ATIS-1000007.2006

GENERIC SIGNALING AND CONTROL PLANE SECURITY REQUIREMENTS FOR EVOLVING NETWORKS

AMERICAN NATIONAL STANDARD FOR TELECOMMUNICATIONS

The Alliance for Telecommunication Industry Solutions (ATIS) is a technical planning and standards development organization that is committed to rapidly developing and promoting technical and operations standards for the communications and related information technologies industry worldwide using a pragmatic, flexible and open approach. Over 1,100 participants from more than 350 communications companies are active in ATIS' 23 industry committees and its Incubator Solutions Program.

< http://www.atis.org/ >

AMERICAN NATIONAL STANDARD

Approval of an American National Standard requires review by ANSI that the requirements for due process, consensus, and other criteria for approval have been met by the standards developer.

Consensus is established when, in the judgment of the ANSI Board of Standards Review, substantial agreement has been reached by directly and materially affected interests. Substantial agreement means much more than a simple majority, but not necessarily unanimity. Consensus requires that all views and objections be considered, and that a concerted effort be made towards their resolution.

The use of American National Standards is completely voluntary; their existence does not in any respect preclude anyone, whether he has approved the standards or not, from manufacturing, marketing, purchasing, or using products, processes, or procedures not conforming to the standards.

The American National Standards Institute does not develop standards and will in no circumstances give an interpretation of any American National Standard. Moreover, no person shall have the right or authority to issue an interpretation of an American National Standard in the name of the American National Standards Institute. Requests for interpretations should be addressed to the secretariat or sponsor whose name appears on the title page of this standard.

CAUTION NOTICE: This American National Standard may be revised or withdrawn at any time. The procedures of the American National Standards Institute require that action be taken periodically to reaffirm, revise, or withdraw this standard. Purchasers of American National Standards may receive current information on all standards by calling or writing the American National Standards Institute.

NOTE - The user's attention is called to the possibility that compliance with this standard may require use of an invention covered by patent rights. By publication of this standard, no position is taken with respect to whether use of an invention covered by patent rights will be required, and if any such use is required no position is taken regarding the validity of this claim or any patent rights in connection therewith.

ATIS-1000007.2006, *Generic Signaling and Control Plane Security Requirements for Evolving Networks*

Is an American National Standard developed by the **Security (SEC)** Subcommittee under the **ATIS Packet Technologies and Systems Committee (PTSC)**.

Published by

Alliance for Telecommunications Industry Solutions
1200 G Street, NW, Suite 500
Washington, DC 20005

ATIS-1000007.2006

American National Standard for Telecommunications

GENERIC SIGNALING AND CONTROL PLANE SECURITY REQUIREMENTS FOR EVOLVING NETWORKS

Secretariat

Alliance for Telecommunications Industry Solutions

Approved April 6, 2006

American National Standards Institute, Inc.

Abstract

Many security threats exist to the signaling and control plane of a telecommunications network. In addition, new security threats to the signaling and control plane are being introduced as the network evolves. The purpose of this document is to provide generic signaling and control plane security requirements and a general security framework to mitigate security risks in the evolving telecommunications networks.

FOREWORD

The information contained in this Foreword is not part of this American National Standard (ANS) and has not been processed in accordance with ANSI's requirements for an ANS. As such, this Foreword may contain material that has not been subjected to public review or a consensus process. In addition, it does not contain requirements necessary for conformance to the Standard.

The Alliance for Telecommunication Industry Solutions (ATIS) serves the public through improved understanding between carriers, customers, and manufacturers. The Packet Technologies and Systems Committee (PTSC) -- formerly T1S1 -- develops and recommends standards and technical reports related to services, architectures, and signaling, in addition to related subjects under consideration in other North American and international standards bodies. PTSC coordinates and develops standards and technical reports relevant to telecommunications networks in the U.S., reviews and prepares contributions on such matters for submission to U.S. ITU-T and U.S. ITU-R Study Groups or other standards organizations, and reviews for acceptability or per contra the positions of other countries in related standards development and takes or recommends appropriate actions.

ANSI guidelines specify two categories of requirements: mandatory and recommendation. The mandatory requirements are designated by the word *shall* and recommendations by the word *should*. Where both a mandatory requirement and a recommendation are specified for the same criterion, the recommendation represents a goal currently identifiable as having distinct compatibility or performance advantages.

This document provides generic signaling and control plane security requirements for evolving networks. This document is part of a suite of signaling and control security standards as shown in Figure #1 below. As the primary requirements document in this suite of standards, it provides a general security framework and overall security requirements which are used by the other detailed security standards.

This standard is in alignment with ITU-T Recommendation X.805 [ITU X.805].

Suggestions for improvement of this document are welcome. They should be sent to the Alliance for Telecommunications Industry Solutions, PTSC Secretariat, 1200 G Street NW, Suite 500, Washington, DC 20005.

At the time it approved this document, PTSC, which is responsible for the development of this Standard, had the following members:

R. Hall, PTSC Chair
J. Zebarth, PTSC Vice-Chair
S. Carioti, ATIS Disciplines
S. Barclay, ATIS Secretariat
C. Underkoffler, ATIS Chief Editor
M. Lee, PTSC Technical Editor

Organization Represented	Name of Representative
AcmePacket	Kevin Klett
Alcatel USA Inc.	Ken Biholar
AT&T	Martin Dolly George Stanek (Alt.)
BellSouth Telecommunications	David M. Brady
C.S.I Telecommunications	Michael S. Newman Thomas G. Croda (Alt.)
Cingular Wireless LLC	Don Zelmer Marc Grant (Alt.)
Cisco Systems	Rajiv Kapoor Chip Sharp (Alt.)
Defense Info. Systems Agency	Chris Fitzgerald Ryan Kuseski (Alt.)
Ericsson Incorporated	Susana Sabater-Maroto Stephen Hayes (Alt.)
FBI ESTS	Gregory Milonovich Eric Mason (Alt.)

Organization Represented	Name of Representative
Harris Corporation	Marlis Humphrey
Hewlett-Packard	Steve Mills
Intelsat	Mark T. Neibert
Juniper Networks	Rao Cherukuri Kireeti Kompella (Alt.)
Lucent Technologies	Stuart O. Goldman
MCI	J. Martin Carroll Robert Schafer (Alt.)
National Communications System	Nicholas Andre Jean Trakinat (Alt.)
Nokia Telecommunications	Joyabrata Mukherjee Ed Ehrlich (Alt.)
Nortel Networks	Joseph A. Zebarth
Qwest	Steve Showell Michael Fargano (Alt.)
SBC Communications, Inc.	B.S. Sambasivan Bob Hall (Alt.)

Organization Represented	Name of Representative
Siemens Info & Comm Ntwks, Inc.	Ron Franks David E. Francisco (Alt.)
Sprint Corporation	Mark L. Jones
Telcordia Technologies	Wesley Downum Cliff Halevi (Alt.)
Tellabs Operations, Inc.	William A. Walker
Tridea Works	Greg Ratta
Verizon Communications	Dave Morris Wendy Pugh (Alt.)

The Security (SEC) Subcommittee was responsible for the development of this document.

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

American National Standard for Telecommunications –

Generic Signaling and Control Plane Security Requirements for Evolving Networks

1 INTRODUCTION, SCOPE, PURPOSE, & APPLICATION

1.1 Introduction

Many security threats exist to the signaling and control plane of a telecommunications network. In addition, new security threats to the signaling and control plane are being introduced as the network evolves. The purpose of this document is to provide generic signaling and control plane security requirements and a general security framework to mitigate security risks in the evolving telecommunications networks.

In some telecommunications networks, signaling and control traffic is transmitted on a separate network from that carrying the service provider's end-user traffic. In these networks, security threats to the signaling and control plane are isolated from any malicious activity on the end-user plane. However, in an increasing number of evolving telecommunications networks, signaling and control traffic is combined on a single transport network with end-user traffic. Combining traffic in this manner minimizes costs by requiring only a single integrated network infrastructure -- but new security challenges are introduced. Threats in the end-user plane now become threats to the signaling and control plane, since the signaling and control plane becomes accessible to the multitude of end-users.

1.2 Scope

This document addresses generic signaling and control plane security aspects of evolving telecommunications networks. Evolving telecommunications networks often combine legacy telecommunication facilities with new technologies such as Wireless, ATM, and Internet Protocol transport mechanisms. The security recommendations given in this document apply to service provider networks and may also be applicable to individual company corporate enterprise networks.

This document is based on Recommendation X.800, *Security Architecture for Open Systems Interconnection for CCITT Applications*, and Recommendation X.805, *Security Architecture for Systems Providing End-to-End Communications*. {Reference [ITU X.800], [ITU X.805]}

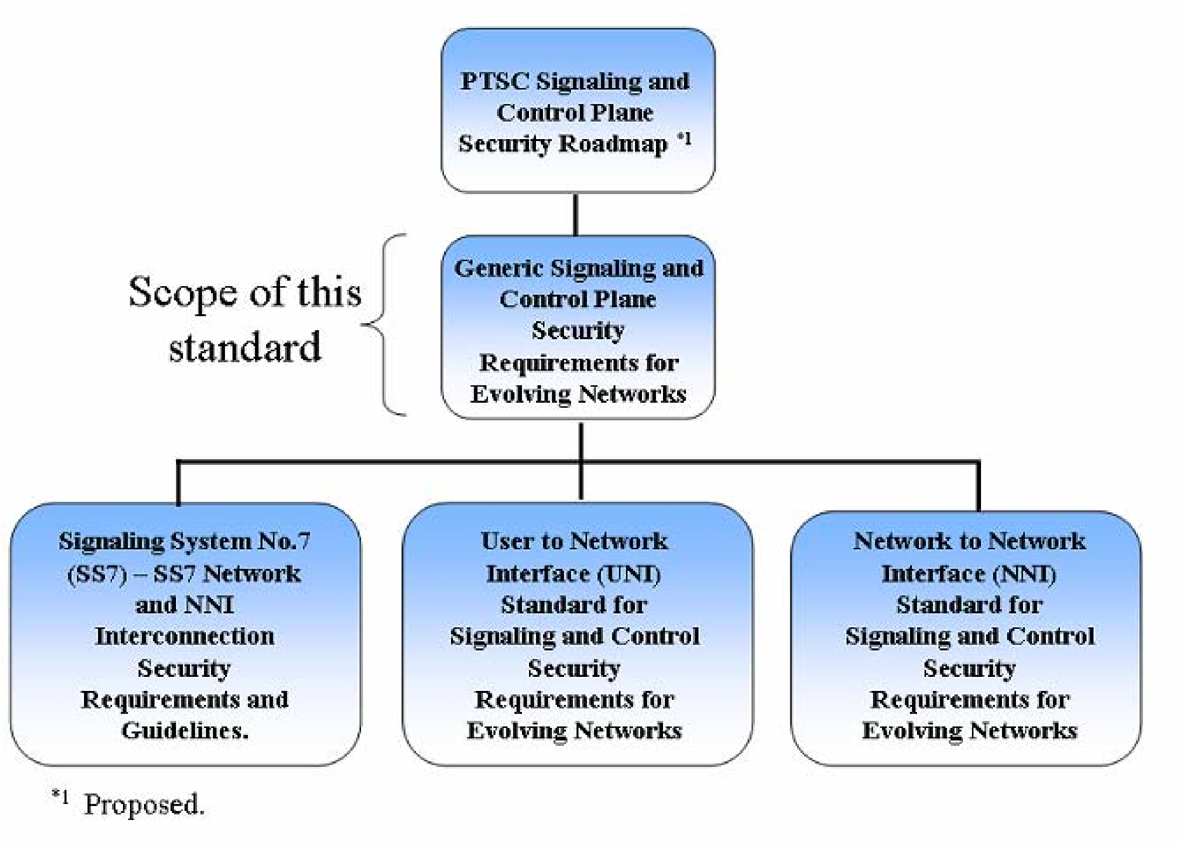
PTSC Signaling and Control Plane Security Roadmap *1
Scope of this standard
Generic Signaling and Control Plane Security Requirements for Evolving Networks
Signaling System No.7 (SS7) – SS7 Network and NNI Interconnection Security Requirements and Guidelines.
User to Network Interface (UNI) Standard for Signaling and Control Security Requirements for Evolving Networks
Network to Network Interface (NNI) Standard for Signaling and Control Security Requirements for Evolving Networks
*1 Proposed.

Figure 1 - Signaling and Control Plane Security Documents

1.3 Purpose

This document provides generic signaling and control plane security requirements and a general security framework for evolving telecommunications networks. The concepts presented in this document are intended for use by other related documents which deal with specific signaling and control security areas such as SS7 and VoP/Multimedia security.

The purpose of the family of documents identified in the Foreword is to specify security requirements for signaling and control plane functions of evolving telecommunications networks. These requirements will help assure secure interoperability of equipment from multiple vendors.

1.4 Related Documents

The related signaling and control plane security standards are shown in the Foreword.

2 Normative References

[RFC2401]	IETF RFC 2401, *Security Architecture for the Internet Protocol,* November 1998, S. Kent, R. Atkinson; http://www.ietf.org/rfc/rfc2401.txt?number=2401
[RFC 2406]	IETF RFC 2406, *IP Encapsulating Security Payload (ESP),* http://www.ietf.org/rfc/rfc2406.txt?number=2406
[RFC 2410]	IETF RFC 2410, *The Null Encryption Algorithm and Its Use with IPsec,* http://www.ietf.org/rfc/rfc2410.txt?number=2410
[RFC 2451]	IETF RFC 2451, *The ESP CBC-Mode Cipher Algorithms,* http://www.ietf.org/rfc/rfc2451.txt
[RFC 3602]	IETF RFC 3602, *The AES-CBC Cipher Algorithm and Its Use with IPsec,* http://www.ietf.org/internet-drafts/draft-ietf-ipsec-ciph-aes-cbc-04.txt
[RFC 2404]	IETF RFC 2404, *The Use of HMAC-SHA-1-96 within ESP and AH,* http://www.ietf.org/rfc/rfc2404.txt?number=2404
[RFC 3566]	IETF RFC 3566, *The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec,* http://www.ietf.org/rfc/rfc3566.txt?number=3566
[RFC 2409]	IETF RFC 2409, *Internet Key Exchange,* http://www.ietf.org/rfc/rfc2409.txt?number=2409
[RFC 3526]	IETF RFC 3526, *More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE).* http://www.ietf.org/rfc/rfc2409.txt?number=2409
[RFC 2246]	IETF RFC 2246, *The TLS Protocol, Version 1.0,* ftp://ftp.rfc-editor.org/in-notes/rfc2246.txt
[RFC 3268]	IETF RFC 3268, *Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)* http://www.ietf.org/rfc/rfc3268.txt?number=3268
[RFC 3546]	IETF RFC 3546, *Transport Layer Security (TLS) Extensions,* ftp://ftp.rfc-editor.org/in-notes/rfc3546.txt
[3DES]	Federal Information Processing Standards (FIPS) Publication 46-3, *Data Encryption Standard*, National Institute of Standards and Technology, October 1999. http://csrc.nist.gov/publications/fips/ fips46-3/fips46-3.pdf
[FIPS-197]	FIPS Publication 197, *Advanced Encryption Standard (AES)*, National Institute of Standards and Technology, November 2001. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
[FIPS-180-2]	FIPS Publication 180-2, *Secure Hash Standard*, National Institute of Standards and Technology. http://csrc.nist.gov/publications/fips/fips180-2/fips180-2withchangenotice.pdf
[RFC 1321]	IETF RFC 1321, *The MD5 Message-Digest Algorithm,* http://www.ietf.org/rfc/rfc2409.txt?number=2409
[ITU X.800]	ITU-T Recommendation X.800, *Security architecture for Open Systems Interconnection for CCITT applications.*
[ITU X.805]	ITU-T Recommendation X.805, *Security architecture for systems providing end-to-end communications.*

3 Definitions

The following definitions apply:

3.1 Access Control - The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner.

3.2 Access Control List - A list of entities, together with their access rights, which are authorized to have access to a resource.

3.3 Access Control Policy - The set of rules that define the conditions under which access to a particular resource may take place.

3.4 Asymmetric Cryptographic Algorithm - An algorithm for performing encryption or the corresponding decryption where the keys used for encryption and decryption differ.

3.5 Authentication - The process of verifying the claimed identity of an entity to another entity or corroboration that the source of data received is as claimed.

NOTE - The authenticated entity may belong either to the Application Security Layer or to the Network Services Security Layer of the Security Architectural Model. In general cases, authentication at one layer does not follow from authentication at the other layer. Authentication spans peer entity and data origin authentication where only data origin authentication provides an integrity mechanism.

3.6 Authorization - The act of giving access rights to a service, device, or resource by an entity with authority to grant this permission.

3.7 Availability - The property of being accessible and useable upon demand by an authorized entity.

3.8 Certificate - A set of security-relevant data issued by a security authority or trusted third party, together with security information which is used to provide the integrity and data origin authentication services for the data. The security information includes subject attributes and an indication of a time period of validity.

3.9 Communication party - The participator or process communicating with another counterpart(s) at the Application Security Layer of the Security Architectural Model by means of application layer protocols using the network element platform.

3.10 Confidentiality - The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

3.11 Cryptographic Algorithm - A mathematical function that is used in cryptography.

3.12 Cryptography - The discipline which embodies principles, means, and methods for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorized use.

NOTE - Cryptography determines the methods used in encipherment and decipherment. An attack on a cryptographic principle, means, or methods is *cryptanalysis*. [ITU X.800]

3.13 Data Integrity - The property that data has not been altered or destroyed in an unauthorized manner.

3.14 Denial of Service (DoS) [attack] - Action that prevents authorized access to resources or that delays time-critical operations.

3.15 Digital Signature - Data appended to, or a cryptographic transformation (see *cryptography*) of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery -- e.g., by the recipient.

3.16 Hash Function - A one way mathematical function which maps values from a large (possibly very large) domain into a smaller range.

NOTE - A “good” hash function has the following properties:

- ♦ It is computationally hard, based on the given hash output, to find at least one input that results in the given output.
- ♦ It is computationally hard, based on the given hash input and output, to find yet another different input that results in the given output.
- ♦ It is computationally hard to find two different inputs that result in the same hash output.

3.17 Hashed Message Authentication Code (HMAC) - The result of a hash function, as per RFC 2104, that uses a secret key and provides data integrity and data origin authentication for data and messages.

3.18 Key - A sequence of symbols that controls the operations of encipherment and decipherment.

3.19 Key Management - The generation, storage, distribution, deletion, and archiving of keys in accordance with a security policy.

3.20 Mutual Authentication - A category of authentication whereby each party authenticates itself to other parties.

3.21 Non-repudiation - Protection from denial by one of the entities involved in a communication of having participated in all or part of the communication.

3.22 Password - Confidential authentication information, usually composed of a string of characters.

3.23 Privacy - The right of individuals to control or influence what information related to them may be collected and stored, and by whom and to whom that information may be disclosed.

NOTE - Because this term relates to the right of individuals, it cannot be very precise and its use should be avoided except as a motivation for requiring security.

3.24 Proxy - An intermediary entity that acts as both a server and a client for the purpose of making requests on behalf of other clients.

3.25 Repudiation - Denial by one of the entities involved in a communication of having participated in all or part of the communication.

3.26 Secret Key - A key that is used in a symmetric cryptographic algorithm.

NOTE - Possession of a secret key is restricted (usually to two entities).

3.27 Security - The process of minimizing the vulnerabilities of assets and resources, or the result of this process.

NOTE - An asset is anything of value. A vulnerability is any weakness that could be exploited to violate a system or the information it contains. A threat is a potential violation of security.

3.28 Security Administrator - An authority (a person or a group of people) responsible for enforcing the security policy for a security domain.

3.29 Transport Mode – A mode of operation of the IPsec protocol whereby the data packet IP header is used for routing.

3.30 Tunnel Mode - A mode of operation of the IPsec protocol whereby a new IP header is added to an original data packet and this new IP header is used for routing.

3.31 X.509 Certificate - A public key certificate specification developed as part of the ITU-T X.500 series.

4 ABBREVIATIONS & ACRONYMS

This standard uses the following abbreviations:

3DES	Triple DES
AAA	Authentication, Authorization and Accounting
AES	Advanced Encryption Algorithm
ASP	Application Service Provider
ATM	Asynchronous Transfer Mode
BICC	Bearer Independent Call Control
CBC	Cipher Block Chaining
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service
DoS	Denial of Service
DSA	Digital Signature Algorithm

ECC	Elliptic Curve Cryptography
FTP	File Transfer Protocol
HMAC	Hashed Message Authentication Code
IDS	Intrusion Detection System
IKE	Internet Key Exchange
ISDN	Integrated Services Digital Network
ISUP	Integrated Services Digital Network (ISDN) User Part
IP	Internet Protocol
IPsec	IP Security Protocol Suite
MD5	Message Digest 5
MPLS	Multi Protocol Label Switching
MTP	Message Transfer Part
NNI	Network to Network Interface
OAM&P	Operations, Administration, Maintenance & Provisioning
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
PSTN	Public Switched Telephone Network
PVC	Permanent Virtual Circuit
QoS	Quality of Service
RSA	Rivest, Shamir, Adleman
SAAL	Signaling ATM Adaptation Layer
SCCP	Signaling Connection Control Part
SCTP	Stream Control Transmission Protocol
SHA	Secure Hash Algorithm
SIP	Session Initiation Protocol
SIGTRAN	Signaling Transport
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SONET	Synchronous Optical Network
STP	Signaling Transfer Point
TCAP	Transaction Capabilities Application Protocol
SS7	Signaling System No. 7
SSL	Secure Socket Layer
TDM	Time Division Multiplexing
TDEA	Triple Data Encryption Algorithm (See 3DES)
TLS	Transport Layer Security
UNI	User to Network Interface
VoIP	Voice over IP

5 Security Architecture & Methodology

5.1 General Architecture Model

The Security Architecture defined in this ANSI standard is based on the model given in ITU-T Recommendation X.805. This Security Architecture provides a comprehensive, top-down, end-to-end perspective of network security and can be applied to network elements, services, and applications in order to detect, predict, and correct security vulnerabilities.

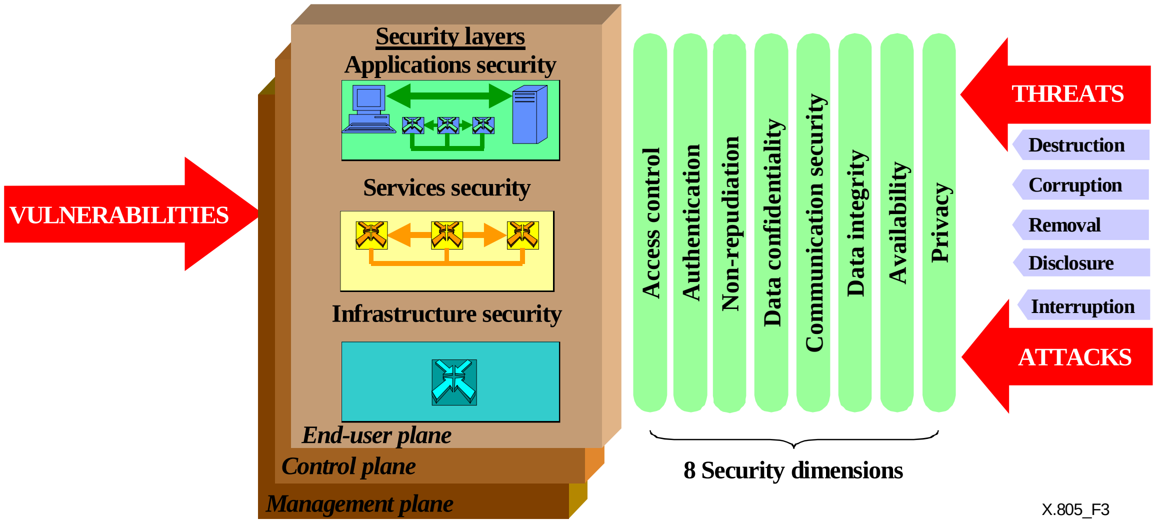

Figure 2 - Security Architecture Model

The Security Architectural Model is shown in Figure 2. It consists of three architectural components:

1. *Security Planes* (End User Plane, Signaling and Control Plane, and Management Plane).
2. *Security Layers* (Applications Security, Network Services Security and Infrastructure Security).
3. *Security Dimensions* (Access Control, Authentication, Non-repudiation, Data Confidentiality, Communication Security, Data Integrity, Availability and Privacy).

The Security Architecture logically divides a complex set of end-to-end network security-related features into separate architectural components. This separation allows for a systematic approach to end-to-end security that can be used for planning of new security solutions, as well as for assessing the security of the existing networks. The principles described by the Security Architecture can be applied to a wide variety of networks independently of the network's technology or location in the protocol stack to provide security solutions.

The architecture model makes provision for interaction between the Management Plane and the End User Plane and Control Plane. This interaction facilitates the exchange of management information, where required.

The following sections describe in detail the architectural elements and their functions with respect to the major security threats.

5.2 Security Planes

Recommendation X.805 defines three *Security Planes* to represent the three types of protected activities that take place on a network. The Security Planes are: (1) the *Management Plane*; (2) the *Signaling and Control Plane*; and (3) 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.

Networks should be designed in such a way that events on one Security Plane are kept totally isolated from the other Security Planes. The concept of Security Planes allows the differentiation of the specific security concerns associated with those activities and the ability to address them independently. Consider, for example, a VoIP Service, which is addressed by the Services Security layer. Securing the management of the VoIP service (e.g., provisioning users) has to be independent of securing the control of the service (e.g., protocols such as SIP) and also has to be independent of securing the end-user data being transported by the service (e.g., the user's voice).

This standard focuses only on security of the Signaling and Control Plane. Requirements for security of the Management Plane and End User Plane are not within the scope of this standard.

5.2.1 End-User Security Plane

The *End-User Security Plane* is concerned with security of the use of the Service Provider's network by customers. This plane also represents actual end-user data flows. End-users may use a network that only provides connectivity, they may use it for value-added services, or they may use it to access network-based applications.

5.2.2 Signaling and Control Security Plane

The *Signaling and Control Security Plane* is concerned with protection of the activities that enable the efficient delivery of information, services, and applications across the network. It typically involves machine-to-machine communications of information that allows the machines (e.g., switches or routers) to determine how to best route or switch traffic across the underlying transport network. This type of information is sometimes referred to as *control* or *signaling information*. The network carrying these types of messages may be in-band or out-of-band with respect to the Service Provider's user traffic. For example, IP networks carry their control information in-band; whereas, the PSTN carries its control information in a separate out-of-band signaling network (the SS7 network). Example traffic of this type could include routing protocols, DNS, SIP, SS7, Megaco/H.248, LDP, RSVP, CR-LDP, RSVP-TE, BGP, OSPF, ISIS, DCC, DHCP, and ICMP.

5.2.3 Management Plane Security

The *Management Security Plane* is concerned with the protection of OAM&P functions of the network elements, transmission facilities, back-office systems (Operations Support Systems, Business Support Systems, Customer Care Systems, etc.), and Data Centers. The Management Plane supports the Fault, Capacity, Administration, Provisioning, and Security (FCAPS) functions. It should be noted that the network carrying the traffic for these activities may be in-band or out-of-band with respect to the Service Provider's user traffic. (Refer to T1.276-2003, *Operations, Administration, Maintenance, and Provisioning Security Requirements for the Public Telecommunications Network: A Baseline Security Requirements for the Management Plane*, for Management Plane Security requirements. {Informative Reference [T1.276]}.)

5.3 Security Dimensions

A *Security Dimension* is a set of security measures designed to address a particular aspect of the network security. This standard identifies eight such sets that protect against major security threats. These dimensions are not limited to the network, but extend to applications and end user information as well. The Security Dimensions are:

1. Access Control
2. Authentication
3. Non-repudiation
4. Data Confidentiality
5. Communication Security
6. Data Integrity
7. Availability
8. Privacy

Properly designed and implemented Security Dimensions enforce a security policy that is defined for a particular network. The local security management function, interacting with a Security Management System, is responsible for controlling the mechanisms which instantiate the Security Dimension capabilities. Requirements for the local security management and control mechanism are outside the scope of this document.

Some of the specific services and mechanisms that support these dimensions are outside the scope of this document. For example, methods to perform disaster recovery and management of security services are not addressed.

5.3.1 Access Control Security Dimension

The *Access Control Security Dimension* protects against unauthorized use of network resources. Access Control ensures that only authorized personnel or devices are allowed access to network elements, stored information, information flows, services, and applications. In addition, *Role-Based Access Control* (*RBAC*) provides different access levels to guarantee that individuals and devices can only gain access to and perform operations on network elements, stored information, and information flows that they are authorized for.

5.3.2 Authentication Security Dimension

The *Authentication Security Dimension* serves to confirm the identities of communicating entities. Authentication ensures the validity of the claimed identities of the entities participating in communication (e.g., person, device, service, or application) and provides assurance that an entity is not attempting a masquerade or unauthorized replay of a previous communication.

5.3.3 Non-repudiation

The *Non-repudiation Security Dimension* provides means for preventing an individual or entity from denying having performed a particular action related to data by making available proof of various network-related actions (such as proof of obligation, intent, or commitment; proof of data origin, proof of ownership, proof of resource use). It ensures the availability of evidence that can be presented to a third party and used to prove that some kind of event or action has taken place.

> NOTE - Security audit logging functionality may be used to help address non-repudiation requirements. The purpose of security audit logs is to maintain an audit trail of activities generated by the devices and users. Audit logs are useful for reconstruction of past events and for proving accountability for actions taken.

5.3.4 Data Confidentiality Security Dimension

The *Data Confidentiality Security Dimension* ensures that data is protected against unauthorized viewing both in transit and in storage, and that data is not disclosed to unauthorized parties.

The application of data confidentiality mechanisms such as encryption, access control lists, and file permissions ensure that data content cannot be understood by unauthorized entities, and that information cannot be intercepted as it flows between authorized end points.

5.3.5 Communication Security Dimension

The *Communication Security Dimension* ensures that information flows only between the authorized end points (the information is not diverted or intercepted as it flows between these end points).

5.3.6 Data Integrity Security Dimension

The *Data Integrity Security Dimension* provides means to ensure the correctness or accuracy of data. The data is protected against unauthorized modification, deletion, creation, and replication. The dimension also provides an indication of these unauthorized activities.

5.3.7 Availability Security Dimension

The *Availability Security Dimension* ensures that there is no denial of authorized access to network elements, stored information, information flows, services, and applications due to events impacting the network. Disaster recovery solutions are included in this category.

5.3.8 Privacy Security Dimension

The *Privacy Security Dimension* provides mechanisms to ensure protection of certain sensitive information, mostly at the application layer, that might be derived from the observation of network activities. Examples of such sensitive information include web-sites that a user has visited, a user's geographic location, calling/called telephone numbers, and DNS names of devices in a Service Provider network.

5.4 Security Layers

In order to provide an end-to-end security solution, the Security Dimensions described in the previous section must be applied to a hierarchy of network equipment and facility groupings, which is composed of Security Layers. ITU-T Recommendation X.805 defines three *Security Layers*: 1) the *Infrastructure Security Layer*; 2) the *Network Services Security Layer*; and 3) the *Applications Security Layer*.

The Security Layers are a series of enablers for secure network solutions: the Infrastructure Layer enables the Network Services Layer and the Network Services Layer enables the Applications Layer. The Security Architecture addresses the fact that each layer has different security vulnerabilities and offers the flexibility of countering the potential threats in a way most suited for a particular Security Layer.

The Security Layers identify where security must be addressed in products and solutions by providing a sequential perspective of network security. For example, security vulnerabilities are first addressed for the Infrastructure Layer, then for the Network Services Layer, and finally security vulnerabilities are addressed for the Applications Layer. Security Dimensions are applied to Security Layers in order to diminish vulnerabilities that exist at each layer and thus mitigate security attacks.

5.4.1 Infrastructure Security Layer

The *Infrastructure Security Layer* consists of the network transmission facilities as well as individual network elements protected by the Security Dimensions. The Infrastructure Layer represents the fundamental building blocks of networks, their services, and applications. Examples of components that belong to the Infrastructure Layer are individual routers, switches, and servers as well as the communication links between individual routers, switches, and servers.

5.4.2 The Network Services Security Layer

The *Network Services Security Layer* focuses on security of network services that Service Providers provide to their customers. These services range from basic transport and connectivity to service enablers like those that are necessary for providing network access. The Network Services Security Layer is used to protect the Service Providers and their customers, both of which are potential targets of security threats. For example, the attackers may attempt to deny the Service Provider's ability to offer the network services, or they may attempt to disrupt service for an individual customer of the Service Provider (e.g., a corporation).

5.4.3 The Applications Security Layer

The *Applications Security Layer* focuses on security of the network-based applications accessed by Service Provider customers. These applications are enabled by network services and include traditional voice applications (e.g., ISUP and TCAP protocols and application services using these protocols) and multimedia applications (e.g., BICC, SIP, and H.323 protocols and application services using these protocols), as well as high-end applications such as customer relationship management, electronic/mobile-commerce, network-based training, video collaboration, etc. Network-based applications may be provided by third-party Application Service Providers (ASPs), Service Providers acting also as ASPs, or by enterprises hosting them in their own (or leased) data centers. At this layer there are four potential targets for security attacks: the application user, the application provider, the middleware provided by third-party integrators (e.g., web-hosting services), and the Service Provider.

As an example of the Security Layers, the following table illustrates the three security layers for the signaling and control plane for traditional SS7 and evolving networks.

Table 1 - Example of Security Layers for the Signaling and Control Plane: Traditional SS7 and Evolving Signaling and Control Networks

Security Layer	Security Layer Descriptions
Infrastructure Security Layer	Transmission facilitates and network elements (e.g., switches, STPs, SS7 links, IP routers, PSTN/VOP gateways, Servers, etc.)
Network Services Security Layer	Network transport layer services and protocols. Two main areas: (a) SS7 traditional transport network services and protocols – SCCP, MTP, and SAAL. (b) IP-Based transport – SIGTRAN protocols, IP including IP routing and control protocols (e.g., DHCP, OSPF, BGP, ISIS, LPT, CR-LDP, RSVP, RSVP-TE, DNS and LDAP).
Application Security Layer	Application protocols and application services. Two main areas: (a) Traditional SS7 application protocols (ISUP, TCAP, and OMAP), and application services supported by these protocols (e.g., POTS, IN, and LNP). (b) Multimedia applications protocols (BICC, SIP, and H.323) and application services supported by these protocols.

5.5 Application of Security Dimensions to Security Layers

The *Security Architecture* can be applied to all aspects and phases of a Security Program. A *Security Program* consists of policies and procedures in addition to technology, and progresses through three phases over the course of its lifetime: (1) the *Definition and Planning phase*; (2) the *Implementation phase*; and (3) the *Maintenance phase*. The Security Architecture can be applied to security policies and procedures, as well as technology, across all three phases of a Security Program.

The Security Architecture can guide the development of comprehensive security policy definitions, incident response and recovery plans, and technology architectures by taking into account each Security Dimension at each Security Layer and Plane during the definition and planning phase. The Security Architecture can also be used as the basis of a security assessment that would examine how the implementation of the Security Program addresses the Security Dimensions, Layers, and Planes as policies and procedures are rolled out and technology is deployed. Once a Security Program has been deployed, it must be maintained in order to keep current in the ever-changing security environment. The Security Architecture can assist in the management of security policies and procedures, incident response and recovery plans, and technology architectures by ensuring that modifications to the Security Program address each Security Dimension at each Security Layer and Plane.

To apply the security architecture to the traditional SS7 and evolving signaling and control networks, the general methodology is to specify requirements and objectives for specific security dimensions for each security layer (Infrastructure, Network Services, and Application). By applying security dimensions starting from the Infrastructure Layer to the Network Services Layer, the end user application would be secure. Specifically, the concept is to obtain end-to-end secure communication by securing and protecting each signaling transport segments between two communicating entities. The specific security feature would depend on the specific network type and protocols employed. For example, in a traditional SS7 network segment, some Security Dimensions would be based on continued use of a closed physical environment. On the other hand, for an SS7 over IP network segment, Security Dimensions would be based on use of specific security capabilities (e.g., IPsec or TLS). Certain situations may need protection at the application level. For example, observation and viewing of application information (e.g., TCAP, ISUP, SIP parameters) might be possible, although security capabilities such as IPsec and TLS are being used at the network layer. This is because the application information could be observed by intruders and unauthorized entities gaining access to intermediate nodes (e.g., STPs and Signaling Gateways) performing transport network interworking and processing. Therefore, certain aspects of securing data contained within an application protocol may have to be addressed by the application at the message origination or termination node.

5.5.1 Applying Security Dimensions to the Signaling and Control Plane Infrastructure Layer

Securing the Control Plane of the Infrastructure Layer consists of securing the control or signaling information that resides in the network elements and server platforms that comprise the network, as well as securing the receipt and transmission of control or signaling information by the network elements and server platforms. For example, the switching tables residing in network switches need to be protected from tampering or unauthorized disclosure. In another example, routers need to be protected from receiving and propagating bogus routing updates or responding to bogus routing requests originating from spoofed routers. The objectives of applying the Security Dimensions to the Control Plane Infrastructure Layer are summarized as follows:

Table 2 - Signaling and Control Plane: Infrastructure Layer

Security Dimensions	Security Objectives
Access Control	• Ensure that only authorized personnel and devices are allowed to access control information resident in the network device (e.g., a routing table) or in offline storage. • Ensure that the network device will only accept control information messages from authorized network devices (e.g., routing updates).
Authentication	• Verify the identity of the person or device observing or modifying control information resident in the network device. • Verify the identity of the device sending control information to the network device. • Authentication techniques may be required as part of Access Control.
Non-repudiation	• Provide a record identifying each individual or device that observed or modified control information in the network device and the action that was performed. This record can be used as proof of access to or modification of the control information. • Provide a record identifying the device originating control messages sent to the network device and the action that was performed. This record can be used as proof that the device originated the control message.
Data Confidentiality	• Protect control information resident in a network device or in offline storage from unauthorized access or viewing. Techniques used to address Access Control may contribute to providing Data Confidentiality for control information resident in the network device. • Protect control information destined for a network device from unauthorized access or viewing as it is being transported across the network.
Communication Security	• Ensure that control information only flows between authorized end points. (Taking action to satisfy the authentication and data integrity dimensions may satisfy this requirement).
Data Integrity	• Protect control information resident in network devices, in transit across the network, or stored offline such that unauthorized modification, creation, and replication are detectable.
Availability	• Ensure that network devices are always available to receive control information from authorized sources. This includes protection against deliberate attacks such as Denial of Service (DoS) attacks and accidental occurrences (e.g., route flapping).
Privacy	• Ensure that information that can be used to identify the network device or communications link is not available to unauthorized personnel or devices. Examples of this type of information include a network device's IP address or DNS domain name. For example, being able to identify the network devices or communications links provides targeting information to attackers. • Ensure that control information being transported across the network (e.g., routing updates) only flows between the source of the control information and its desired destination. The control information is not diverted or intercepted as it flows between these endpoints.

5.5.2 Apply Security Dimensions to the Signaling and Control Plane Network Services Layer

Securing the Control Plane of the Services Layer consists of securing the control or signaling information used by the network services. The objectives of applying the Security Dimensions to the Control Plane Services Layer are summarized as follows:

Table 3 - Signaling and Control Plane: Network Services Layer

Security Dimensions	Security Objectives
Access Control	• Ensure that control information received by a network device for a network service originates from an authorized source (e.g., a VoIP session initiation message has originated from an authorized user or device) before accepting it. For example, protect against the spoofing of a VoIP session initiation message by an unauthorized device.
Authentication	• Verify the identity of the origination of network service control information sent to network devices participating in the network service. Authentication techniques may be used as part of Access Control.
Non-repudiation	• Provide a record identifying the person or device originating the network service control messages received by a network device participating in the network service and the action that was performed. This record can be used as proof that the person or device originated the network service control message.
Data Confidentiality	• Protect network service control information resident in a network device (e.g., IPsec session databases), being transported across the network, or stored offline from unauthorized access or viewing. Techniques used to address Access Control may contribute to providing Data Confidentiality for network service control information residing in the network device.
Communication Security	• Ensure that network service control information only flows between authorized end points. (Taking action to satisfy the authentication and data integrity dimensions may satisfy this requirement).
Data Integrity	• Protect control information resident in network devices, in transit across the network, or stored offline such that unauthorized modification, creation, and replication are detectable.
Availability	• Ensure that network devices participating in a network service are always available to receive control information from authorized sources. This includes protection against active attacks such as Denial of Service (DoS) attacks.
Privacy	• Ensure that information that can be used to identify the network devices or communications links participating in a network service is not available to unauthorized personnel or devices. Examples of this type of information include a network device's IP address or DNS domain name. For example, being able to identify the network devices or communications links provides targeting information to attackers. • Ensure that network service control information being transported across the network (e.g., IPsec key negotiation messages) only flows between the source of the control information and its desired destination. The network service's control information is not diverted or intercepted as it flows between these endpoints.

5.5.3 Applying Security Dimensions to the Signaling and Control Plane Applications Layer

Securing the Applications Layer consists of securing the control or signaling information used by the network-based applications. This type of information typically causes the application to perform an action in response to receiving the information. The objectives of applying the Security Dimensions to the Applications Layer are summarized as follows:

Table 4 - Signaling and Control Plane: Applications Layer

Security Dimensions	Security Objectives
Access Control	• Ensure that application control information received by a network device participating in a network-based application originates from an authorized source before accepting it.
Authentication	• Verify the identity of the origination of application control information sent to network devices participating in the network-based application. Authentication techniques may be used as part of Access Control.
Non-repudiation	• Provide a record identifying the person or device originating the application control messages received by a network device participating in the network-based application and the action that was performed. This record can be used as proof that the person or device originated the application control message.
Data Confidentiality	• Protect application control information resident in a network device, being transported across the network, or stored offline from unauthorized access or viewing. Techniques used to address Access Control may contribute to providing Data Confidentiality for network-based application control information resident in the network device.
Communication Security	• Ensure that application control information only flows between authorized end points. (Taking action to satisfy the authentication and data integrity dimensions may satisfy this requirement).
Data Integrity	• Protect network-based application control information resident in network devices, in transit across the network, or stored offline such that unauthorized modification, creation, and replication are detectable.
Availability	• Ensure that network devices participating in network-based applications are always available to receive control information from authorized sources. This includes protection against active attacks such as Denial of Service (DoS) attacks.
Privacy	• Ensure that information that can be used to identify the network devices or communications links participating in a network-based application is not available to unauthorized personnel or devices. Examples of this type of information include a DNS domain name. For example, being able to identify the network devices or communications links provides targeting information to attackers. • Ensure that application control information being transported across the network only flows between the source of the control information and its desired destination. The network-based application's control information is not diverted or intercepted as it flows between these endpoints.

5.6 Signaling Network Interconnection Model

Signaling Network Interconnection involves direct or indirect interconnection among different signaling network types to support services across networks. The governing factor is that required security mechanisms, mitigation services, procedures, practices, etc., are dependent on the specific characteristic of the network. These characteristics include the network architecture, transport network type (e.g., MTP, ATM or IP), and application protocols (e.g., ISUP, BICC, SIP, H.323). In addition, technology specific characteristics will dictate specific mitigation solutions. The general model for signaling network interconnection security is illustrated in Figure 3 below:

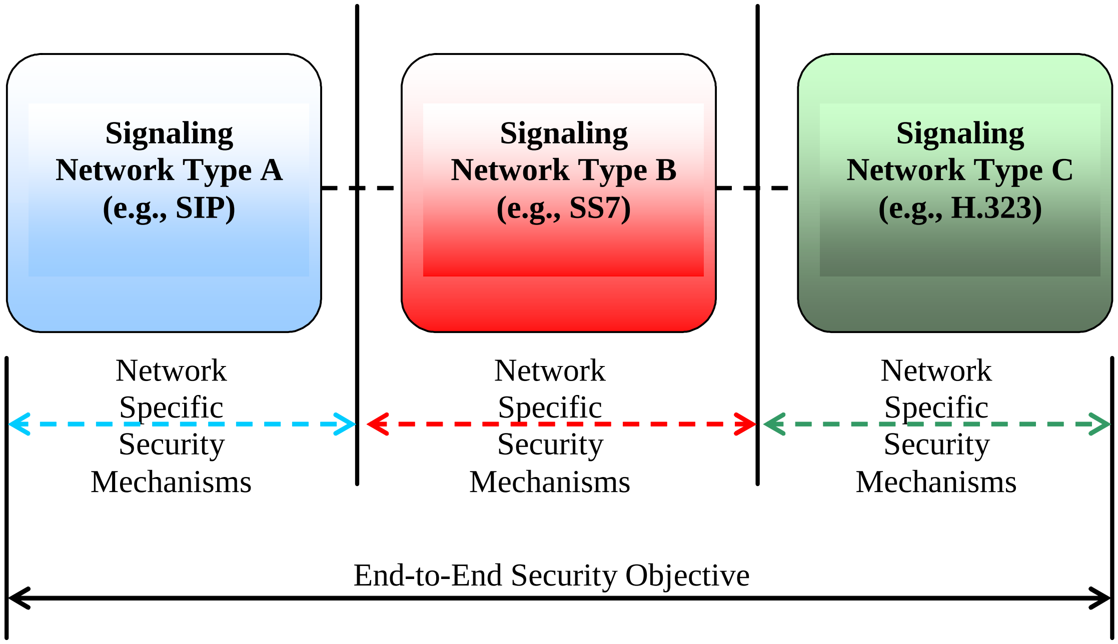
Signaling Network Type A (e.g., SIP)
Signaling Network Type B (e.g., SS7)
Signaling Network Type C (e.g., H.323)
Network Specific Security Mechanisms
Network Specific Security Mechanisms
Network Specific Security Mechanisms
End-to-End Security Objective

Figure 3 - Model for Signaling Network Interconnection Security

The primary objective of security functions and procedures is to obtain end-to-end secure signaling communications across multiple interconnected signaling network types by allowing each network to employ network specific security mechanisms, mitigation services, etc, within its domain. This includes but is not limited to:

- Obtaining secure end-to-end signaling associations across multiple interconnected signaling network types.
- Maintaining network integrity and availability of signaling across multiple interconnected signaling network types.
- Maintaining integrity and availability of applications/services supported across multiple interconnected signaling network types, including integrity and availability of applications/services supported within a network domain.

The basic concept is that each signaling network type will be responsible for security within its network domain and at its interconnection interface using network specific solutions. For example, a traditional SS7 network could employ security mechanisms, mitigation services, practices, etc, that are specific to the traditional SS7 environment (e.g., the use of a closed network for SS7 signaling) for security within its own domain. A VoP network would employ a different set of security mechanisms, services, and practices (e.g., use of IPsec) for security within its domain. To achieve secure signaling communications and signaling network integrity and availability end-to-end requires specification and implementation of appropriate capabilities for inter-network (cross domain) integrity and interworking and qualification of the allowed security risk in each network type. Specifically, at the interconnection points, capabilities must be available to prevent exploitation of network interfaces and interworking functions to compromise the integrity and availability of the internetworking signaling.

Each signaling network type is responsible for providing and maintaining secure connections for the signaling association segment within its network domain**.** Specifically, each signaling network type shall specify and implement network specific security mechanisms, mitigation services, practices, etc., to protect interconnection interfaces and internetwork signaling associations. Specifically, this includes:

- Protecting and maintaining integrity and availability of network elements providing signaling network interconnections.
- Protecting and maintaining integrity and availability of signaling interconnections and interconnections interfaces.
- Protecting and maintaining integrity of protocol mapping and interworking functions between network domains.

Security requirements for specific signaling networks are given in the detailed specifications.

6 DESIGN GUIDELINES

The following guidelines were considered when this document was created:

Guideline	Description
Isolation	Isolation of signaling and control traffic from customer traffic where possible. Physical and logical isolation should be considered.
Effective Security Policies	Requirements and supporting architectures must allow for policies that are definable, flexible, enforceable, auditable, verifiable, reliable, and usable.
Reduced complexity	Improve security by implementing security mechanisms that have widely available implementations and widespread deployment, so that use histories allow security mechanisms to be reviewed.
Extensibility	Consider next steps for enhancing and improving network signaling and control security to further satisfy given requirements with evolving technology and mechanisms or to satisfy newly defined security requirements.
Housekeeping	Requirements should have minimal impact on network operations.
Standards	Use ideas and concepts that are already standardized as appropriate (e.g., IP security [IPsec], digital signatures). All aspects of the openly developed standards should be addressed including system, protocols, modes, algorithm, option, key size, and encoding.
Interoperability	Minimize interoperability issues by limiting number of options.

7 SIGNALING AND CONTROL PLANE

7.1 Signaling and Control Plane Protocols

The security requirements in this document were developed to apply at a minimum to the following signaling and control protocol and interface areas:

- *Multimedia over Packet Protocols* responsible for controlling voice and multimedia services over packet networks:
  - H.323
  - Session Initiation Protocol (SIP)
  - H.248
- *SS7 Network Protocols*:
  - SS7 Application Protocols (e.g., ISUP and TCAP)
  - SS7 Transport Protocols (e.g., SCCP and MTP)
- *Access Network Protocols*:
  - SIP and H.323
  - ISDN User Adaptation layer (IUA)

- *Network Interfaces*:
    - User to Network Interface (UNI)
    - Network to Network Interfaces (NNI)

7.2 Signaling and Control Plane Vulnerabilities

This section provides a general discussion of the threats and vulnerabilities associated with the signaling and control plane.

The signaling and control plane is generally transparent to the legitimate user, but not to the malicious attacker.

Some of the attacks to the signaling and control plane that could seriously disrupt network operation are listed below:

- Spoofing of communications.
- Disruption of signaling.
- Denial of TDM or packet based telephony service.

8 GENERAL SECURITY REQUIREMENTS

This section provides requirements for general security tools including security protocols, cryptographic algorithms, cryptographic key sizes, and other security facilities that can be used to provide signaling and control plane security. This document presents the general requirements for these tools that are in turn referenced by the more detailed documents within this family of standards to provide security at the infrastructure layer, the network transport services layer and the application security layer as described in reference [ITU X.805].

Various referenced source documents -- for example, IETF RFCs -- have their own definitions for mandatory, recommended, and optional requirements. This document specifies whether the features referenced in source documents are mandatory requirements for securing the signaling and control plane as per this specification. Security features identified as mandatory requirements within this specification will take precedence over categorizations defined in the source documents.

The use of any particular security tool or protocol such as IPsec or TLS is conditional on this protocol being required by the detailed specific security documents (e.g., VoP/Multimedia Security, SS7 Security). It is not assumed that all security protocols must be implemented in any given network. In addition, some individual requirements are designated as "conditional requirements." This indicates that the choice to specify a requirement for a particular interface is dependent on it being specified in the detailed specific security documents or on particular customer needs.

Features not mentioned in this specification are assumed by default to be non-recommended security features for the signaling and control plane. As such, this specification neither encourages nor discourages use of omitted features.

In addition to the Requirements, Conditional Requirements, and Objectives in this section, Annex A specifies best practices and guidelines to minimize security risks. The general methodology described in this section is applicable to all the security related documents. Requirements, Conditional Requirements, and Objectives are testable. Recommendations and best practices that are not testable are considered as guidelines and are not numbered. Requirements, Conditional Requirements, and Objectives are numbered in increments of 100.

The requirements are highlighted in *tags* to facilitate requirements traceability. Each tag in the series of the security related documents has a label containing a unique number (e.g., <REQ-SEC-00900>) where REQ-SEC is the type of requirement and 00900 is the number, which identifies the specific requirement. Bold text within the tag identifies the specific requirement. Non-bold text provides supplementary explanation of the requirement. Non-bold text is not an additional requirement.

The series of the security related documents use the following terminology:

- *Requirement* – Feature or function that is necessary to meet the needs of a service provider. Failure to meet a requirement may cause application or service restrictions, result in improper functioning of the product, or hinder operations. A requirement is identified by the letters "*REQ-SEC*".
- *Conditional Requirement* - Feature or function that is needed by some but not all service providers and as such are left for the individual service providers to choose. Conditional requirements may also be specified by the specific detailed security specifications (e.g., VoP/Multimedia Security, SS7 Security) to meet the needs of a particular application. A conditional requirement is identified by the letters "*CR-SEC*".
- *Objective* – Feature or function that is desirable and may be required by a service provider. An Objective represents a goal to be achieved. An Objective may be reclassified as a Requirement at a future date. An objective is identified by the letters "*O-SEC*" and includes the words *it is desirable* or *it is an objective*.

8.1 Security Protocol Overview

This section gives an overall view of security protocols which can be used to address the security dimensions for the signaling and control plane as described in reference [ITU X.805]: Access Control Security, Authentication Security, Non-repudiation Security, Data Confidentiality Security, Communication Security, Data Integrity Security, Availability Security, and Privacy Security.

The recommended protocols used to provide assurance of authenticity and confidentiality for signaling and routing, as depicted in Figure 4, are: H.235, TLS, IPsec and Routing Protocol Security Extensions. H.235 specifies security for the H.series family of multimedia protocols and is described here, although H.235 utilizes message exchanges within H.245 for establishing cryptographic key and algorithm parameters and attributes. SIP, where used in this document, refers to the overall IETF family of protocols related to the Session Initiation Protocol.

<table>
<tr><td colspan="5">H.323 (& H.235), SIP, H.248, SS7 and Adaptation Protocols (e.g., ISUP/M3UA), etc.</td></tr>
<tr><td><i>Null Functionality</i></td><td>TLS</td><td colspan="3"></td></tr>
<tr><td>UDP</td><td>TCP</td><td>TCP</td><td>SCTP</td><td>UDP</td></tr>
<tr><td colspan="2"><i>Null Functionality</i></td><td colspan="3">IPsec</td></tr>
<tr><td colspan="5">IPv4 (and IPv6)</td></tr>
</table>

Figure 4 - Security Protocol Usage

8.2 Cryptographic Algorithms & Keys

This clause provides information on cryptographic algorithms and key management.

8.2.1 Definitions

8.2.1.1 Symmetric Encryption

Symmetric, or *secret key encryption*, refers to a cryptographic system where enciphering and deciphering keys are the same. Symmetric cryptosystems require that initial arrangements be made for the individuals to share a unique secret key. The key must be distributed to the individuals via a secure means, because knowledge of the enciphering key implies knowledge of the deciphering key and vice-versa. Symmetric encryption algorithms include the Advanced Encryption Standard (AES) and 3DES (Triple DES Algorithm).

8.2.1.2 Asymmetric Encryption

An *asymmetric encryption* system is one in which the enciphering and deciphering keys are related but different. One is made public, whereas the other is kept secret. The public key is different from the private key, and no feasible way is known for deriving the private key from the public key. Public keys are distributed widely; however, the private key is always kept secret. The use of asymmetric encryption is usually limited to the encryption of symmetric keys for key exchange and the signing of message digests for digital signatures. In key exchange, the recipient's public key is used and in the signing of message digests the signer's private key is used. Asymmetric encryption algorithms include Rivest, Shamir, Adleman (RSA), Digital Signature Algorithm (DSA), and Elliptic Curve Cryptography (ECC).

8.2.1.3 Message Integrity

Message integrity algorithms are used to ensure data integrity for arbitrary length messages. Symmetric data integrity algorithms use a message digest algorithms combined with a hashing function and a symmetric key. Asymmetric message verification algorithms such as the Digital Signature Algorithm (DSA) use a private key for signing a message digest to ensure data integrity. Symmetric data Integrity algorithms include the Hashed Message Authentication Code (HMAC) with both MD5 (Message Digest 5) and SHA-1 (Secure Hash Algorithm-1) hashing algorithms.

8.2.2 Cryptographic Key Management

Specific requirements for cryptographic key management beyond those provided by the IPsec and TLS protocols as described below may be addressed in the detailed specifications.

8.3 IPsec and IKE Protocol Requirements

This section specifies security features that are required to be supported when use of IPsec is required for a given interface. For example, when use of IPsec is required by a specific detailed standard (e.g., VoP/Multimedia Security, SS7 Security) all the requirements in this section must be met. Additional detailed features of IPsec beyond this generic set will be addressed in the specific individual detailed documents.

8.3.1 IPsec Security Modes

IPsec supports two modes of operation: *transport mode* and *tunnel mode*. See reference [RFC 2401] for a complete discussion of IPsec modes of operation. Note that at least one mode is required to be supported for any IPsec usage.

(a) Tunnel mode	[CR-SEC-GEN-00100]
(b) Transport mode	[CR-SEC-GEN-00200]

8.3.2 IPsec Protocols

IPsec provides two protocols; the *Encapsulation Security Payload (ESP) protocol* and the *Authentication Header (AH) protocol*. ESP protocol provides data confidentiality, data integrity, and data origin authentication. AH protocol provides only data integrity and data origin authentication. ESP protocol is selected as a requirement since it can provide data confidentiality in addition to data integrity/data origin authentication. When data integrity/data origin is required without data confidentiality, the ESP protocol can be used with null encryption.

(a) ESP (RFC 2406)	[REQ-SEC-GEN-00100]

8.3.3 IPsec Encryption Algorithms

IPsec relies on underlying cryptographic algorithms to provide encryption services.

(a) Null encryption [RFC 2410]	[REQ-SEC-GEN-00200]
(b) 3DES CBC-mode [RFC 2451] (with 3 independent 56 bit keys)	[REQ-SEC-GEN-00300]
(c) AES CBC [RFC3602] (with 128 bit key)	[REQ-SEC-GEN-00400]

8.3.4 IPsec Implementation Authentication Algorithms

IPsec relies on underlying cryptographic algorithms to provide data origin authentication/data integrity services. These services should always be used when IPsec is being used. Note that AES-XCBC is emerging as an improved message authentication algorithm based on AES. MD5 is included as an option since it is currently widely implemented; however, it has been found to have collision weaknesses in some other applications.

(a) HMAC-SHA-1 [RFC 2404] (with 160 bit key)	[REQ-SEC-GEN-00500]
(b) AES-XCBC [RFC 3566] (with 128 bit key)	[O-SEC-GEN-00100]

8.3.5 IPsec Implementation Selectors

Selectors support a packet filtering capability within the IPsec architecture. This enables the IPsec implementation to selectively process or discard packets based on matching selector criteria.

(a) Source IP address	[REQ-SEC-GEN-00600]
(b) Destination IP address	[REQ-SEC-GEN-00700]
(c) Transport layer protocol (UDP, TCP or SCTP)	[REQ-SEC-GEN-00800]
(d) Transport layer protocol (UDP, TCP or SCTP) port numbers	[REQ-SEC-GEN-00900]
(e) Wildcards	[REQ-SEC-GEN-01000]

8.3.6 Support for Internet Key Exchange (IKE)

Internet Key Exchange (IKE) is used to provide an automatic mechanism for key generation. Two versions of IKE are available: *IKEv1* and *IKEv2*. Currently, IKEv1 is standardized and widely implemented and IKEv2 is only emerging. Support for IKEv2 in addition to IKEv1 is considered an objective.

(a) Support of IKEv1 [RFC2409]	[REQ-SEC-GEN-01100]
(b) Support of IKEv2 [draft-ietf-ipsec-ikev2-12.txt]	[O-SEC-GEN-00200]

8.3.7 IKE Implementation Modes

IKEv1 provides two modes of operation: *main mode* and *aggressive mode*. Main mode is more secure; however, it takes more time to complete than aggressive mode. Support for aggressive mode may not be required by all products.

(a) Main mode	[REQ-SEC-GEN-01200]
(b) Aggressive mode	[CR-SEC-GEN-00300]

NOTE - Implementation modes will depend on the IKE version recommendation.

8.3.8 IKE Implementation Encryption Algorithms

IKE relies on underlying encryption algorithms to provide confidentiality services.

(a) 3DES [3DES] (with three independent 56 bit keys)		[REQ-SEC-GEN-01300]
(b) AES [FIPS-197]	(with 128 bit key)	[CR-SEC-GEN-00400]
(c) AES [FIPS-197]	(with 196 bit key)	[CR-SEC-GEN-00500]
(d) AES [FIPS-197]	(with 256 bit key)	[CR-SEC-GEN-00600]

8.3.9 IKE Implementation Secure Hash Algorithms

IKE relies on underlying secure hash algorithms to provide data integrity services.

(a) MD5 [RFC 1321] (with 128 bit message digest)	[REQ-SEC-GEN-01400]
(b) SHA-1 [FIPS 180-2] (with 160 bit message digest)	[REQ-SEC-GEN-01500]

8.3.10 IKE Implementation Authentication Methods

IKE performs authentication of devices identities as part of the key exchange protocol.

(a) Pre-shared keys		[CR-SEC-GEN-00700]
(b) Digital signatures (RSA)	with 1024 bit or greater key	[REQ-SEC-GEN-01600]

8.3.11 IKE Implementation Oakley groups

Different Oakley groups are used within IKE during the Diffie-Hellman key derivation process depending on security and speed of processing requirements. Oakley Group 14 is recommended to provide sufficient security when IKE is used to establish security associations with 128 bit symmetric encryption. [RFC 2409], [RFC 3526].

(a) Group 1 (768 bit prime MODP group)	[REQ-SEC-GEN-01700]
(b) Group 2 (1024 bit prime MODP group)	[REQ-SEC-GEN-01800]
(c) Group 3 (Elliptic curve group over GF[2^155])	[CR-SEC-GEN-00800]

(d) Group 4 (Elliptic curve group over GF[2^185])	[CR-SEC-GEN-00900]
(e) Group 5 (1536 bit prime MODP group)	[REQ-SEC-GEN-01900]
(f) Group 14 (2048 bit prime MODP group)	[REQ-SEC-GEN-02000]

8.3.12 IKE Support of Perfect Forward Secrecy

Perfect Forward Secrecy, where new keys are derived independently from old keys, is necessary to ensure a high security level.

(a) Support for Perfect Forward Secrecy	[REQ-SEC-GEN-02100]

8.3.13 Random number generators for IPsec/IKE

Random number generation implementations tend to be weak. Many semiconductor manufacturers are adding secure random number generators to their integrated circuits, which should be used if available. If no hardware is available, strong pseudo-random number generator software may optionally be used in keeping with IETF informational RFC 1750 – Randomness Recommendations for Security. [RFC 1750].

(a) Hardware random number generator	[O-SEC-GEN-00300]
(b) Pseudo random number generator software	[CR-SEC-GEN-01000]

8.4 TLS Protocol Requirements

This section specifies security features that are required to be supported when use of *Transport Layer Security (TLS)* is required for a given interface. [RFC 2246]. For example, when use of TLS is required by a specific detailed standard (e.g., VoP/Multimedia Security, SS7 Security) all the requirements in this section must be met. Additional detailed features of TLS beyond this generic set will be addressed in the specific individual detailed documents.

Note that TLS is the IETF standardized successor to the Secure Socket Layer (SSL) protocol. TLS has security enhancements over the SSL protocol. See [RFC-2246], [RFC 3268], and [RFC 3546].

8.4.1 TLS Encryption Algorithms

TLS relies on underlying cryptographic algorithms to provide encryption services.

(a) 3DES CBC-mode (with 3 independent 56 bit keys)	[REQ-SEC-GEN-02200]
(b) AES CBC (with 128 bit key)	[REQ-SEC-GEN-02300]
(c) Null encryption	[REQ-SEC-GEN-02400]

8.4.2 TLS Authentication Algorithms

TLS relies on underlying cryptographic algorithms to provide data origin authentication/data integrity services. These services should always be used when TLS is being used. Note that AES-XCBC is emerging as an improved message authentication algorithm based on AES.

(a) HMAC-SHA-1 (with 160 bit key)	[REQ-SEC-GEN-02500]

8.4.3 Key Exchange Algorithms for TLS

TLS specifies various methods for key exchange. The following are recommendations for methods for key exchange within the TLS protocol:

(a) Rivest Shamir Adleman (RSA)	[REQ-SEC-GEN-02600]
(b) Diffie Hellman (DH)	[REQ-SEC-GEN-02700]

8.4.4 Ciphersuites for TLS

TLS specifies various ciphersuites for use within the TLS protocol, as discussed in detail in [RFC 3268]. The following are recommendations for ciphersuites to be used within the TLS protocol:

(a) TLS_RSA_WITH_NULL_SHA	[REQ-SEC-GEN-02800]
(b) TLS_RSA_WITH_3DES_EDE_CBC_SHA	[REQ-SEC-GEN-02900]
(c) TLS_RSA_WITH_AES_128_CBC_SHA	[REQ-SEC-GEN-03000]
(d) TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA	[REQ-SEC-GEN-03100]
(e) TLS_DH_RSA_WITH_AES_128_CBC_SHA	[REQ-SEC-GEN-03200]

8.4.5 Use of X.509 Certificates in TLS

X.509 certificates are used for authentication in TLS, and all X.509 certificates must be signed by a trusted party.

(a) X.509 certificates must be signed by a trusted party	[REQ-SEC-GEN-03300]

8.4.6 TLS Authentication

TLS allows either *unidirectional authentication* (where the server is authenticated to the client only) or *bidirectional authentication* (where both client and server authenticate to each other). Bidirectional authentication is the usual method used in the public Internet where the server uses a digital signature and X.509v3 server certificate to authenticate its identity, and the client uses an ID and password to authenticate its identity. For network signaling and control applications, bidirectional authentication is mandatory to allow each party to know it is communicating with the desired endpoint.

(a) Bi-directional authentication for TLS applications	[REQ-SEC-GEN-03400]

8.4.7 Random number generators for TLS

Random number generation implementations tend to be a weak. Many semiconductor manufacturers are adding secure random number generators to their integrated circuits, which should be used if available. If no hardware is available, strong pseudo-random number generator software may optionally be used in keeping with IETF RFC 1750, *Randomness Recommendations for Security*. [RFC 1750].

(a) Hardware random number generator	[O-SEC-GEN-00400]
(b) Pseudo random number generator software	[CR-SEC-GEN-00900]

Annex A
(informative)

A SIGNALING & CONTROL PLANE – SECURITY BEST PRACTICES

Best practice security mechanisms such as the use of firewalls, operating system hardening, vulnerability scanning, and Intrusion Detection Systems (IDS) may be employed to help ensure a more secure signaling and control plane. This section provides a summary of such best practice security mechanisms. The use of these best practice security mechanisms for specific signaling networks is given in the detailed specifications.

This document does not comment on the applicability or the completeness of security best practices, including those developed by the NRIC and the IETF.

A.1 Firewalls

A *firewall* is a fundamental security building block that provides network isolation at boundaries between network segments or between different networks. A firewall performs isolation based on specific traffic filtering rules configured onto the firewall. Firewalls may be used in conjunction with other security mechanisms to provide an additional layer of security for the signaling and control plane. The addition of firewalls helps provide "defense in depth" security whereby multiple security mechanisms are overlaid to achieve stronger security.

A firewall examines both inbound and outbound traffic, and should be configured to deny all traffic unless specifically allowed by the firewall rules. A firewall may also provide logging of traffic and trigger alarms when unauthorized packets are detected. Firewalls can physically be provided as separate appliances or may be provided as software on the host machines themselves. Types of firewalls include static packet filtering, application layer, and state aware packet filtering firewalls, and the choice of the type of firewall will depend on particular customer needs and preferences.

Static packet filtering firewalls examine incoming and outgoing packets and apply a set of rules to determine whether packets will be allowed to transit the firewall or be dropped. This determination is typically based on the packet source and destination IP addresses, the protocol type, and the TCP source and destination ports. Depending on the packet and the criteria, the firewall will drop or forward the packet, and possibly create a log entry and/or raise an alarm. Some static packet filtering firewalls may also provide deeper inspection of packets, possibly up to the application layer.

Application layer firewalls run applications on behalf of the machines in the network they are protecting, and are often called *proxy firewalls*. When performing the applications, application layer firewalls will detect any anomalous activity; if found, they will not pass the data onto the machines they are protecting. Application layer firewalls must be enabled with all necessary applications and must run these applications on behalf of all protected machines. Because of this, application layer firewalls have a high impact on network performance.

State aware firewalls perform packet filtering functions similar to static packet filtering firewalls, and in addition maintain information about the state of traffic connections. The state information allows the firewall to make better decisions about whether to allow or deny particular traffic. For example, a state aware firewall may be configured to only allow traffic from machines on one side of the network to initiate communications. This is particularly useful where private networks are connected to public networks, since typically only the machines on the private network are trusted to initiate data communications.

When using firewalls as an additional signaling and control plane security, the firewalls should be configured to allow only desired signaling and control communication between a set of machines. Any other traffic on the network other than the desired communications should be denied, thereby providing a layer of protection for these machines.

Note that providing firewalls may have system engineering and product impacts, and some applications may have to be made firewall aware. Also note that firewalls will not protect against all security attacks —for example, an attacker spoofing legitimate signaling packet information.

A.2 Operating System Hardening

Servers and network elements used for signaling and control plane functions are vulnerable to any number of attacks including the following:

- Backdoor programs;
- Sniffing programs;
- Password grabber and cracking tools;
- Exploitation of defects in operating system services; and
- Denial of service (DoS).

Some of these attacks are based on well-publicized techniques, with scripts and other tools available to make it possible for less knowledgeable crackers to apply exploits against systems. Once a system has been compromised, an intruder can do a number of things, among which are:

- Modify or destroy information.
- Disclose sensitive information.
- Install malicious code to gather information.
- Use the compromised server to attack other systems.

Operating system hardening procedures may be used to improve the resistance of operating systems to attacks. Operating system hardening procedures are essentially sound practices that are followed during the installation and configuration of an operating system. While no system is absolutely secure, following operating system hardening procedures will result in systems that are harder for crackers to compromise.

Operating system hardening essentially involves the restriction of services, ports, and access to applications and files. Operating system hardening also involves only running applications from a restricted access privilege account and with only absolutely necessary ports and services running.

Operating system manufacturers should be consulted to obtain the latest OS hardening procedures and security patches.

A.3 Vulnerability Assessment

The goal of performing a *vulnerability assessment* on network elements is to discover security vulnerabilities, weaknesses, and areas of risk. Vulnerability testing is designed to try and make systems fail by interrupting services, circumventing devised security controls, capturing confidential data, obtaining unauthorized access to the system, or stealing or denying service. Vulnerability assessment may be included for signaling and control plane network elements in order to ensure even stronger security.

Vulnerability assessment for network elements may be conducted at the product verification stage, and then ongoing as part of network maintenance. Including security vulnerability testing at the product verification stage is advantageous since there is already a pre-established procedure to record and submit requests for changes. Ongoing routine vulnerability assessments are useful to identify new threats and vulnerabilities and initiate action to mitigate the issues identified.

A wide range of vulnerability assessment tools are available both commercially and as open source software. These tools include ISS Internet Scanner, Nessus, ISIC, Protos Test Suites, NMAP, and many others. One or more of these or other similar tools may be used to perform vulnerability assessment on signaling and control plane network elements and servers.

A.4 Intrusion Detection Systems

Intrusion Detection Systems (IDS) can be incorporated in a network solution to provide even stronger security for the signaling and control plane. For example, IDS can be used to warn network administrators of the possibility of a security incident such as a SIP server compromise or denial-of-service attack to the signaling and control plane.

IDS can be broadly categorized according to the following criteria:

- *Real Time or Off Line Incident Detection*: A real time IDS network traffic and logs as events take place. An off-line IDS system analyzes intrusions in batch mode after incidents have occurred.
- *Network Based or Host Based Installation*: A network-based IDS typically involves multiple monitors installed at choke points on the network where all traffic between two points can be monitored. A host-based IDS requires that software be installed directly on the servers to be protected, and monitors the network connections and user activity on those servers.
- *Reactive of Passive*: A reactive IDS actively intervenes to head off attacks by modifying firewall rules or router filters or other measures. A passive IDS system only notifies administrators or other network systems of the problem.

Most commercial IDS products provide a combination of network and host-based monitoring capabilities, with a central management device to receive the reports from the various monitors and alert the network administrators.

Annex B
(informative)

B References

[T1.276]	T1.276-2003, *Operations, Administration, Maintenance, and Provisioning Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane.* https://www.atis.org/docstore/default.aspx
[H.323]	ITU-T Recommendation H.323 (2000), *Packet-Based multimedia communications systems.* http://www.itu.int/ITU-T/
[H.323 – Annex R]	ITU-T Recommendation H.323 – Annex R (2001), *Robustness Methods for H.323 Entities.* http://www.itu.int/ITU-T/
[H.225.0]	ITU-T Recommendation H.225.0 (2000), *Call signaling protocols and media stream packetization for packet based multimedia communications Systems.* http://www.itu.int/ITU-T/
[H.225.0 – Annex G]	ITU-T Recommendation H.225.0 – Annex G (2002), *Communication Between Administrative Domains.* http://www.itu.int/ITU-T/
[H.245]	ITU-T Recommendation H.245 (2003), *Control protocol for multimedia communication.* http://www.itu.int/ITU-T/
[H.235]	ITU-T Recommendation H.235 (2000), *Security and encryption for H Series (H.323 and other H.245 based) multimedia terminals.* http://www.itu.int/ITU-T/
[ANSI X9.52-1998]	ANSI X9.52-1998, *Triple Data Encryption Algorithm Modes of Operation*, http://webstore.ansi.org/ansidocstore/dept.asp?dept_id=80
[RFC 2402]	IETF RFC 2402, *Internet Protocol Authentication Header*", November 1998, S. Kent, R. Atkinson; http://www.ietf.org/rfc/rfc2402.txt?number=2402
[RFC 2403]	IETF RFC 2403, *The Use of HMAC-MD5-96 within ESP and AH*, http://www.ietf.org/rfc/rfc2403.txt?number=2403
[RFC 2405]	IETF RFC 2405, *The ESP DES CBC Cipher Algorithm with Explicit IV*, http://www.ietf.org/rfc/rfc2405.txt?number=2405
[RFC 2407]	IETF RFC 2407, *The Internet IP Security Domain of Interpretation for ISAKMP*," http://www.ietf.org/rfc/rfc2407.txt?number=2407
[RFC 2408]	IETF RFC 2408, *Internet Security Association and Key Management Protocol*," http://www.ietf.org/rfc/rfc2408.txt?number=2408
[RFC 2411]	IETF RFC 2411, *IP Security Document Roadmap*," http://www.ietf.org/rfc/rfc2411.txt?number=2411
[RFC 2412]	IETF RFC 2412, *The OAKLEY Key Determination Protocol*," http://www.ietf.org/rfc/rfc2412.txt?number=2412
[RIPEMD-160]	3.ISO/IEC 10118-3:1998, *Information technology - Security techniques - Hash-functions - Part 3: Dedicated hash-functions*," International Organization for Standardization, Geneva, Switzerland, 1998.
[RFC 2857]	IETF RFC 2857, *The Use of HMAC-RIPEMD-160-96 within ESP and AH*, http://www.ietf.org/rfc/rfc2857.txt
[SSL V3]	*Secure Socket Layer Version 3.0 Specification*, Netscape Communications. http://wp.netscape.com/eng/ssl3/
[RFC 1750]	IETF RFC 1750, Randomness Recommendations for Security. http://www.ietf.org/rfc/rfc1750.txt?number=1750

[RFC 3261]	IETF RFC 3261, SIP: Session Initiation Protocol ftp://ftp.rfc-editor.org/in-notes/rfc3261.txt
[RFC 3265]	IETF RFC 3265, Session Initiation Protocol (SIP)-Specific Event Notification. ftp://ftp.rfc-editor.org/in-notes/rfc3265.txt
[ITU X.500]	ITU-T Recommendation X.500 (03/00), Information technology - Open Systems Interconnection - The Directory: Overview of concepts, models and services.
[RFC 3057]	IETF RFC 3057, ISDN Q.921-User Adaptation Layer. http://www.ietf.org/rfc/rfc3057.txt?number=3057