing the management of devices and EMSs over a wide geographical area. Complete visibility of the whole network is expected, and an NMS is supposed to provide a technology-independent view to service management layer (SML) systems. According to the TMN, an NMS has the following five principal roles:

1. Control and coordination of the network view of all NEs within the NMS's scope or domain;
2. Provision, cessation, or modification of network capabilities for the support of services to customers;
3. Maintenance of network capabilities;
4. Maintenance of statistical, log, and other data about the network and interaction with service manager layer systems on performance, usage, availability, etc.; and
5. May manage interaction between and connectivity with other NMSs.

TMN NMSs are intended to manage a network by coordinating activity across all network devices to support the "network" demands made by SML systems. These NMSs are expected to know what network resources are available, how these resources are interrelated, and how these resources can be controlled. Systems within this layer are identified as responsible for the performance of the network and control available network resources to provide necessary accessibility and quality of service (QoS).

Unfortunately, commercially available NMS products provide extensive management capabilities over diverse NEs but are rarely designed to be subservient to SML systems; nor do they actually understand the relationship between network resources and service establishment, access, or service quality. As with EMSs, available NMSs primarily focus on NE Fault, Configuration, and Performance management via SNMP's "set", "get", and "trap" commands. Also, these NMSs have minimum specific security management capabilities beyond what can be provided by Fault reporting and Configuration change capabilities, especially as security-related parameters should be identified and managed as specifically security related. The primary difference between typical NMS products and typical EMS products is that NMS products are usually designed to manage a heterogeneous collection of NEs whereas the EMS products are not.

As defined within the TMN architecture, Service Management Layer (**SML**) systems focus on the administrative aspects of services that are being provided to customers. Some of the main functions provided by systems within this layer are service order handling, complaint handling, and invoicing/billing. These SML systems are expected to:

1. provide support for customer service personnel for all service transactions including service ordering, provisioning, modification and termination of services, account administration, QoS, and fault reporting, etc.;

2. interface with SML systems of other SPs; and
3. maintain service-oriented statistical data for ensuring QoS/performance commitments are met.

Historically, these SML systems were directly developed by PSTN SPs in-house with no regard for security issues beyond basic administrative and user login authentication. Throughout much of the twentieth century, very few PSTN-offered services included any form of security capabilities resulting; therefore, security management capabilities for service-related security have been basically non-existent.

The TMN **Business Management Layer (BML)** is described as having responsibility for the total enterprise with BML systems accessing information and functionality in other management layer systems. Systems in this layer are expected to carry out "goal setting tasks rather than goal achievement but can become the focal point for action in cases where executive action is called for."[28]

M.3010 goes on to say that the main functions of the BML systems are for optimizing investment and use of new SP resources and support:

1. the decision-making process for the optimal investment and use of new telecommunications resources;
2. the management of OA&M-related budget;
3. the supply and demand of OA&M-related manpower; and
4. aggregation of data about the total enterprise.

Table 1.6 provides a snapshot of the functionality within each TMN layer and other details.

EML and NML management systems rarely provide management of functionality above the transport protocol (layer 4), or Transport Stratum. SML management systems either rely on EML/NML systems for direct administration of elements or some may subsume EML and NML capabilities internally. Many SP SML systems fall into the latter type and are referred to as OSSs. The TMN approach to organizing management systems and functionality served well for many years, yet has led to a series of separate TMNs, with each TMN supporting a specific business/service activity. These separate TMNs evolved over time with little concern for cross-resource management among all products/services and as such are colloquially called "siloed" systems as they are totally stand-alone as a grain silo on a farm, as represented in Figure 1.13.

So long as business/organizations focused only on a single type of service, having siloed management was not an issue. With convergence of services onto common communications infrastructures (CCIs) and consolidation of businesses offering integrated services, siloed management now represents an operational inefficiency, likely source of coordination problems, security vulnerabilities, and even loss of actual or potential revenue. This reality has led to further study of the necessary management functions, and their organization, for economical, secure, and efficient management of multiple services. The TeleManagement Forum (TMF) has been working on the "Next Generation

[28] Section 9.5.1.4 of ITU-T M.3010.

TABLE 1.6. TMN Management Layers.

TMN Layers	Role/Purpose
BML systems	Provide high-level planning, budgeting, goal setting, decision support, and business level agreements. These are proprietary in design and frequently "home-grown," geographically redundant, typically deployed following a client–server approach, and usually utilize CORBA, DCE, XML, .NET, and SNMP protocols.
SML systems	Rely on information presented by NML systems to manage contracted for services of existing and potential customers. Provides basic point of contact support with customers for provisioning, accounts, QoS, and fault/performance management. SML systems are also a key point for SP interaction with other PSTN administrative domains. These systems may be quasi standards based, geographically redundant, and using a distributed deployment design, and usually utilize CORBA, TL1,[29] DCE, XML, .NET, and SNMP protocols.
NML systems	Responsible for management of heterogeneous collections of NEs frequently co-located or integrated into a service or organization security domain. These are usually standards based, geographically distributed, typically designed to use a client–server architecture, and usually utilize SNMP, TMF-814,[30] and sometimes XML and telnet protocols.
EML systems	Responsible for management of homogeneous collections of NEs. These are usually vendor specific, geographically distributed, typically designed to use a client–server architecture, and usually utilize SNMP and sometimes TL1, XML, and telnet protocols.
NEL systems	Devices that provide transport, application, and infrastructure services within a network infrastructure.

Operations Systems and Software" (NGOSS) program to address these very issues. Before considering NGOSS components, we will first review how the TMN deals with the management of security.

1.4.1.2 TMN Security Management Concepts. The management of security outlined in ITU-T X.800 is further developed in ITU-TM.3400 by mapping the services defined in ITU-T X.800 for authentication, access control, data confidentiality, data integrity, and non-repudiation using the perspective of a set of functional capabilities organized around:

- Prevention;
- Detection;
- Containment and recovery; and
- Security administration.

ITU-TM.3400 notes that security of management is necessary for all TMN management functional areas and transactions that occur during communications between

[29]TL1 messages are used to accomplish specific functions between an OSS and an NE. TL1 is defined in Telcordia Technologies (formerly Bellcore) Generic Requirements document GR-831-CORE.

[30] TMF 814, "Multi-Technology Network Management Solution Set, NML-EML Interface Version 2.0", TeleManagement Forum, 2001.

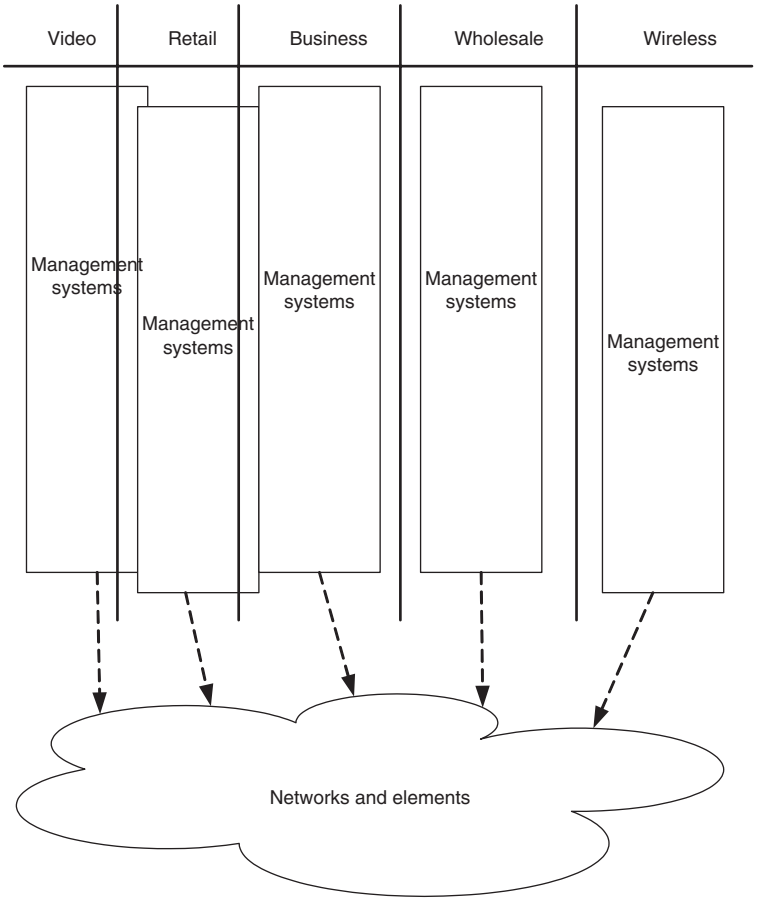

Figure 1.13. Siloed Management System Structuring.

systems, between customers and systems, and between internal users and systems. The set of pervasive security mechanisms discussed in ITU-T X.800 (i.e., event detection, security audit trail management, and security recovery) are also considered applicable to any network communication activities so that security event detection and reporting are communicated to higher security management systems of any activity that may be a security violation (e.g., unauthorized user or access attempt, logical or physical tampering with equipment, network traffic indicative of malicious behavior or actions, etc.).

1.4.1.2.1 TMN Prevention Security Concepts. The Prevention functions are organized into sets of capabilities identified as those needed to prevent intrusions. The TMN Prevention concepts span the following activities:

- Legal review of corporate documents and service offerings;
- Physical access controls to enterprise facilities and areas within these facilities;

- Human access monitoring and inspection of packages/containers entering/leaving enterprise facilities;
- Personnel controls focusing on checking the trustworthiness of employees and other personnel that access enterprise facilities for business purposes; and
- Customer verification of the ability to pay for services ordered/purchased as well as determining that a customer is legally permitted access to requested services or products.

These capabilities are primarily procedural in nature, rather than technology focused. However, these are not the only Prevention capabilities an enterprise would or should deploy.

Prevention is the act of limiting the occurrence of unauthorized or potentially harmful behavior or activities. Thusly, there are a large number of authentication and authorization access control capabilities that should be deployed such as:

- IEEE 802.1x for Peer-entity or Data-origin authentication and authorization for link layer usage;
- IPsec (especially ESP-nul) for Peer-entity and Data-origin authentication, authorization, and optional confidentiality of both network and host packet flows;
- transport layer security (i.e., TLS, SSL, DTLS, SSH) for Peer-entity and/or Data-origin authentication, authorization, and confidentiality of application communications flows; and
- device operating system and application hardening for user/administrator authentication, authorization, and access control.

From an access control perspective, an enterprise should be deploying mechanisms such as firewalls, Intrusion Prevention Systems, and Session Border Controls. Anti-malware (viruses, worms, keyboard scanners, root-kits, Trojans, etc.) scanners should be included within the Prevention area as these products are designed to remove, not just identify the presence of, malware. Unfortunately, the ITU-TM series recommendations do not provide any procedural and technical details of these prevention security mechanisms that necessitate some level of security administration.

1.4.1.2.2 TMN Detection Security Concepts. The TMN Detection functions are organized into sets of capabilities identified as those needed to detect intrusions. The TMN procedurally oriented Detection capabilities are:

- revenue pattern analysis for significant shifts in revenue that might indicate fraud or theft of service;
- determination of need for, including monitoring and analysis of, security alarm systems and alarms indicating power or HVAC (heating, ventilation, and air conditioning) failures in addition to the occurrence of fire, flood, and open doors or cabinets/chassis; and
- investigation of fraud or theft of service by customer and internal users based on usage patterns.

These procedural Detection capabilities will certainly require information processing resources; yet it is primarily personnel who are responsible to ensure the pre-requisite

analyses, determinations, and investigations occur consistent with approved enterprise security policy and procedures within the context of the enterprise's overall security governance program.

The TMN service-oriented Detection capabilities are:

- Customer access to SP security alarm information that indicates security attacks on a customer's network infrastructure, and
- Collection and analysis of customer usage data profiles to identify anomalies and irregularities indicative of a security breach or theft of service.

SPs may, or may not, consider informing their customers that these customers are under some form of attack; however, this capability will be likely based on SP service design and market considerations, and not a general offering by all SPs. It is more likely that an SP will track customer service usage as one way to perhaps identify a security breach or theft of service. The use of this capability will be affected by the budget limitations the SP places on allocation of personnel and Information Technology (IT) resources to such data collection and analysis along with any decided upon follow-up actions.

The TMN SP infrastructure-oriented Detection capabilities are:

- data collection and analysis of network traffic and activity patterns to identify anomalies, abnormalities, or actual activity indicative of a security breach or attack;
- capabilities to receive, store, correlate, and analyze audit trail log information from:
  - network intrusion detection systems (IDS);
  - network traffic and activity pattern analysis systems (i.e., NetFlow[31]);
  - NE IDS (host IDS);
  - NE security alarm management systems (SEMs[32]); and
  - NE log and audit trail management systems (such as syslog[33]) for the purposes of identification, reporting, and recording of anomalies or abnormalities;

[31] Although initially implemented by Cisco, the NetFlow protocol, described in RFC 3954 has been superseded by Internet Protocol Flow Information eXport (IPFIX), described in RFC 5101 and RFC 5102, with network product vendors adding IPFIX support to their devices. With IPFIX, a router will output a flow record when it determines that a unique flow of packets has ended.

[32] A security event manager (SEM) is an application used to centralize the storage and interpretation of events generated by other networked devices. The SEM concept is about 10 years old and still evolving. Some of these products are called security information managers (SIMs) or security information and event managers (SIEMs).

[33] Syslog is a standard (RFC 5424) for logging program logging message by separating the system that generates messages from the system that stores them and the software that reports and analyzes them. Syslog can be used for device management and security auditing and is supported by a wide variety of devices and receivers across multiple platforms. Because of this, syslog can be used to integrate log data from many different types of systems into a central repository.

- capabilities to receive, store, correlate, and analyze security alarms generated by NML, EML, and NE systems from:
  - network IDS;
  - network traffic and activity pattern analysis systems;
  - NE IDS;
  - NE SEMs; and
  - NE log and audit trail management systems;
- reporting and display of security alarm information that indicate the occurrence of network security violations indicative of a security breach or attack.

The deployment of any of the aforementioned detection mechanisms will be affected by the budget constraints the SP has on the allocation of personnel and IT resources to such data collection and analysis along with any decided upon follow-up actions. All deployed procedural and technical detection security mechanisms necessitate some level of security administration that is not covered by the TMN recommendations.

1.4.1.2.3 TMN Containment and Recovery Security Concepts. The TMN discussed Containment and Recovery functions are organized into sets of capabilities identified as those needed to deny access to an intruder, to repair damage done by an intruder, and to recover losses. The TMN information-protection-oriented Containment and Recovery capabilities are:

- access and management mechanisms to protect storage of business, customer, network configuration, and NE configuration data;
- maintaining backup copies of data; and
- monitoring for data corruption.

Protection of stored information on customers, the enterprise, and enterprise infrastructure components should not be considered part of Containment and Recovery but rather as a Prevention capability. The protection mechanisms would include use of access control lists (ACLs), assignment of access rights to customers, and internal users commensurate with each subject's authorized "need to know" rights/privileges. Maintaining backup copies of information necessary for enterprise continued operation is just sound business continuity policy and should not be described as primarily a security capability. However, monitoring for data integrity is a valid security concern and is properly a Prevention function, especially when provided by the use of mechanisms such as Tripwire.[34]

The TMN containment-oriented Containment and Recovery capabilities are:

- isolation of equipment or data so that corruption is not propagated;
- remove/revoke of customer or internal user access privileges; and

[34] Tripwire is a software security and data integrity tool useful for monitoring and alerting on specific file change(s) within systems. An available open-source version detects changes to file system objects serving purposes, such as integrity assurance, change management, and policy compliance. Other open-source projects exist that provide similar functionality. Examples include OSSEC, AIDE, and Samhain.

- severance of either internal user or customer connections to limit data and system corruption as the result of a detected security violation.

These are quite properly containment-type capabilities. However, action to effect device isolation, access privilege revocation, or connection termination routinely requires human interaction via generalized configuration management system functions. Some industry designers consider it desirable to have security management software be able to automatically perform isolation, revocation, and termination actions; yet, there are others who believe that a human needs to be part of the decision-making "loop" and argue for automation of these capabilities with humans making the decision to initiate the corresponding action.

The TMN identifies a number of forensic- and legal-involvement-oriented Containment and Recovery capabilities including:

- cooperation with law enforcement agencies against a perpetrator of an illegal action;
- forensic investigation of a detected, or suspected, security violation;
- assistance to law enforcement agencies in apprehending an intruder including identification of an intruder via actions such as analyzing security logs, monitoring targets of intrusion, or feeding misinformation to a suspected intruder; and
- ability to initiate litigation against a perpetrator of an illegal action.

Cooperation with law enforcement agencies and the ability to litigate perpetrators are actually security governance capabilities, and not security management capabilities. The performance of forensic investigations necessitates an enterprise possess personnel qualified and trained in forensic investigation procedures and procedurally required to act as "first responders" whenever an actual, or suspected, security breach occurs or some type of abnormal event occurs.

The TMN recovery-oriented Containment and Recovery capabilities are:

- restoration of backed up data upon request;
- backup and restoration of stored data in support of intrusion recovery;
- service intrusion recovery that supports requests to access backup files in order to restore service after detection of a security violation;
- network intrusion recovery that supports requests for restoration of the network configuration after detection of a security violation; and
- NE intrusion recovery that provides access to backup files in order to restore NE or element management information after detection of a security violation.

The secure and routine creation of data backup sets (regardless of contents) should be a standardized part of general enterprise operations, and not just a part of security management. The creation, transportation (physical or electronic), storage, and restoration of data backup sets should always be subject to appropriate authentication, authorization, integrity, and confidentiality mechanisms and operational procedures.

The TMN authentication-and–authorization-revocation-oriented Containment and Recovery capabilities are identified as the ability to:

- revoke network device public key, customer public key, and employee public key certificates used for NE or service access that are known as, or suspected of being, invalid due to a security violation resulting in suspected private key theft, or the private key is no longer available due to it being modified or lost while stored in an encrypted form;
- revoke network device public key, customer public key, and employee public key certificates used for NE or service access due to administrative procedures (e.g., a system has been replaced, a customer has moved elsewhere, an EMS or NE has been replaced, etc.);
- revoke network device, customer, and employee access control certificates used for NE or service access that are known as, or suspected of being, invalid due to a security violation;
- revoke network device, customer, and employee access control certificates used for NE or service access due to administrative procedures (e.g., a system has been replaced, a customer has moved elsewhere, an EMS or NE has been replaced, etc.); and
- revoke or replace shared secret keys known as, or suspected of being, invalid due to security violation (e.g., theft of secret keys, actual or suspected breach, or KDC system, etc.).

Whenever asymmetric encryption public keys are used within an enterprise, these public keys should only be stored, distributed, and used when embedded within ITU-T X.509 version 3 digital certificates issued by authenticated and authorized Digital Certificate Authorities that are part of a formally recognized Public Key Infrastructure (PKI) (see Appendix B). The certificate revocation capabilities contained within a PKI (whether use of CRLs[35] or OCSP[36]) should be the approach relied upon by enterprises regardless of the cause being: private key theft, private key loss, or revocation due to administrative decisions. These PKI revocation mechanisms can support both public-key-containing digital certificates as well as authorization (access control) digital certificates. The use of shared secret keys for symmetric encryption or secret-key-based message authentication (such as with HMAC[37] algorithms) should only be accomplished via a standardized KDC[38] (such as the Kerberos system), via secure dynamic key

[35] CRL stands for Certificate Revocation List which is a mechanism that allows for verifying whether a Certificate Authority (CA)-issued X.509 digital certificate has been revoked prior to its stated "Not After" date due to the corresponding private key either no longer available for use has actually been stolen or cannot be used for administrative reasons.

[36] OCSP represents the Online Certificate Status Protocol which provides the capability for a requester to make a query whether a specified X.509 digital certificate has been revoked.

[37] HMAC stands for Hash-Based Message Authentication Code. U.S. Federal Information Processing (FIPS) Publication 198 generalizes and standardizes the use of HMACs such as HMAC-SHA-1 and HMAC-MD5 which are used within the IPsec and TLS protocols.

[38] KDC stands for Key Distribution Center which is a facility responsible for the generation, storage, distribution, and revocation/destruction of shared symmetric secret encryption keys.

agreement algorithms such as the Internet Key Exchange and Internet Security Association Key Management Protocol within IPsec, or a secure Diffie–Hellman key negotiation within the context of TLS, SSL, DTLS, SSH protocols, or XML key management.

1.4.1.2.4 TMN Security Administration Concepts. The Security Administration function sets are those needed for planning and administering security policy and managing security-related information.

The planning- and analysis-oriented Administration capabilities include:

- Security policy that provides access to company guidelines for establishing and maintaining a secure environment for personnel, hardware, and software;
- Disaster recovery planning that supports access to methods and procedures to be used in restoring the network in the event of a security breach and the resulting corruption of data; and
- Assessment of corporate data integrity that provides access to information to determine the need for security, monitoring, and analysis of security measures instituted to protect corporate data from unauthorized access, altering, tampering, and/or corruption.

The procedure-oriented Administration capabilities include:

- Manage guards that provides access to information about the management of physical and mechanized devices used to provide security;
- Audit trial analysis that provides access to methods and procedures for audit trail information to be collected and evaluated to identify possible and/or potential security violations by individuals or groups of users; and
- Security alarm analysis that provides access to guidelines for monitoring, evaluating, and correlating security alarms.

The authentication-oriented Administration capabilities include:

- Administration of external authentication that supports requests for and distributes codes for verification that a customer or user of a peer Administration is who they present themselves to be. It also supports an authentication path involving external authenticators. If a customer has been authenticated by an authentication agent outside the TMN, this function supports the certification, if appropriate, that the external authentication agent is a valid entity for providing that kind of authentication.
- Administration of internal authentication that receives requests for and distributes codes for verification that internal users are who they present themselves to be.

The authorization-oriented Administration capabilities include:

- Administration of external access control that supports requests for and distributes permissions (in accordance with security policy) for control over

what a customer or user of a peer Administration can do with any given resource and includes establishing and validating customer permissions and credentials.

- Administration of external certification that supports requests for and distributes permissions (in accordance with security policy) for control over what a customer or user of a peer Administration can do with any given resource and includes establishing and validating customer permissions and credentials.
- Administration of internal access control that supports requests for and distributes permissions (in accordance with security policy) for control over what an internal user can do with any given resource.
- Administration of internal certification that supports requests for and distributes Access Control Certificates that permit internal users access to previously agreed upon sets of capabilities.

The encryption-key-oriented Administration capabilities include:

- Administration of external encryption and keys that supports requests for and distributes encryption keys to be used in communications between an external customer or user of a peer Administration and a TMN (such keys may be used for authentication, integrity, confidentiality, and non-repudiation).
- Administration of internal encryption and keys that supports requests for and distributes encryption keys to be used in communications between internal users (such keys may be used for authentication, integrity, and confidentiality). It provides information on which encryption algorithms are to be used and in which mode.
- Administration of keys for NEs that supports requests for the generation of encryption keys to be used in communications between NEs or between an NE and an EMS or other building block. It also supports the distribution of these keys to NEs and communicating entities. Such keys may be used for authentication, integrity, and confidentiality.
- Administration of keys by an NE that supports requests for the generation of encryption keys within an NE to be used in communications between NEs or between an NE and an EMS or other building block. It also supports the distribution of these keys to communicating entities. Such keys may be used for authentication, integrity, and confidentiality.

The encryption-algorithm-oriented Administration capabilities include:

- Administration of external security protocols that provides for the management of joint implementation agreements with other jurisdictions to assure interoperability of security protocols. For example, it assures that both communicating parties use the same encryption algorithm with the same set of options and parameters. Further, it assures agreement on the kind of security information that shall be provided for authentication. It also provides for the administration of external security protocols.

The event- and alarm-oriented Administration capabilities include:

- Network security alarm management that supports the collection of security alarm information that indicates network security violations. It allows an internal user access to such data.
- NE(s) security alarm management that supports the collection of security alarms detected by lower level functions. It provides access to such information, possibly including information resulting from the correlation of such alarms.

The audit-oriented Administration capabilities include:

- Customer audit trial that allows a customer to establish and configure audit trails to obtain information about service usage. It allows a customer access to usage and security event information related to their portion of the network.
- Customer security alarm management that allows a customer access to security alarm information that indicates security attacks on their portion of the network.
- Testing of audit trail mechanism that supports testing to ascertain that designated events are recorded in a security log.
- Network audit trail management that allows for internal users, generally security personnel, to establish and configure audit trails to obtain information about network usage. This function collects and allows an internal user access to network usage and security event information.
- NE audit trail management that allows internal users, generally security personnel, to establish and configure audit trails to obtain NE usage data and reports on actions involving, for example, identification, authentication, user address space actions, and administrative data.

The TMN security mechanism management capabilities covered in ITU-T M.3400 are predominantly operational in nature and do not provide much guidance for the:

- planning of an information security management program;
- consideration of what organizational security capabilities are required;
- consideration of what technical security capabilities are required; or
- consideration of what operational security capabilities are required.

1.4.2 Next Generation Operations Systems and Software

The TeleManagement Forum (TMF[39]) has been evolving management concepts with its Next Generation Operations Systems and Software (NGOSS) activity that represents an industry-agreed set of frameworks driven and managed by the TMF that provide:

- Business process modeling that provides an industry agreed upon set of process definitions and an organization of these processes that reflect the relationship of these processes to each other;

[39] www.tmforum.org.

- Standard information and data models that provide an industry agreed upon set of information and data definitions furthering a common understanding as to what information business processes rely upon which furthers the interoperability of business process software applications from competing application system vendors;
- Systems architecture definition that provides an industry agreed upon architecture that identifies and describes how business process support applications should interact with each other which furthers the interoperability of business process software applications from competing application system vendors;
- Integration interfaces that provide an industry agreed upon set of definitions for the interfaces between business process support applications which furthers the interoperability of business process software applications from competing application system vendors; and
- Methodology for the application of the aforementioned process models, information and data definitions, systems architecture, and interfaces.

Five key NGOSS principles are:

1. Separation of Business Process from Component Implementation through the use of the enhanced Telecom Operations Map (eTOM) NGOSS business process framework.
2. A loosely coupled distributed Systems approach so that each application is relatively independent of the other applications in the overall system, thereby allowing that one application can be altered without the alteration necessarily affecting others.
3. A shared information model so that data can be shared between the applications where all applications know how other applications interpret the data that is shared via a common model of the shared data. Within the NGOSS, the Shared Information/Data Model (SID) provides this capability.
4. A CCI allowing OSSs to interface with the CCI rather than directly with each other as had been common since the mid-1980s. The CCI allows these applications to work together using the CCI so that each application only requires one interface instead of many application-specific interfaces reducing interface complexity.
5. Contract-defined interfaces that describe how applications interface to the CCI both in terms of the technology employed and the functionality of the application, the data used, the pre- and post-conditions, etc. These NGOSS contract specifications provide a means to document these interfaces and can be seen as extensions of Application Programming Interface specifications.

The NGOSS initiative is based on the following four interrelated frameworks that form the NGOSS program (depicted in Figure 1.14):

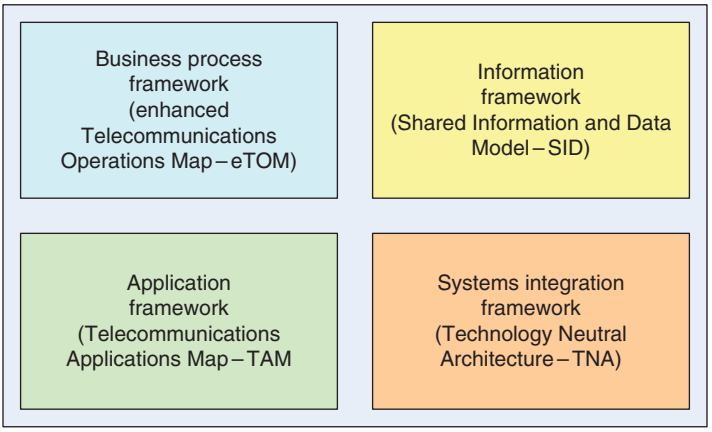

Figure 1.14. NGOSS Initiative Components.

- Business Process Framework—the eTOM[40];
- Enterprise-wide information framework—the SID;
- Systems Integration Framework—the TNA; and
- Telecom Applications Framework—the TAM.

The NGOSS perspective does not contradict the concepts put forth in prior ITU-T recommendations. Rather, ITU-T M.3200 and M.3400 provide a technology- and resource-oriented view of the management domain, which provides value when considering the structure and organization of a management solution. The eTOM framework provides a business-oriented viewpoint that is important in considering the business requirements of the enterprise and ensuring management functions are arranged in a meaningful and useful way reflecting how business is conducted. Where ITU-T M.3400 provides a detailed, functional view on the EMLs, NMLs, and SMLs, the ITU-T M.3050 series of

[40] M.3050.0, "eTOM – Introduction," International Telecommunication Union, TELECOMMUNICATION STANDARDIZATION SECTOR, March 2007; M.3050.1, "eTOM – The business process framework," International Telecommunication Union, TELECOMMUNICATION STANDARDIZATION SECTOR, March 2007; M.3050.2, "eTOM – Process decompositions and descriptions," International Telecommunication Union, TELECOMMUNICATION STANDARDIZATION SECTOR, March 2007; M.3050.3, "eTOM – Representative process flows," International Telecommunication Union, TELECOMMUNICATION STANDARDIZATION SECTOR, March 2007; M.3050.4, "eTOM – B2B integration: Using B2B inter-enterprise integration with the eTOM," International Telecommunication Union, TELECOMMUNICATION STANDARDIZATION SECTOR, March 2007; M.3050 Supplement 1, "eTOM – An Interim View of and Interpreter's Guide for eTOM and ITIL Practitioners," International Telecommunication Union, TELECOMMUNICATION STANDARDIZATION SECTOR, February 2007; M.3050 Supplement 2, "eTOM – Public B2B Business Operations Map (BOM)," International Telecommunication Union, TELECOMMUNICATION STANDARDIZATION SECTOR, February 2007; M.3050 Supplement 3, "eTOM to M.3400 mapping," International Telecommunication Union, TELECOMMUNICATION STANDARDIZATION SECTOR, May 2004; M.3050 Supplement 4, "eTOM – An eTOM Primer," International Telecommunication Union, TELECOMMUNICATION STANDARDIZATION SECTOR, February 2007.

recommendations provide the business view for those layers, and details of this relation are described in the M.3050 eTOM to M.3400 mapping supplement. It has been proposed that the eTOM level 1 horizontal functional process groupings correspond to the layering in M.3010 in that:

- the eTOM Service Management & Operations (SM&O) grouping corresponds to the M.3010 SML, and
- the eTOM Resource Management & Operations (RM&O) grouping corresponds to both the M.3010 NML and the EML.

Of the four NGOSS areas (eTOM, SID, TNA, and TAM), only the eTOM has progressed to a significant level of detail worth discussing from a security management perspective.

1.4.3 Enhanced Telecom Operations Map

The eTOM Business Process Framework is the ongoing TMF initiative to deliver a business process model, or framework, for describing the enterprise processes required by an SP, or any enterprise, with complex telecommunications and business processes. eTOM analyzes these enterprise processes to different levels of detail according to their significance and priority for the business. Figure 1.15 depicts the overall structure of the eTOM organization of functions.

A key concept with the eTOM is that there are four primary components to an enterprise:

- General Enterprise Management covering the general management and administrative activities that any enterprise needs to address independent of whatever products or services the enterprise provides. Put another way, any organization, be it an appliance manufacturer, telecommunications SP, hospital, university, or even government agency, has management responsibilities for most, if not all, of these activity sub-areas.
- Strategy, Infrastructure, and Product Management covering the management and administrative activities that focus on the planning, design, development, and supply chain required to product the products or services offered by the enterprise. Again most, if not all, of these activities are applicable to most any organization.
- Operations Management covering the management and administrative activities that focus on the delivery of products and services to customers. Again most, if not all, of these activities are applicable to most any organization.
- Customers that are, or should be, the focus of any enterprise, for without customers an enterprise has no reason to exist. One should remember that customers may come from the general population, could be other enterprises, or even be the employees of a larger organization of which the enterprise is part of (namely, an internal support organization).

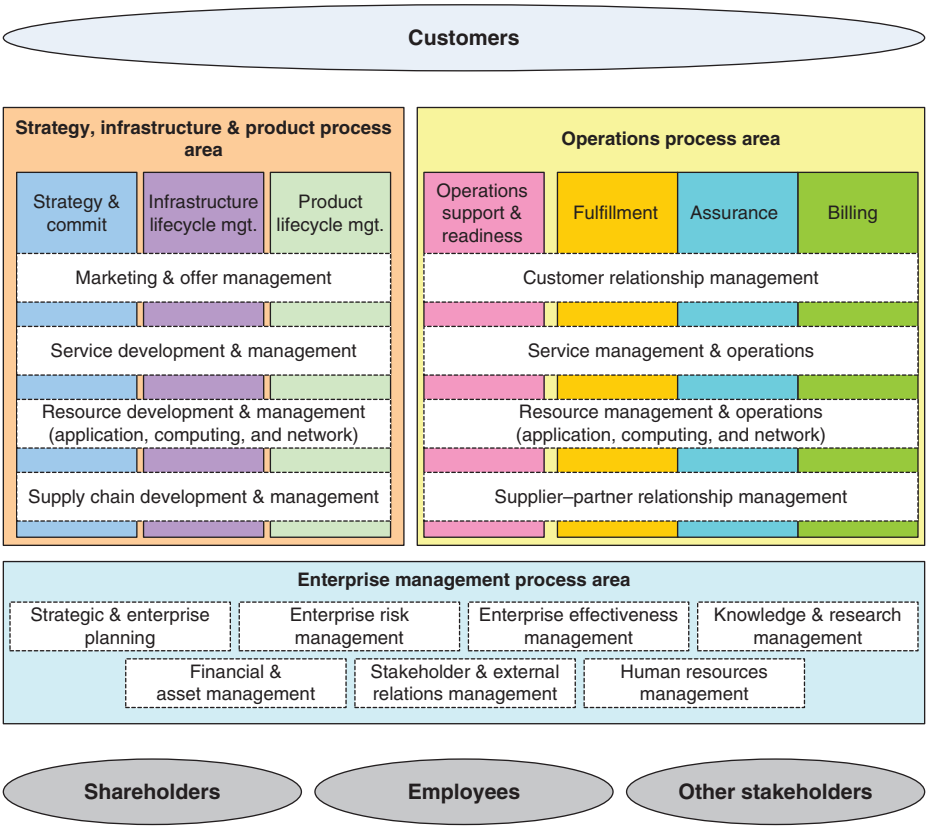

Figure 1.15. eTOM Structure of Functions.

The degree to which these management areas apply to any given enterprise will be primarily affected by the size of the enterprise, the complexity of its offered products or services, and its financial resources.

The eTOM begins at the Enterprise level and defines business processes in a series of groupings to structure business processes and define process descriptions, inputs and outputs, as well as other key elements for each process at each level. These groupings are organized around the three key enterprise areas (shown in Figure 1.16) of:

1. Strategy, Infrastructure, and Product (SIP) Process Area which is concerned with the activities necessary to develop services and resources;
2. Operations Process Area which is concerned with the activities necessary to operate and administer services and resources; and
3. Enterprise Management Process Area which is concerned with the core administrative activities of the enterprise.

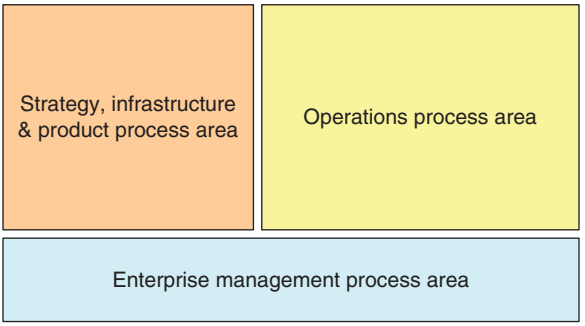

Figure 1.16. eTOM—Key Process Areas.

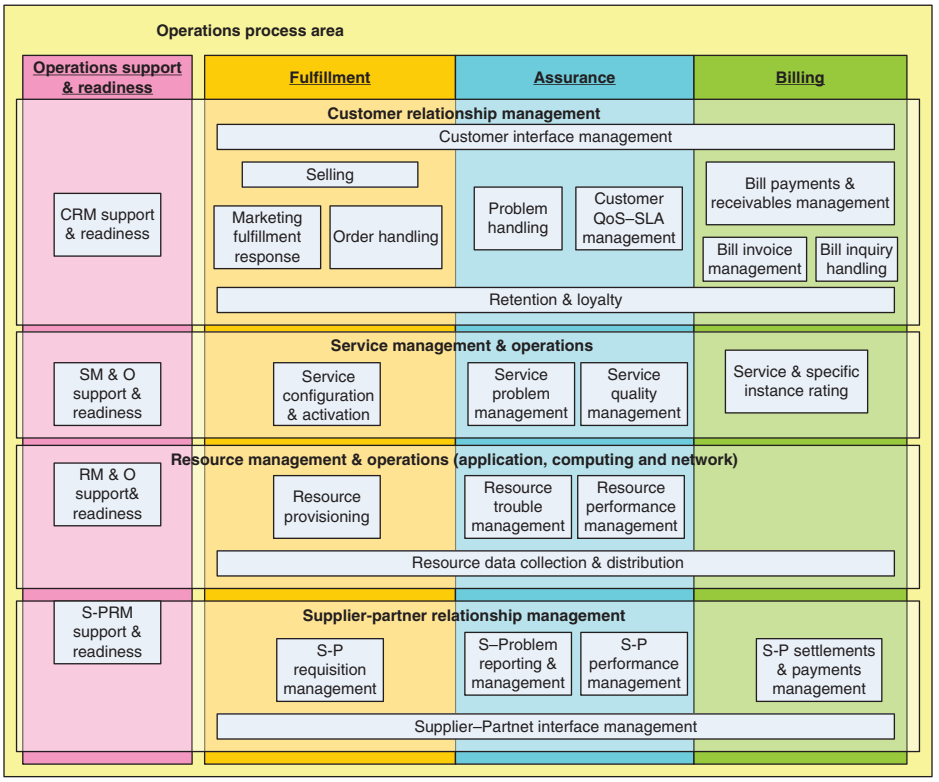

Figure 1.17. eTOM—Level 2 Operations Activity Areas.

The eTOM Framework contains seven vertical and four horizontal process groupings required to support customers and to manage the business. Under the Operations Process Area are the core customer-oriented operations processes of Operations Support and Readiness, Fulfillment, Assurance, and Billing (eTOM 2007 Process Area Identifier 1.1) as depicted in Figure 1.17.

The SIP Process Area (eTOM 2007 Process Area Identifier 1.2), shown in Figure 1.18, contains the Strategy and Commit verticals, as well as two Lifecycle Management verticals. The eTOM also includes horizontal views of functionality across an SP's organization. The horizontal functional process groupings span functional operations processes and other types of business functional processes, for example, Marketing versus Selling, Service Development versus Service Configuration, etc. Among these horizontal functional process groupings, those on the left (that cross the Strategy and Commit, Infrastructure Lifecycle Management, and Product Lifecycle Management vertical process groupings) enable, support, and direct the work in the Operations Process Area.

The Enterprise Management Process Area (eTOM 2007 Process Area Identifier 1.3), shown in Figure 1.19, contains the seven verticals spanning:

- Strategic and Enterprise Planning;
- Financial Asset Management;
- Enterprise Risk Management;
- Stakeholder and External Relations Management;
- Enterprise Effectiveness Management;
- Human Resource Management; and
- Knowledge and Research Management.

The eTOM also includes horizontal views of functionality across an SP's organization.

The mapping of the eTOM (M.3050 version 2007) security-related process areas to M.3400 security management function sets, as provided by M.3050Sup3,[41] is far from complete (see Appendix G for an augmented mapping). The following 14 eTOM clauses are simply mapped to the M.3400 Introduction clause (9) which provides no further specifics:

- Customer Relationship Management (clause 1.1.1);
- SM&O (clause 1.1.2);
- Design Solution (clause 1.1.2.2.1);
- Track & Manage Service Provisioning (clause 1.1.2.2.3);
- Issue Service Orders (clause 1.1.2.2.7);
- Create Service Trouble Report (clause 1.1.2.3.1);
- Diagnose Service Problem (clause 1.1.2.3.2);
- Correct & Resolve Service Problem (clause 1.1.2.3.3);
- Track & Manage Service Problem (clause 1.1.2.3.4);
- Report Service Problem (clause 1.1.2.3.5);
- Close Service Problem Report (clause 1.1.2.3.6);

[41] M.3050 Supplement 3, "eTOM to M.3400 mapping," International Telecommunication Union, TELECOMMUNICATION STANDARDIZATION SECTOR, May 2004.

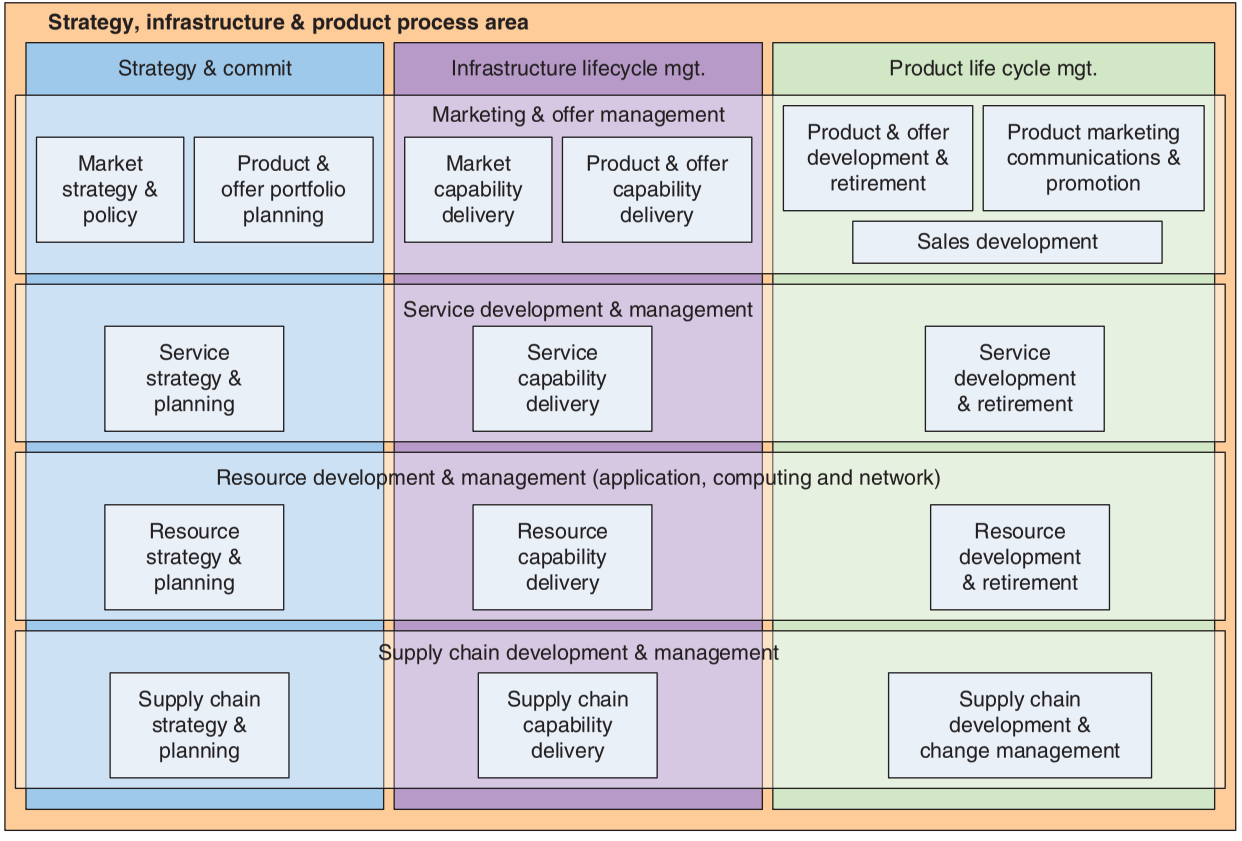

Figure 1.18. eTOM—Level 2 SIP Activity Areas.

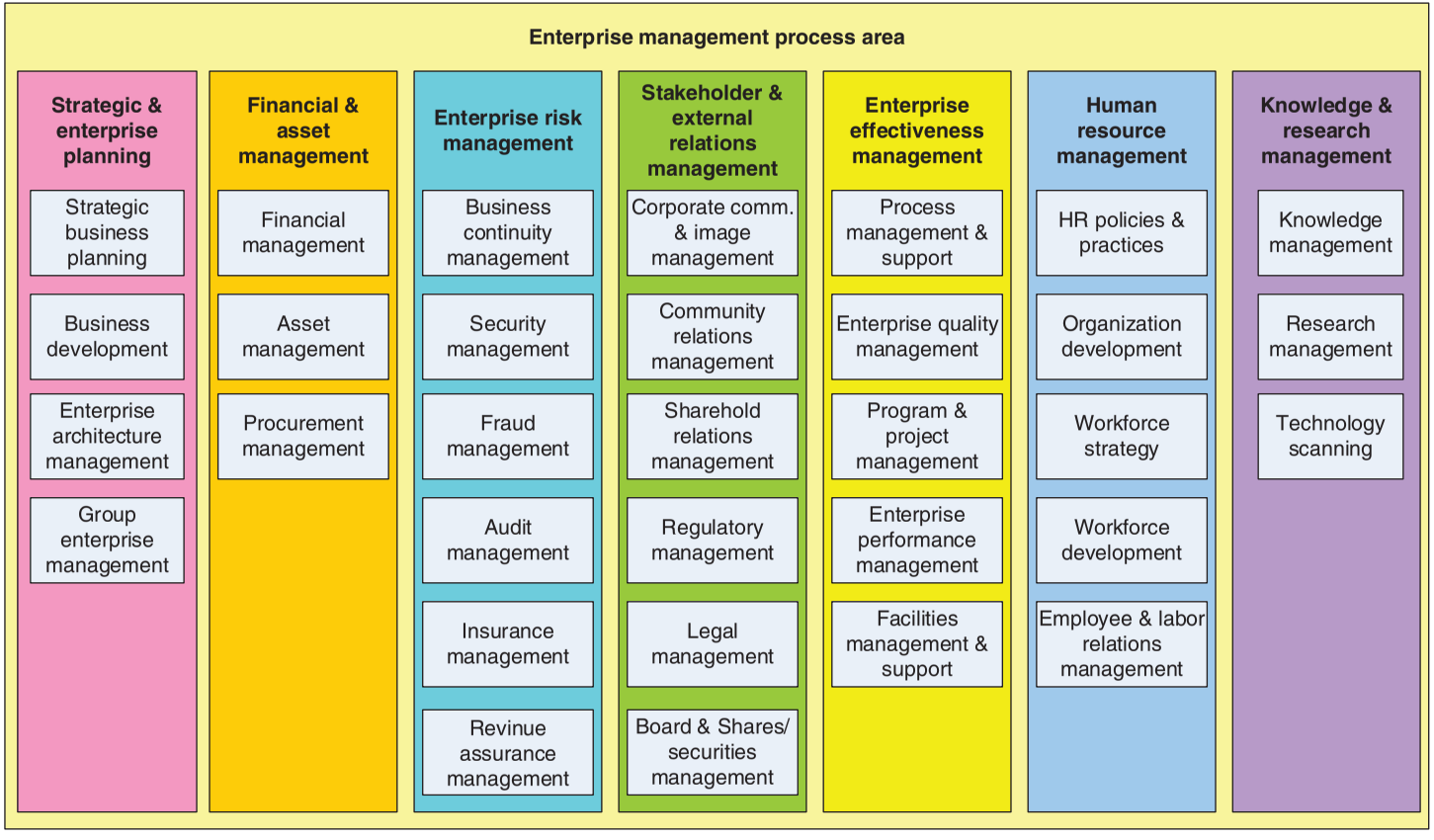

Figure 1.19. eTOM—Level 2 Enterprise Management Activity Areas.

- Survey & Analyze Service Problem (clause 1.1.2.3.7);
- Enterprise Risk Management (clause 1.3.2); and
- Stakeholder & External Relations Management (clause 1.3.6).

The following 39 (out of 212) eTOM Operations Support and Readiness, Fulfillment, Assurance, and Billing Area clauses are mapped to M.3400 Security Management sub-clauses which do not necessarily address the specifics of the M.3050-2 processes:

- Customer Relationship Management (clause 1.1.1);
- Order Handling (clause 1.1.1.5);
- Authorize Credit (clause 1.1.1.5.2);
- Complete Customer Order (clause 1.1.1.5.5);
- Issue Customer Orders (clause 1.1.1.5.6);
- Problem Handling (clause 1.1.1.6);
- Establish & Terminate Customer Relationship (clause 1.1.1.9.1);
- Analyze & Manage Customer Risk (clause 1.1.1.9.3);
- Service Management & Operation (SM&O) (clause 1.1.2);
- SM&O Support & Readiness (clause 1.1.2.1);
- Manage Service Inventory (clause 1.1.2.1.1);
- Enable Service Configuration & Activation (clause 1.1.2.1.2);
- Support Service Problem Management (clause 1.1.2.1.3);
- Enable Service Quality Management (clause 1.1.2.1.4);
- Service Configuration & Activation (clause 1.1.2.2);
- Design Solution (clause 1.1.2.2.1);
- Track & Manage Service Provisioning (clause 1.1.2.2.3);
- Implement, Configure, & Activate Service (clause 1.1.2.2.4);
- Issue Service Orders (clause 1.1.2.2.7);
- Service Problem Management (clause 1.1.2.3);
- Create Service Trouble Report (clause 1.1.2.3.1);
- Diagnose Service Problem (clause 1.1.2.3.2);
- Correct & Resolve Service Problem (clause 1.1.2.3.3);
- Track & Manage Service Problem (clause 1.1.2.3.4);
- Report Service Problem (clause 1.1.2.3.5);
- Close Service Problem Report (clause 1.1.2.3.6);
- Survey & Analyze Service Problem (clause 1.1.2.3.7);
- Service & Specific Instance Rating (clause 1.1.2.5);
- Analyze Usage Records (clause 1.1.2.5.3);
- Enable Resource Performance Management (clause 1.1.3.1.2);
- Enable Resource Data Collection & Processing (clause 1.1.3.1.4);

- Configure & Activate Resource (clause 1.1.3.2.2);
- Collect, Update & Report Resource Configuration Data (clause 1.1.3.2.4);
- Resource Data Collection & Processing (clause 1.1.3.5);
- Collect Resource Data (clause 1.1.3.5.1);
- Report Resource Data (clause 1.1.3.5.3);
- Audit Resource Usage Data (clause 1.1.3.5.4); and
- S/P Interface Management (clause 1.1.4.6).

The following 2 (out of 128) eTOM SIP Process Area clauses are mapped to M.3400 Security Management sub-clauses which do not necessarily address the specific details that the M.3050-2 processes would need:

- Resource Development & Management (clause 1.2.3), and
- Resource Strategy & Planning (clause 1.2.3.1).

The coverage of modern security management in the M.3400 and M.3050 documents is further compounded by M.3400[42] being predominantly operational in nature and does not provide much guidance for many of the processes discussed in eTOM. Given the deficiencies in M.3050 and M.3400, we will develop the details for security management in modern networking environments in Chapter 3. This development will consider not just ISO 27001 and 27002 but will also discuss Information Technology Infrastructure Library (ITIL), a set of concepts and practices for IT services management, and Control Objectives for Information and related Technology (COBIT), a set of best practices (framework) for IT management concepts for security management, and also consider concepts from ITU-T M.3401 and other documents.

1.5 HOW THE NEED FOR INFORMATION SECURITY HAS CHANGED

How has the need for security progressed over the last 10 years? One indication of the change in the security of networked systems can be seen by the statistics[43] developed by the CERT within the Software Engineering Institute at Carnegie Mellon University (shown in Table 1.7 of cataloged vulnerabilities in various systems). Although the table only covers up to October 2008, one can reasonably presume that not only will the number of vulnerabilities in 2008 exceed those cataloged in 2007 but the frequency of vulnerabilities in future years will be similar if not greater than those shown (note that more current data are discussed later). Many security events/attacks leverage system vulnerabilities; therefore, the magnitude of vulnerabilities is related to the frequency of security events.

[42] ITU-T M.3400, "SERIES M: TMN AND NETWORK MAINTENANCE: INTERNATIONAL TRANSMISSION SYSTEMS, TELEPHONE CIRCUITS, TELEGRAPHY, FACSIMILE AND LEASED CIRCUITS: Telecommunications Management Network: TMN management functions", INTERNATIONAL TELECOMMUNICATION UNION TELECOMMUNICATION STANDARDIZATION SECTOR, 02/2000

[43] CERT Statistics (n.d.). Retrieved October 11, 2011, from: http://www.cert.org/stats/

TABLE 1.7. CERT Cataloged Vulnerabilities.

Year	Total Vulnerabilities Cataloged	From Direct Reports
Q1–Q3, 2008	6058	310
2007	7236	357
2006	8064	345
2005	5990	213
2004	3780	170
2003	3784	191
2002	4129	343
2001	2437	153
2000	1090	—
1999	417	—
1998	262	—
1997	311	—
1996	345	—
1995	171	—
Total	44,074	

From http://www.cert.org/stats/

Notes: Year—This column represents the calendar year, not fiscal year.
Total Vulnerabilities Cataloged—This column reflects the total number of vulnerabilities that we have cataloged based on reports from public sources and those submitted to us directly. Storing the information in our database allows our analysts to systematically record vulnerability data; helps provide insight into significant preconditions, impacts, and scope; and gives us a way to validate reports and recognize new classes of vulnerabilities.

From Direct Reports—This column reflects the total number of vulnerabilities we have cataloged based on vulnerabilities reported directly to us. We encourage people to report vulnerabilities so we can coordinate with affected vendors to resolve vulnerabilities while minimizing the risk to all stakeholders. To determine an approximate number of vulnerabilities from public sources, subtract the number of direct reports from the total vulnerabilities cataloged. The actual number may differ slightly because, occasionally, vulnerabilities are reported directly to us and disclosed to the public at the same time.

Another source of information regarding the evolving need to security can be found in print/online media reports of security incidents between June 2008 and February 2011. One growing area is the concern over privacy which has mushroomed over the last decade with the rapid deployment of "high-speed" worldwide communications capabilities and now ubiquitous information services available to billions of individuals and organizations. In 2010 alone, there were over 4600 articles published in the popular and trade press (including online and print sources) reporting on privacy issues and privacy-related activities. Societies across the world have adopted many forms of IT and reliance on such technology. Another perspective is provided by William Norton (2011) where he cited the 2010 Security Report from Verizon Business that presented a couple of findings including:

- an increasing number of breaches originated from internal sources—mostly lower-level employees of the breached organizations with deliberate and malicious intentions, and

- confirmation that the largest number of compromised data records still result from outsider attacks.

The 2010 study, conducted in association with the U.S. Secret Service, analyzed 900 breaches and over 900 million compromised records. Norton went on to note that "Verizon found that of all organizations whose financial information had been breached, more than three-quarters had failed to comply with PCI DSS standards."

A small sample of other SP-related security issues reported upon includes the following:

- A blog by Dave Jevans discussed a data breach in April 2011 at the email service provider (ESP) Epsilon which revealed the names and email addresses of tens of millions of customers of banks and e-commerce companies, including CitiBank, Chase, Wal-Mart, U.S. Bank, Capital One, Ameriprise, Target, Kroger, TiVo, HSN, Disney, Walgreens, Best Buy, and many others. Jevans also noted that he has heard from industry sources that this was not the first major break-in to an ESP in 2011.
- Andrei Patrick (2011) discussed a massive distributed denial-of-service (DDoS) attack in 2010 brought down the voice-over-IP (VoIP) call processing supplied by TelePacific Communications and cost the VoIP provider hundreds of thousands of dollars. In the same article, Patrick noted the statements of a number of panelists/presenters at the 2011 Comptel Plus Conference:
  - "The pace of many types of DDoS attacks appears to be increasing," and "to this day, TelePacific is still fighting against denial-of-service attacks, which traffic comes from China and Africa" according to Don Poe, vice president of TelePacific Communications' network engineering.
  - The competitive communications services provider industry trade group Comptel said "it does believe its membership is seeing growth in DDoS attacks."
  - "Many cases of network attacks which the FBI works on do appear to involve a financial motive," according to Stacy Arruda, a supervisory FBI special agent of the Cybercrime division.
  - "Service providers need to remember that they are a target and they need to have a plan in place for this kind of problem," noted Patrick Gray, principal security strategist at Cisco Systems.
  - "DDoS attacks and SYN floods are extraordinarily common nowadays," said Stacy Griggs, senior director at Cbeyond Cloud Services.
- Ellen Messmer (2011), also covering the Comptel Plus Conference, noted that Don Poe stated "TelePacific sees a multitude of daily scans against its network, and low-level attacks can occur about twice a day."
- An article by securitywatch.eweek.com discussed Arbor Networks fifth annual Worldwide Infrastructure Security Report. The report included responses from 132 IP network operators from North America, South America, Europe, Africa, and Asia and reported that:

- The size of DDoS attacks hitting SP infrastructures did not increase as much between third quarter of 2008 and the third quarter of 2009 as it had in previous years.
- The size of the attacks still went up by more than 20%.
- SPs had reported in the past that peak DDoS attack rates were nearly doubling year over year.
- In 2010, the largest sustained attack rate was 49 Gbps (gigabit per second), a 22% increase over last year's peak of a 40 Gbps attack.
- The 2009 largest sustained attack rate represented a 67% increase over the largest attack reported in the 2007 survey.
- The Arbor Networks report went on to say that non-technical factors such as poorly defined operational policies and responsibilities are hurting efforts to strengthen security while "The complexity introduced by the continuing convergence of critical services onto IP networks and multi-tenant cloud-based solutions significantly increases the exposed risk profile of infrastructure and customer-visible services."

- A recent *New York Times* article by Riva Richmond (2011) focused on how digital certificates were fraudulently issued by the Comodo Group, an Internet security company. In the attack at Comodo, it was reported that the hackers were able to infiltrate an Italian computer reseller and use the reseller's access to Comodo's systems to automatically create certificates for websites operated by Google, Yahoo, Microsoft, Skype, and Mozilla. With the certificates, the attacker could then set up servers that appear to work for those sites. Quoting the article, "many security experts say the problems start with the proliferation of organizations permitted to issue certificates. Browser makers like Microsoft, Mozilla, Google and Apple have authorized a large and growing number of entities around the world—both private companies and government bodies—to create them. Many private 'certificate authorities' have, in turn, worked with resellers and deputized other unknown companies to issue certificates in a 'chain of trust' that now involves many hundreds of players, any of which may in fact be a weak link." This type of attack was targeting a foundation technology used by virtually all types of organizations with an Internet presence, not just SPs, and thusly could serve as a "stepping stone" to future attacks specifically targeting SP infrastructures.
- A more direct (i.e., physical) attack in April 2010 was discussed by Bruce Perens (2011) about how unidentified attackers cut eight fiber cables which caused the city of Morgan Hill and parts of three counties to lose 911 service, cellular mobile telephone communications, landline telephone, DSL Internet and private networks, central station fire and burglar alarms, ATMs, credit card terminals, and monitoring of critical utilities. The objective of the perpetrators was not known; yet this act demonstrated how metropolitan communications can be disrupted in the absence of physical monitoring of manhole-located communications links. Also noted in the report was the point that "networks, even those of emergency

services providers, are rarely tested for operation while disconnected from the outside world. Many such networks depend on outside services to match host names to network addresses, and thus stop operating the moment they are disconnected from the internet." SP communications cables have been cut by accident over the years; yet this incident was intentional and raises concern over the need for security monitoring access to SP outside plant whether underground or on poles/towers.

The continuing growth of concern over how secure SP infrastructures are has led to the U.S. Federal Communications Commission (FCC) launching an inquiry seeking public comments regarding a proposed Cyber Security Certification Program for communications SPs in 2010. The proposed voluntary certification program would use either private sector auditors or the FCC to conduct security assessments of participating communications SPs' networks, including their compliance with stringent cyber security practices. SPs, whose networks successfully completed this assessment, would then be able to claim their networks complied with these FCC network security requirements. As noted, the aforementioned reports/articles represent just a small sampling of the extended discussion regarding SP security issues; a short amount of time spent searching the "web" can quickly find many more such posts and reports.

1.6 SUMMARY

In this chapter, we started with a review of how information security, and its management, were first defined and specified in a standardized manner. An overview was presented on how networks have been designed and developed over the last 30 years and the different standards used to define security within these networks. As noted, networks have evolved over time and now are significantly more complex than the base standards ever anticipated. Focus was then directed at the management of networks, especially security. Again the baseline standards failed to address management and security in a comprehensive manner, although important concepts were introduced, namely, FCAPS, technology-independent security services, and the need for both specific and pervasive security mechanisms. Then the most current standards for network management were reviewed for their treatment of security management and deficiencies noted.

Chapter 2 presents a review of the technologies used for constructing modern communications networks. Also considered is how NGNs and associated services are being defined and specified. This review is provided to further emphasize the growing need for a holistic approach toward managing security within, not just network infrastructures, but integrating security management into, and within, general organizational management activities and plans. Starting with Chapter 3, we discuss what efforts have been made to standardize an organizational approach for security management with a review of the four main methodologies in use currently.

FURTHER READING AND RESOURCES

FCC (2010) Notice of Inquiry for Public Comments On Proposed Cyber Security Certification Program For Communications Service Providers, Docket No. 10–93. Retrieved October 10, 2011, from http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-10-63A1.pdf

Jevans, D. (2011) Privacy and Identity Theft. Retrieved October 10, 2011, from http://blog.ironkey.com/?p=1250

Kaufman, C., Perlman, R., Speciner, M. (2002) *Network Security—Private Communication in a Public World*. 2nd ed. Prentice-Hall

Messmer, E. (2011) Massive DDoS attacks threaten VoIP services, Network World Creator. Retrieved October 10, 2011, from http://www.itworldcanada.com/news/massive-ddos-attacks-threaten-voip-services/144077

Norton, W.K. (2011) 2010 Security Report from Verizon Reveals New Patterns of Cybercrime (n.d.). Baker, Donelson, Bearman, Caldwell and Berkowitz, P.C. Retrieved October 11, 2011, from http://www.bakerdonelson.com/2010-security-report-from-verizon-reveals-new-patterns-of-cybercrime-04–13–2011/

Patrick, A. (2011) Massive DDoS attacks a growing problem to VoIP providers. Retrieved October 10, 2011, from http://www.iptelephony.org/article/massive-ddos-attacks-growing-problem-voip-providers

Perens, B. (2011) A Cyber-Attack on an American City. Retrieved October 11, 2011, from http://perens.com/works/articles/MorganHill/

Richmond, R. (2011) Attack on Comodo Sheds Light on Internet Security Holes—NYTimes.com. Retrieved October 11, 2011, from http://www.nytimes.com/2011/04/07/technology/07hack.html

securitywatch.eweek.com (2010) Service Providers Face Security Challenges. Retrieved October 11, 2011, from http://securitywatch.eweek.com/ddos/service_providers_face_security_challenges.html