ATIS-0100010

SECURITY FOR NEXT GENERATION NETWORKS -- AN END USER PERSPECTIVE

TECHNICAL REPORT

Notice of Disclaimer & Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER, NO REPRESENTATION OR WARRANTY IS MADE OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, WITH RESPECT TO ANY CLAIM, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES ANY AND ALL USE OF OR RELIANCE UPON THIS INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

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-0100010, *Security for Next Generation Networks -- An End User Perspective*

Is an ATIS Standard developed by the **PRQC Security (SEC)** Task Force under the **ATIS Network Performance, Reliability, and Quality of Service Committee (PRQC)**.

Published by

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

Printed in the United States of America.

ATIS-0100010

Technical Report on

SECURITY FOR NEXT GENERATION NETWORKS – AN END USER PERSPECTIVE

Secretariat

Alliance for Telecommunications Industry Solutions

Approved January 17, 2007

Abstract

This Technical Report (TR) provides a security overview and guidelines for security in Next Generation Networks (NGN) relevant to the end user.

FOREWORD

The Alliance for Telecommunication Industry Solutions (ATIS) serves the public through improved understanding between carriers, customers, and manufacturers. The Network Performance, Reliability, and Quality of Service Committee (PRQC) -- formerly T1A1 -- develops and recommends standards, requirements, and technical reports related to the performance, reliability, and associated security aspects of communications networks, as well as the processing of voice, audio, data, image, and video signals, and their multimedia integration. PRQC also develops and recommends positions on, and foster consistency with, standards and related subjects under consideration in other North American and international standards bodies.

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

At the time it approved this document, PRQC, which is responsible for the development of this Technical Report (TR), had the following members:

M.Neibert, PRQC Chair
N. Seitz, PRQC Vice-Chair
S. Barclay, ATIS Secretariat
C. Underkoffer, ATIS Chief Editor
M. Lee, PRQC Technical Editor
A. Nguyen, PRQC Technical Editor
A. Webster, PRQC Technical Editor

Organization Represented	Name of Representative
Alcatel-Lucent	Stuart O. Goldman
AT&T	Percy Tarapore Charles A. Dvorak (Alt)
Avici Systems	Esmeralda Swartz
Cingular Wireless LLC	Don Zelmer Marc Grant (Alt)
Department of Defense	Chris Fitzgerald
Embarq Corporation	Carl M. Coopage John M. Heinz (Alt)
Ericsson Incorporated	Mustafa Kocaturk Susan Sabater-Maroto(Alt)
ETRI	Tae-Soo Chung Sung-Soo Kang (Alt)
Intelsat	Mark Neibert
National Communications Systems	An Nguyen Carol-Lyn Taylor (Alt)

Organization Represented	Name of Representative
National Telecom & Info Admin - NTIA	Neal B. Seitz Arthur Webster (Alt)
Nortel	Joseph A. Zebarth
Qwest	Steve Showell Michael Fargano (Alt)
Siemens Communications Inc.	Suhas S. Gandhi David E. Francisco (Alt)
Sprint Nextel	Mark L. Jones
Telcordia Technologies	Spilios Makris Cliff Halevi (Alt)
Tellabs Operations, Inc.	William A. Walker Kevin Stodola (Alt)
Verisign, Inc.	Anthony M. Rutkowski
Verizon Communications	John Colombo Greg Cermak (Alt)

The PRQC Security (SEC) Task Force was responsible for the development of this document.

TABLE OF CONTENTS

TABLE OF FIGURES

Technical Report on –

Security for Next Generation Networks -- An End User Perspective

1 Scope, Purpose, & Application

1.1 Scope

This Technical Report (TR) provides guidelines for security in Next Generation Networks (NGN) relevant to the end user.

1.2 Purpose

The purpose of this TR is to provide an overview and guidelines for security in the NGN. This TR will provide information that is needed to develop a consistent set of security requirements as they relate to the end user. User plane security requirements are not the focus of this document and are the subject of a proposed ANSI Standard that provides End User Security Requirements.

1.3 Application

This TR discusses security mechanisms that are available for the implementation and maintenance of secure and reliable communications over the NGN. This TR identifies cryptographic standards that could be used by products required to implement these cryptographic mechanisms.

2 References

[1] RFC 2828, *Internet Security Glossary*.[1]

[2] ISO/IEC 7498-2, *Information Processing Systems--Open Systems Interconnection Reference Model---Part 2: Security Architecture*.[2]

[3] T1.276-2003, *Operations, Administration, Maintenance, and Provisioning Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane*.[3]

[4] IETF RFC3830, *MIKEY: Multimedia Internet KEYing*.[4]

[1] RFC text is available at < http://www.freesoft.org/CIE/RFC/index.htm >.

[2] This document is available from the International Organization for Standardization.
< http://www.iso.ch/iso/en/prods-services/ISOstore/store.html >

[3] This document is available from the Alliance for Telecommunications Industry Solutions (ATIS), 1200 G Street N.W., Suite 500, Washington, DC 20005. < https://www.atis.org/docstore/default.aspx >

[5] IETF RFC2327, *SDP - Session Description Protocol*.[5]

[6] ITU-T X.800, *Security Architecture for Open Systems Interconnection for CCITT Applications*.[6]

[7] ITU-T X.805, *Security Architecture for Systems Providing End-to-end Communications*.[6]

[8] ATIS-0100523.2007, *ATIS Telecom Glossary 2007*.[7]

3 DEFINITIONS, ACRONYMS & ABBREVIATIONS

3.1 Definitions

3.1.1 Authorization: The granting of rights, which includes the granting of access based on access rights. [X.800]

3.1.2 Authentication:

3.1.2.1 Data Origin Authentication: The corroboration that the source of data received is as claimed. [X.800]

3.1.2.2 Peer Entity Authentication: The corroboration that a peer entity in an association is the one claimed. [X.800]

3.1.3 Authentication Service: A security service that verifies an identity claimed by or for an entity.

NOTE -- In a network, there are two general forms of authentication service: *data origin authentication service* and *peer entity authentication service*. [X.800]

3.1.4 Confidentiality: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes. [X.800]

3.1.5 Data Confidentiality Service: A security service that protects data against unauthorized disclosure. (See: *data confidentiality*.)

3.1.6 Data Integrity: The property that data has not been altered or destroyed in an unauthorized manner. [X.800]

3.1.7 Data Integrity Service: A security service that protects against unauthorized changes to data, including both intentional change or destruction and accidental change or loss, by ensuring that changes to data are detectable. See Section 6.6.

3.1.8 Data origin authentication: The corroboration that the source of data received is as claimed. [X.800]

3.1.9 End-user security plane: End-user security plane addresses security of access and 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 such as VPNs, or they may use it to access network-based applications.

[4] This document is available from ftp://ftp.rfc-editor.org/in-notes/rfc3830.txt

[5] This document is available from < ftp://ftp.rfc-editor.org/in-notes/rfc2327.txt.

[6] This document is available from the International Telecommunications Union. < http://www.itu.int/ITU-T/ >

[7] The *ATIS Telecom Glossary 2007* is available online at < http://www.atis.org/glossary/ >.

3.1.10 Peer-entity authentication: The corroboration that a peer entity in an association is the one claimed. [X.800]

3.1.11 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. [X.800]

3.1.12 User: A person or a machine delegated by a customer to use the services and/or facilities of a telecommunications network. [ITU-T Rec. I.112]

3.1.13 User Plane (UP): A classification for objects whose principal function is to provide transfer of end user information: user information may be user- to- user content (e.g., a movie), or private user- to-user data. [ITU-T Rec. G.993.1]

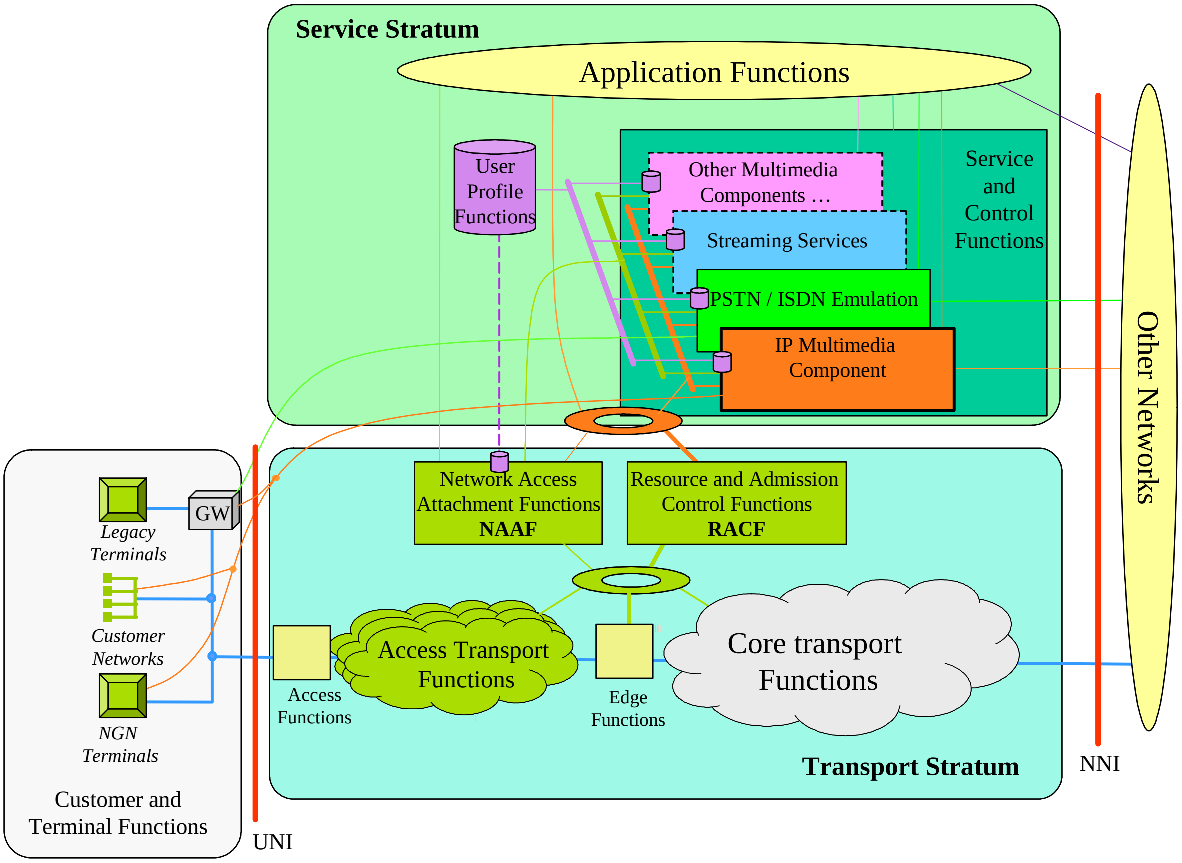
3.2 Acronyms & Abbreviations

3DES	Triple DES
3GPP	3rd Generation Partnership Project
AES	Advanced Encryption Standard
AES-128	Advanced Encryption Standard with 128 bit key
AES-192	Advanced Encryption Standard with 192 bit key
AES-256	Advanced Encryption Standard with 256 bit key
ALG	Application Level Gateway
ANSI	American National Standards Institute
API	Application Programming Interface
ATIS	Alliance for Telecommunications Industry Solutions
CALEA	Communications Assistance for Law Enforcement Act of 1994
CBC	Cipher Block Chaining mode (an AES mode of operation)
CC	Common Criteria for Information Technology Security
CCRA	Common Criteria Recognition Agreement
CEM	Common Evaluation Methodology
CFB	Cipher Feedback mode (An AES mode of operation)
CM	Counter Mode (an AES mode of operation)
CMVP	Cryptographic Module Validation Program
CNRI	Corporation for National Research Initiatives
DES	Data Encryption Standard
EAL	Evaluated Assurance Level
EAP	Extensible Authentication Protocol
EAP-TTLS	EAP-Tunneled Transport Layer Security
ECB	Electronic Codebook mode (an AES mode of operation)
ECC	Elliptic Curve Cryptography
ECDLP	Elliptic Curve Discrete Logarithm Problem
ETS	Emergency Telecommunications Service
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act

GETS	Government Emergency Telecommunications Service
HIPPA	Health Information Privacy and Portably Act
HMAC	Keyed-Hash Message Authentication Code
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPsec	IP Security protocol
ISO	International Organization for Standardization
IT	Information Technology
IV	Initialization Vector
LAN	Local Area Network
LEA	Law Enforcement Access
MIKEY	Multimedia Internet Keying
NAT	Network Address Translation
NGN	Next Generation Network
NS/EP	National Security / Emergency Preparedness
OECD	Organization for Economic Co-Operation and Development
OFB	Output Feedback mode (an AES mode of operation)
OTP	One-Time Pad
PEAP	Protected EAP
PIN	Personal Identification Number
PKCS	Public-Key Cryptography Standard
PKI	Public-Key Infrastructure
PSTN	Public Switched Telephone Network
QoE	Quality of Experience
QoS	Quality of Service
RSA	Rivest Shamir Adelman (encryption algorithm)
RTP	Real-time Transport Protocol
SDP	Session Description Protocol
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SIP	Session Initiation Protocol
SRTCP	Secure RTP Control Protocol
SRTP	Secure Real-time Transport Protocol
SVZ	Secure VoIP Zone
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
TLS	Transport Layer Security
UDP	User Datagram Protocol
VLAN	Virtual LAN
VoIP	Voice over IP
VPN	Virtual Private Network
WLAN	Wireless LAN
XIWT	Cross-Industry Working Team

5 Reference Network Model and Architecture

The Network Model and Architecture shown in the following diagram was used in the production of this TR. Other Network models may be used, as appropriate, to illustrate different aspects of network security.



Source: ITU-T SG 13's FGNGN OD-00132

6 Security Topics

This section will discuss general security topics related to Next Generation Networks (NGNs).

6.1 Authentication

Authentication for user plane security is a critical feature for NGNs. An authentication process consists of two steps:

1. *Identification step*: Presenting an identifier to the security system. (Identifiers should be assigned carefully, because authenticated identities are the basis for other security services, such as access control service.)
2. *Verification step*: Presenting or generating authentication information that corroborates the binding between the entity and the identifier.

Authentication can apply at various levels -- e.g., at the device level and at the user level. In a network, there are two general forms of authentication service: 1) *data origin authentication service*, and 2) *peer entity authentication service*. [X.800]

Authentication applies at the device level, as well as the user level. Appropriate authentication technology should be applied in all instances.

Different authentication mechanisms exist and can be designed to use one or more authentication mechanisms. Two examples follow:

1. Authentication of calls/sessions originating in an NGN network can be achieved by calling a special number and entering a personal identification number (PIN) before the call or session can continue.
2. Authentication can be achieved by the NGN system's recognition of the preferential users' equipment. This authentication may only be available on particular pieces of equipment (e.g., phones, modems) and may additionally require further mechanisms (e.g., smartcards, tokens).

Care should be taken not confuse authentication with authorization. Authorization is addressed in 6.2.

Increased security can be achieved through the use of *two* or three *factor authentication*. *Two factor authentication* refers to the use of something that is known and something that is possessed -- for example, a bank card and PIN. The PIN is the thing that is known, and the card is the thing that is possessed. *Three factor authentication* augments two factor authentication with the additional factor of something that is intrinsic to a person -- for example, biometric information provided through a reader.

6.1.1 Device Level Authentication

Device level authentication involves validating that the device is allowed to attach to the network and receive service. Device authentication in the context of 802.1x wireless access authentication is discussed in 6.15.

6.1.2 User Level Authentication

User level authentication involves validating that the user is allowed to make use of the network and receive service.

How User Level Authentication may be achieved using authentication technology or tokens is addressed in 6.9.3, *Authentication Card Interfaces*.

6.1.3 GETS Authentication

The telecommunication infrastructure is rapidly evolving to an IP-based technology. There is a need to provide authentication for Emergency Telecommunications Service (ETS) users in multiple service domains. As service providers migrate to IP-based networks and start to provide services, they should be capable of providing security functionalities for Government Emergency Telecommunications Service (GETS) as well as future ETS services.

Currently, using the Public Switched Telecommunication Networks (PSTN), authorized emergency users (e.g., , NS/EP community) can make GETS calls almost anywhere during disaster events such as hurricanes, earthquakes, floods, and terrorist attacks. GETS is a prescribed service. Before emergency users can initiate a GETS call, they have to be authenticated by authorized inter-exchange carriers. Once the authentication process is successfully completed, users can communicate into, out of, and within the disaster areas when facilities are available.

NGN will have to address authentication both for GETS and for the newer ETS services on IP-based networks.

6.2 Access Control/Authorization

Access Control, also called *Authorization*, should not be confused with authentication, which is addressed in 6.1. Authorization allows a mediated access to the correct services. Authenticated users or devices can be granted access privileges, which allow controlled access to appropriate assets, services, and features. Within the VoIP space, authorization can control the services and features that are made available to authenticated users and authenticated end sets. Authorization requires that access to information resources may be controlled by or for the target system.

6.3 Non-repudiation

Non-repudiation as used in this document is defined in the digital signature sense: non-repudiation, when offered as a service, provides proof of the integrity and either origin of data or receipt of data, both in an un-forgeable relationship, which can be verified by any third party at any time; or, when used in the context of authentication, provides an authentication that with high assurance can be asserted to be genuine, and that can not subsequently be refuted.

6.4 Audit Logging

Audit logs are created to allow for the incident post-mortems and resulting investigation. They are also required to support repudiation services.

For a detailed discussion on audit logging, see T1.276-2003 [3].

6.5 Data Confidentiality and Privacy

Additional security requirements are usually placed on the user plane due to the nature of IP traffic.. Requirements need to be based on the premise of achieving, at a minimum, the same level of security that would be provided by a legacy TDM system.

In developing the analogy with the legacy system, consideration must be given to whether the user is trying to achieve a limited level of 'privacy' for the session or requires a higher level of security that provides 'confidentiality' of the content.

While users and enterprises often will express the need for 'security' of the voice traffic or secure VoIP, they will not differentiate between confidentiality, privacy, and other security services. They will state their requirement as 'security' or 'encryption'. In the case of security of the user channel, when questioned, the user wants the same level of privacy that was present on a legacy system. Legacy systems offer no formal confidentiality mechanisms; they only offer a level of privacy implicit in their point-to-point local loop design.

Confidentiality implies a degree of 'back traffic' (i.e., stored encrypted traffic) protection -- the encrypted traffic will resist brute force attack for specified number of years. Conversely, privacy does not provide any degree of 'back traffic' protection; it refers more to the rights of individuals and organizations to control the collection, storage, and dissemination of their information or information about themselves. Unlike *confidentiality*, which has a weak legal definition, *privacy* is defined by the Organization for Economic Co-Operation and Development (OECD) < http://www.oecd.org >. The European Union and numerous national laws.

Care must be taken to ensure that those users' security requirements are understood; whether they require 'confidentiality' or they actually require 'privacy' equivalent to a TDM network. The User-Network and Network-Network Interfaces will provide for both privacy enhancing technologies as well as more formal confidentiality technologies based on the user requirement. These confidentiality technologies will meet FIPS 140-2 as discussed in 6.10; however, privacy-enhancing technologies will just provide various degrees of privacy protection.

6.5.1 Contrasting Data Confidentiality and Privacy

Confidentiality is perhaps the most confusing term in the information security community. It is a:

- *Label for data*: "This document is confidential";
- *Security service*: "Confidentiality is provided by cryptography"; or
- *Security policy*: "This information will be treated as confidential."

More formally, the definition is given as assurance that information is not disclosed to unauthorized entities or processes.

Many individuals when speaking about security are referring indirectly to confidentiality. They may also use the term 'encryption,' or as discussed previously 'privacy.' Strictly speaking, confidentiality -- with its requirement to protect the information long after the information interchange has completed is a limited requirement for the VoIP space. Most telephone calls are less than three (3) minutes in length, with a requirement for protection of the contents of the bearer path for a very short duration. In these cases, the needed level of confidentiality can be provided by privacy-enhancing technologies instead of cryptography.

Privacy and Data Confidentiality are terms often confused by the popular press and used as synonyms by some well-meaning technical documentation. It is proposed that in this context the definitions for privacy, as defined by the ATIS-0100523.2007, *ATIS Telecom Glossary 2007*, be used. ATIS-0100523.2007 [8] defines privacy as:

> **privacy**: 1. In a communications system or network, the protection given to information to conceal it from unauthorized persons having access to the system or network at large. *Synonym* segregation. 2. In a communications system, protection given to unclassified information, such as radio transmissions of law enforcement personnel, that requires safeguarding from unauthorized persons. 3. In a communications system, the protection given to prevent unauthorized disclosure of the information in the system. *Note 1*: The required protection may be accomplished by various means, such as by communications security measures and by directives to operating personnel. *Note 2*: The limited protection given certain voice and data transmissions by commercial crypto equipment is sufficient to deter a casual listener, but cannot withstand a competent cryptanalytic attack. 4. 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 [7498-2].

The term *privacy enhancing technologies* means by inference, technologies that limit surveillance. Similarly, the term *data confidentiality mechanisms* are technologies that provide for maintaining the confidentiality of data. It should be also noted that encryption is a data confidentiality mechanism, but it is not the only data confidentiality mechanism. Many times the term *encryption* is used colloquially to refer to a broad class of data confidentiality mechanisms.

The distinction must be made since new legislation requirements such as the Health Information Privacy and Portably Act (HIPPA) require both privacy enhancing technologies as well as data confidentiality mechanisms.

6.5.2 Data Confidentiality Requirements for the User Plane

In order to achieve at least the same level of data confidentiality protection that is present in TDM systems, NGN must implement services which ensure data confidentiality. These mechanisms must ensure that the information in a Network system and transmitted information is accessible for reading or modification only by authorized parties. These confidentiality mechanisms must also provide an appropriate level of "back-traffic" (i.e., stored encrypted traffic) protection that will protect the information for the desired length of time.

In order to validate that the algorithm used is properly implemented, both the algorithm and its implementation must be FIPS 140-2 validated.

6.6 Data Integrity

Data integrity is a requirement of the user plane. Integrity is often confused with confidentiality, as some levels of integrity can be provided indirectly with confidentiality. Integrity is a security feature that provides protection against undetected unauthorized modification of information. Integrity can provide assurance that given information has not been modified. Data integrity ensures that information held in a system is a proper representation of the information intended, and has not been accidentally or maliciously altered or destroyed.

A data integrity service can only detect a change and report it to an appropriate system entity. However, a system that offers data integrity service might also attempt to correct and recover from changes.

A close relationship between data integrity service and authentication services exists. Although data integrity service is defined separately from data origin authentication service and peer entity authentication service, it is closely related to them. Authentication services depend, by definition, on companion data integrity services. Data origin authentication service provides verification that the identity of the original source of a received data unit is as claimed; there can be no such verification if the data unit has been altered. Peer entity authentication service provides verification that the identity of a peer entity in a current association is as claimed; there can be no such verification if the claimed identity has been altered. [1]

6.7 Availability

Availability is a characteristic present both in reliability and information security. As an information security characteristic, availability ensures the computer, network, database, and information resources will be available to authorized users when they need them. It is sometimes called *timeliness of service*, which is defined as the correct resource being made available within a prescribed length of time to a properly authorized and authenticated user. Availability from an information security perspective in VoIP space protects against attacks like denial of service (DoS) as well as helping ensure that critical calls get through (e.g., 9-1-1). Availability is also an important factor in overall network performance.

- ♦ Availability is used to define the security services intended to assure that system assets are available, work promptly, and service is not denied to authorized parties. In the event of a security breach, disrupted operations must be restored in a timely manner.

6.8 Law Enforcement Access

User plane security mechanisms such as confidentiality and privacy enhancing technologies introduce challenges in providing effective Law Enforcement Access (LEA). This section will discuss this issue, and present recommendations to ensure that the requirements of warranted access can be met.

In many nations worldwide, there is a requirement to provide effective LEA after due process is followed (warrant, etc.). Converged networks and VoIP introduces additional challenges for telecommunications equipment manufacturers and carriers to comply with these national requirements. Consideration must be given as to how to provide access when required by legal authority. When carrier-provided security services extend confidentiality to the handset, two options to achieve LEA exist, viz.

1. The key to decrypt the message traffic must be retrievable or provided along with the message to law enforcement.
2. Decrypted traffic is provided directly to law enforcement.

NOTE -- When the customer terminals provide the encryption and the customer generates the encryption keys, the carrier is not in a position to make available the encryption keys to the law enforcement agency and can only pass the encrypted data stream.

The two preferred options for providing this decrypted traffic are:

1. *All confidentiality mechanisms between the handset and the call server will be terminated at the call server*. This allows the call server to forward the message traffic unencrypted to law enforcement personnel. To ensure that the traffic is protected beyond the call server, the call server may re-encrypt the data stream before forwarding.
2. *The call server, when appropriately configured causes the phone to route all RTP traffic to both the call server and the called party*. This allows the call server to forward the message traffic unencrypted to law enforcement personnel.

In the United States, in October 1994, the United States Congress took action to protect public safety and ensure national security by enacting the Communications Assistance for Law Enforcement Act of 1994 (CALEA), Pub. L. No. 103-414, 108 Stat. 4279. The law further defines the existing statutory obligation of telecommunications carriers to assist Law Enforcement in executing electronic surveillance pursuant to court order or other lawful authorization. The objective of CALEA implementation is to preserve Law Enforcement's ability to conduct lawfully-authorized electronic surveillance while preserving public safety, the public's right to privacy, and the telecommunications industry's competitiveness. CALEA implementation responsibilities are delegated to the Federal Bureau of Investigation by the Attorney General at 28 C.F.R. § 0.85(o). Since its enactment, CALEA concepts have now been adopted by other nations, most notably Canada and the European Union.

The applicability of CALEA to NGN VoIP Systems is currently under review by the United States Federal Communications Commission. Under a Notice of Proposed Rule Making (FCC Docket 97-213 Report and Order), the FCC is proposing extending CALEA to VoIP systems.

6.9 Cryptography

6.9.1 Algorithms

The section will provide guidance regarding cryptographic algorithms, key length, cryptographic modes, and random number generators. This recommendation will be based on the supporting the needs of the security mechanisms in providing the needed security functionality to secure the user plane.

6.9.1.1 AES

The Advanced Encryption Standard (AES) is specified in FIPS-197. This standard specifies a FIPS-approved symmetric encryption algorithm that may be used by U.S. Government organizations (and others) to protect unclassified but sensitive information. The AES algorithm is a symmetric block cipher that can process data blocks of 128 bits, using cipher keys with lengths of 128, 192, and 256 bits. These different "flavors" are referred to as "AES-128", "AES-192", and "AES-256".

The modes of operation of AES are:

- Electronic Codebook Mode (ECB)
- Cipher Block Chaining Mode (CBC)
- Cipher Feedback Mode (CFB). CFB variants supported are:
- (CBF1, CBF8, CBF128), where the length of the data segment is s bit, s=1, s=8 or s=128)
- Output Feedback Mode (OFB)
- Counter Mode (CM)

Counter Mode of AES is Mandatory for SRTP.

6.9.1.2 ECC

Elliptic Curve Cryptography (ECC) is a new method of performing public-key cryptography comparable to the existing RSA encryption algorithm. With ECC, an elliptic curve is defined over a certain field and then the elliptic curve discrete logarithm problem (ECDLP) is solved over this field. The main advantage of ECC as compared to other public-key algorithms is key size. An ECC key of 160-bits is roughly equivalent in security to a 1024-bit RSA key, and a 210-bit ECC key is roughly equivalent to a 2048-bit RSA. The smaller ECC key results in less computational overhead and a more efficient cryptosystem.

NOTE -- ECC and RSA are typically used in the key-management functions and peer-entity authentication, and not for encrypting bulk data.

6.9.2 APIs/Abstraction Layers

To support the needs of various jurisdictions and to encourage the use of standard cryptographic implementations this section will explore the use of cryptographic abstraction layers or APIs.

6.9.2.1 RSA Public Key Crypto Standards

The RSA Public Key Crypto Standards outline the protocols and formats for the use of cryptographic tokens to support these interchange of security credentials and the use of different types of crypto logic. In particular:

- ♦ *PKCS #10*: *The certification request standard*. This defines a methodology and format for requesting the generation of X.509v3 digital certificates by a Certificate Authority within a Public Key Infrastructure (PKI).
- ♦ *PKCS # 11*: *The cryptographic token interface standard.* This defines a technology-independent programming interface for cryptographic devices such as smartcards.
- ♦ *PKCS # 12*: *The personal information exchange syntax standard.* This describes a portable format for storage and transportation of user private keys, certificates, etc.
- ♦ *PKCS # 15*: *The cryptographic token information format standard.* This describes a standard for the format of cryptographic credentials stored on cryptographic tokens.

6.9.3 Authentication Card Interfaces

The use of Smart Cards and other similar tokens are being proposed for providing two-factor authentication (something you know, something you have). Recommendations will need to be developed for the use of authentication cards and an appropriate interface.

6.10 User Plane Assurance

There is a growing requirement to have third party assurance that the security features and mechanisms in network elements are correctly implemented, and provide the requisite level of protection. Formal programs have been established to provide this level of assurance or trust in the security features and the functionality of products.

6.10.1 Cryptographic Module Certification

In 1995, The National Institute of Standards and Technology of the U.S. Government and the Communications Security Establishment of the Government of Canada established the Cryptographic Module Validation Program (CMVP). This program, which makes use of third party accredited laboratories, validates cryptographic modules as meeting the requirements of FIPS 140-2 Security Requirements for Cryptographic Modules.

The Federal Information Security Management Act (FISMA) (Public Law 107–347) requires that all Federal agencies and their contractors use only those cryptographic-based security systems that were validated to FIPS 140–2 or to its predecessor, FIPS 140–1.

FIPS 140–2 identifies requirements for four increasing, qualitative levels of security for cryptographic modules. The four security levels cover a wide range of potential applications and a wide spectrum of information types, including data with the potential to cause low, moderate and serious impacts on organizations should there be a loss of confidentiality, integrity, or availability of the data.

It may be advantageous that devices built to secure the user-network interface and the network-network interface be validated to FIPS 140-2 Level 2.

6.10.2 Common Criteria for IT Security Certification

Since the unfortunate events of 9/11, an increased focus on the security of information systems and critical information infrastructure has developed. Individuals, organizations, and governments want to know if they can trust the claims that manufacturers make on the strength of their security products. They are looking for a level of assurance or trust that the security features and mechanisms are correct, and that the products have no hidden vulnerabilities or malicious code.

Fortunately, a standard and conformance test exists to assess the level of assurance in IT products. In 1992, Canada, France, Germany, the Netherlands, the United Kingdom, and the United States embarked on a project to develop computer security criteria that would allow the assessment of the degree of trust or assurance in an IT product. The Common Criteria for Information Technology Security (CC) was born from this effort. Together with the Common Evaluation Methodology (CEM), they form an internationally accepted means to specify and measure the assurance present in an IT product. The formal acceptance of products evaluated under the CEM to the CC is specified in the Common Criteria Recognition Agreement (CCRA).

The multipart Common Criteria achieved its goal of becoming an ISO standard – it is now ISO/IEC 15408. An additional 14 countries have now signed the CCRA.

In recent months, industry groups have begun adopting the Common Criteria and require certification to the standard for products being used in their vertical markets. These groups include the U.S. Department of Defense and the Financial Services Roundtable. Other industry associations, such as the U.S. Process Control Industry and the North American Electric Reliability Council, are considering its adoption. In Europe, Asia, and Australia, similar trends have been identified. The most significant efforts have been under the U.S. Department of Defense. The Common Criteria is mandatory for all information equipment acquired by the department and allied intelligence agencies. BITS group of the Financial Services Roundtable – which represents the major U.S. Financial Institutions – has recently adopted the Common Criteria, and is aligning its product certification process with it. This will require a Common Criteria evaluation on all information equipment within the U.S. Financial Services sector.

The CC provides a Common structure and language for expressing product/system IT security requirements, as well as a catalog of standardized IT security requirement components and packages. With this language and catalogue, two different specifications can be developed that specify IT security requirements and specifications for products and systems, namely 1) *Security Targets*, and 2) *Protection Profiles*.

A Security Target is a product-specific statement of the security requirements, policies, and environment assumptions; in contrast, a *Protection Profile* is a specification of security requirements, polices, and environment assumptions for a product family or class of products (i.e., , Firewalls, VPN, etc.).

The formal specifications provided by a protection profile and Security Target allow third-party evaluators to certify products and systems as meeting specific security requirements.

An appropriate Protection Profile (PP) for User Plane Security should be developed. It is recommended that once the standards addressing the User-Network Interface and the Network-Network Interface for User Plane Security are complete, corresponding PPs should be developed. These PPs will allow Common Criteria Certification of products to confirm that they are conformant to the User-Network Interface and the Network-Network Interface for User Plane Security. Similarly, PPs should be developed for ANSI Standard T1.276-2003 (Reference [3]), and the evolving signaling security standards under development in ATIS PTSC.

This evolution is shown graphically in Figure 1 below.

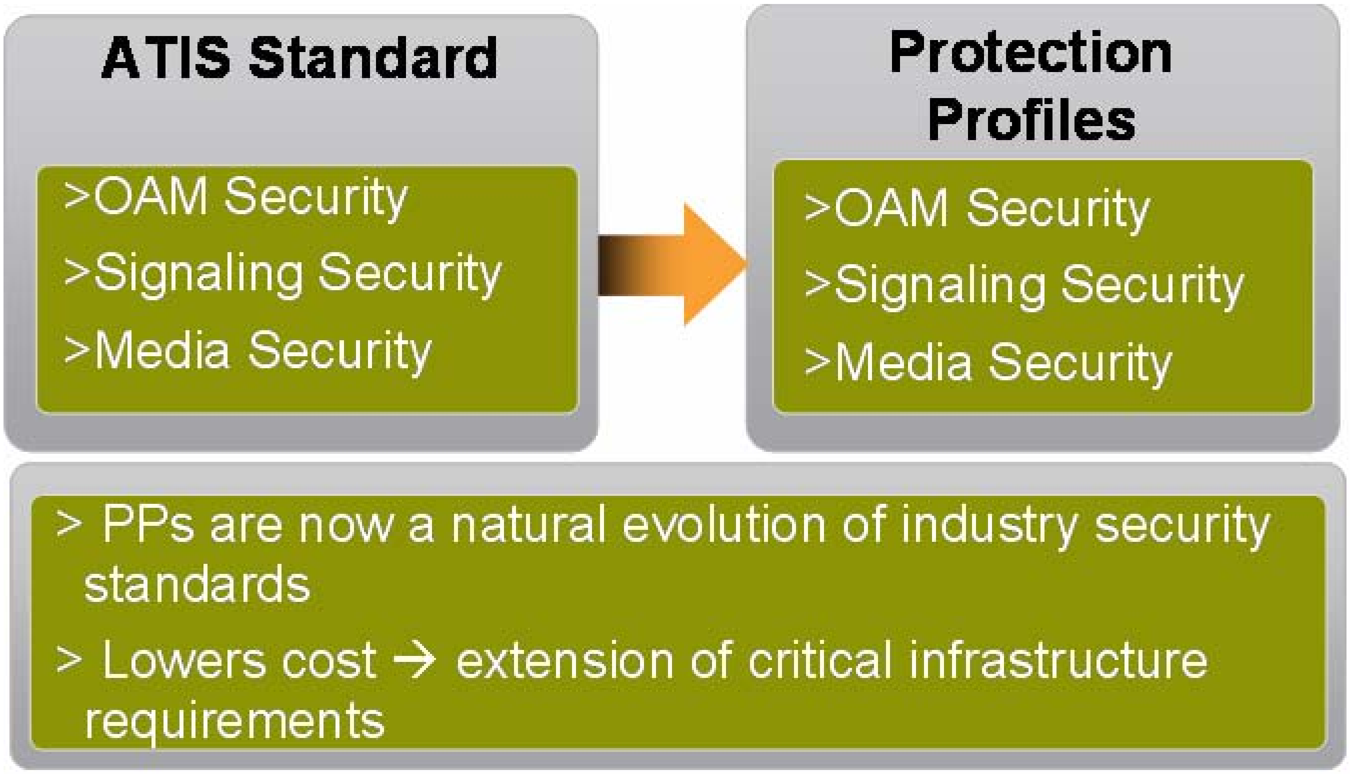

ATIS Standard
>OAM Security
>Signaling Security
>Media Security
Protection Profiles
>OAM Security
>Signaling Security
>Media Security
> PPs are now a natural evolution of industry security standards
> Lowers cost → extension of critical infrastructure requirements

Figure 1 - Evolution of Security Protection Profiles

CC Certified products are awarded an "Evaluated Assurance Level (EAL)" from 1 to 7, depending on the rigor of the evaluation to which it was subjected. It is expected that a recommended value of EAL-2 will be the target for User-Network Interface and Network-Network Interface User Plane Security products.

CC certifications provide well-defined IT security requirements and security specifications; these describe the types of security features that customers want. As well, CC certifications providing quality security metrics with appropriate testing, evaluation, and assessment procedures can provide assurance that the customer will receive what was asked for.

6.11 Quality of Experience/Quality of Service Related Aspects

The selection of security mechanisms and features must consider the Quality of Experience (QoE) and Quality of Service (QoS) targets of the system. Issues related to the length of time to establish security associations and cryptographic overhead may reduce the effective throughput of the system. Also, encryption of the packet payload may prevent deep packet inspect necessary to provide priority service. Line errors may impact the performance of cryptographic systems.

IPsec, the security mechanisms of choice for data networks, is proposed by many to meet the needs of user plane security. This section will provide information on the selection of appropriate mechanisms to ensure that QoE and QoS targets are achievable which is especially significant for the user plane.

6.12 Media Protocols

The section will provide information on appropriate security protocols to provide security mechanisms and services to secure the user plane. The following sections discuss key protocols and issues that have been identified. Additional protocols or issues may be added as the development of these standard progresses.

6.13 Secure Real-time Transport Protocol (SRTP)

SRTP [RFC3711] is an RTP [RFC3550] profile that provides the following security services: encryption, message integrity, and replay protection. The SRTP profile is an extension to the RTP audio/video profile [RFC3551]. Similar to TLS for secure http, SRTP has several interesting properties that make it more attractive than IPsec as the RTP security encapsulation protocol. IPsec encryption transformations result in a significant amount of per-packet overhead: a sequence number (4 or 8 octets) for replay protection and -- depending on the encryption algorithm (including 3DES-CBC and AES-CBC) -- an Initialization Vector (IV), with variable length of 8 octets for 3DES-CBC and 16 octets for AES-CBC-128, are part of an IPsec packet.

SRTP defines AES-counter mode (CM) as the mandatory encryption transform, making it easier to implement efficiently in hardware. The counter used for AES-CM is based on the RTP sequence counter, and hence does not add to the per-packet overhead. Furthermore, the counter also offers replay protection. Another significant advantage of SRTP is that only the RTP payload is encrypted, keeping the UDP and RTP headers in the clear. In some networks, this is helpful for QoS engineering. Furthermore, SRTP (unlike IPsec) would allow for RTP header compression mechanisms to continue to work.

Secure RTCP (SRTCP) provides the same security services to RTCP as SRTP does to RTP. SRTCP message authentication is **mandatory**; it protects the RTCP fields that keep track of membership, provide feedback to RTP senders, or maintain packet sequence counters. Without integrity protection, an adversary may inject RTCP packets (e.g., RTCP BYE messages) to close RTP sessions and cause Denial of Service (DoS).

However it should be noted that the use of SRTP and SRTCP may have an impact on a service provider’s ability to comply with CALEA. This depends upon how these protocols are implemented.

6.14 Key Management for SRTP

An IETF standard for SRTP key management called Multimedia Internet Keying (Mikey) is currently available. [4] In addition, other key management protocols are being proposed as extensions to the Session Description Protocol (SDP). SDP is currently used for describing multimedia sessions for the purposes of session announcement, session invitation, and other forms of multimedia session initiation. [5]

6.15 802.1x

The concept of IEEE 802.1x is to provide a standardized security authentication method for IEEE 802 based network technologies, including Local Area Networks (LANs) and Wireless LANs (WLANs). It does not preclude the use of higher layer authentication methods; in fact, these are usually complementary.

VoIP technology requires the same level of reliability as the PSTN to ensure that services will not be interrupted or compromised. The VoIP service can only be achieved by strongly authenticating every element in the VoIP system.

IEEE's 802.1X is a standardized method for securing network access of network devices. Many vendors have implemented proprietary solutions for securing network access. Each control provides a particular advantage that is often unique to each vendor. By adopting 802.1X for network access, using a standard based approach, interoperability across multiple vendors is enabled.

802.1X is a data link layer transport that defines wireless and physical networks port-access control standards. The Extensible Authentication Protocol (EAP) is used to carry authentication credentials. Within this framework, port access refers to 'user port' access controlled by a wireless access point or wired switch. Users do not get IP-connectivity until they have successfully authenticated.

In IEEE 802.1X-2004, an Authenticator establishes a dialog with a single Supplicant in order to establish its credentials. It prevents unauthorized access by supplicants to the services offered by the system. Access control is achieved by the system enforcing authentication of supplicants that attach to the Authenticator's controlled ports. In a port-access control, the authentication occurs at the edge rather than in the core of the LAN.

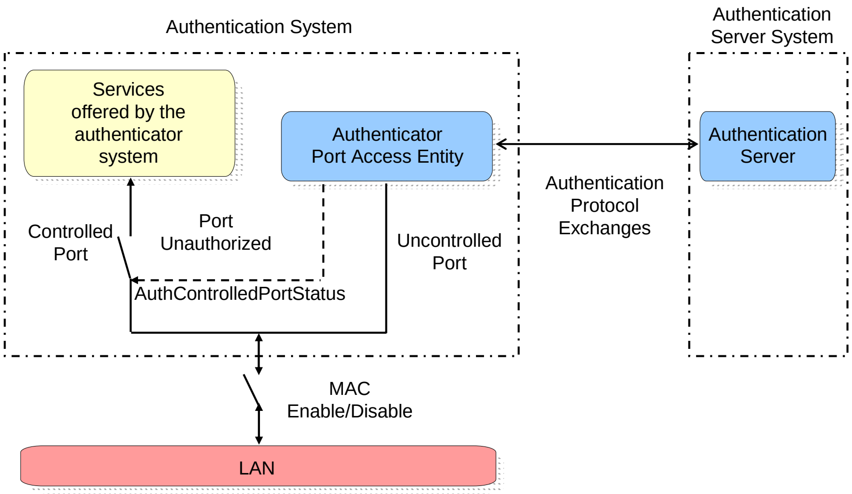

Authentication System
Authentication Server System
Services offered by the authenticator system
Authenticator Port Access Entity
Authentication Server
Authentication Protocol Exchanges
Controlled Port
Port Unauthorized
Uncontrolled Port
AuthControlledPortStatus
MAC Enable/Disable
LAN

Figure 2 - Port-based Access Control

Authentication occurs when a Supplicant is connected to an Authenticator's port. Until authentication has been successfully completed, the Supplicant only has access to the Authenticator to perform authentication exchanges. Depending on the result of the authentication process, the Authenticator can determine whether or not the Supplicant is authorized to access its services on that controlled port. A possible outcome is that when the supplicant is successfully authenticated, its traffic is directed to a particular virtual LAN (VLAN). If the Supplicant is not authorized for access, the Authenticator sets the controlled port state to "unauthorized." In the unauthorized state, the use of the controlled port is restricted, thus preventing unauthorized data transfer between the Supplicant and the services offered by the Authenticator. In order to perform the authentication, the Authenticator makes use of an Authentication Server.

Secure user authentication is obtained through the encrypted exchange of the user's security credentials or challenges. *Security Credentials* are used in this context to mean something that the Authentication Server knows about a particular user or device, for example the knowledge of a valid user name, password, token, PIN, a challenge -- or in the case of a device authentication -- the device ID.

The process of authenticating a user or device involves the following:

1. The Supplicant is an entity at one end of a point-to-point LAN segment that is being authenticated by an Authenticator attached to the other end of that link.
2. The Authenticator is an entity at one end of a point-to-point LAN segment that enables authentication of the entity attached to the other end of that link, the Supplicant.
3. The 802.1X port-based network access control protocol provides the means to authenticate and authorize devices attached to a LAN port that has point-to-point connection characteristics; it can also prevent access to that port in cases in which the authentication and authorization process fails.
4. An EAP authentication method (such as EAP-TLS, EAP-TTLS, EAP-PEAP, etc.), that provides specific authentication mechanisms between the client and the authentication server. The choice of method often implies a choice of mechanisms.
5. An authentication mechanism such as one-time passwords, token cards, biometrics, Kerberos, pre-shared keys, or digital signatures, that authenticates a client or supplicant.
6. An authentication server that performs the authentication function necessary to check the credentials of the Supplicant on behalf of the Authenticator, and indicates whether the Supplicant is authorized to access the Authenticator's services.

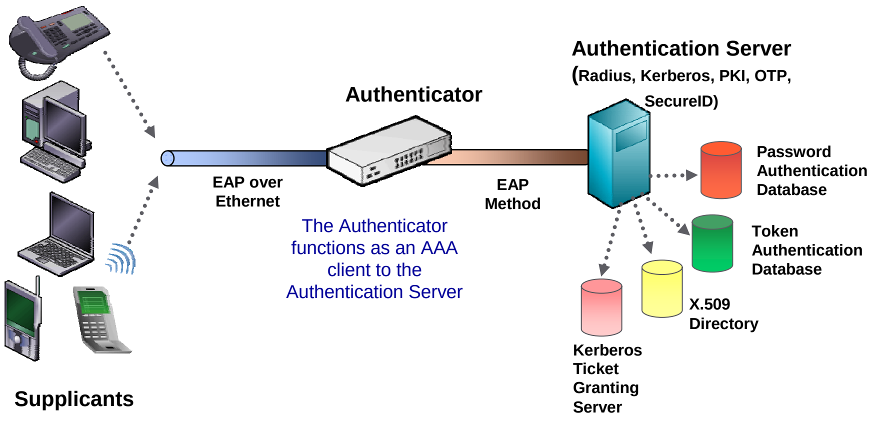

Authentication Server
(Radius, Kerberos, PKI, OTP, SecureID)
Authenticator
Password Authentication Database
EAP over Ethernet
EAP Method
The Authenticator functions as an AAA client to the Authentication Server
Token Authentication Database
X.509 Directory
Kerberos Ticket Granting Server
Supplicants

Figure 3 - Authentication Process

802.1x EAP use to authenticate VoIP endpoints to the network should be considered.

6.16 Mobility and Nomadicity

Nomadicity is the name used by the Cross-Industry Working Team (XIWT) at the Corporation for National Research Initiatives (CNRI) to denote an architecture for the entire mobile computing environment. Nomadicity applies to both wireline and wireless networks. The ITU-T definition is

> **Nomadicity**: Continuity of access between two information infrastructure components as they move in space. [Y.101 (00)].

Nomadicity does not keep application sessions alive whereas mobility does.

6.17 Secure VoIP Zone

There is a need for a Secure VoIP Zone (SVZ), since all VoIP servers are vulnerable to attacks (malicious or otherwise) from within the enterprise as well as from outside. To secure these critical servers and ensure voice is highly available, a stateful firewall with SIP and/or H.323 protocol support is needed. The SVZ firewall must run a stateful inspection engine and act as an application level gateway (ALG) to provide extensive support for H.323 and/or SIP protocols. Until such time as the NGN itself is secure, secure VoIP zones will need to be established on a customer's network.

By definition, *Stateful Packet inspection firewalls* are based on the filtering of packets at the network level. These firewalls examine protocol packet header fields: source IP address, destination IP address, TCP/UDP source ports, and TCP/UDP destination ports. They are 'stateful' because the firewall can remember prior connection states, and continuously updates this information in dynamic connection tables. The firewall evaluates subsequent transactions against prior connection histories.

A stateful inspection firewall usually has :

- A policy database and lookup engine.
- A connection table which has source port, source IP, destination port, destination IP, protocol, history/state of the connection, and other fields.

As each packet arrives at the firewall, it is checked against the connection table to determine whether it is part of an existing connection. The theory is that if the communication has already been authorized, there is no need to authorize it again. The source and destination addresses of the new packet must match the table entry, as well as the source and destination ports. Because there is a 'history' in the state tables, flags are analyzed to ensure the proper sequence in a TCP 3-message handshake for connection setup and teardown. The firewall can drop or reject packets that are not, or which do not appear to be, a genuine response to a request. If the packet belongs to an established connection and everything seems to be in order, it is forwarded. Forwarding based on the connection table rather than reexamining the entire firewall rule set leads to higher throughput performance.

If the incoming TCP packet (for example, an H.323 call control packet) does not appear to match a connection already established, the flags are verified to ensure it is a SYN packet. A TCP ACK without an existing connection table entry is typically dropped. And, of course, if a packet arrives with an inappropriate combination of flags (such as all flags on, all flags off, SYN/FIN, etc.), the packet is dropped. Finally, if the packet has appropriate flags, then it is sent to the policy engine. The policy engine checks the packet and assures that it is destined for an authorized host and an authorized service, and has satisfied any other authentication criterion that has been established. Then, a new table entry is created for that connection.

If the incoming packet is a UDP packet (for example, a SIP or RTP packet), there is no handshake to validate the communication since UDP is stateless in nature; there is no sequence in which the packets must arrive. However, there is a source and destination along with a set of port numbers. An entry is still created in the state table for a UDP connection, based on source and destination IP and ports. Since there are no FIN or RST flags to close the connection, a connection must timeout to be cleared from the connection table.

Apart from stateful inspection, Application Level Gateway (ALG) functionality for SIP and H.323 support is **mandatory**. ALGs are firewall processes that are programmed to understand specific IP protocols, like H.323 and SIP. Rather than simply looking at packet header information to determine if packets can or cannot pass, ALGs go deeper by parsing the data in the packet payload. H.323 and SIP both put critical control information in the payload, such as which data ports the voice endpoint is expecting to use to receive the voice information from the other endpoint in the call. By understanding which ports need opening, the firewall dynamically opens only those ports needed by the application, leaving all others securely closed. This technique of opening small numbers of ports in the firewall dynamically is called *pinholing*.

By opening up ports dynamically for SIP and/or H.323 calls and performing a stateful inspection on packets traversing through it, the firewall provides DoS and protocol attack protection, and a greater level of security to the VoIP servers in the SVZ. This leads to a highly available and more secure service of voice for the enterprise. It is strongly desirable that the firewall also has configurable H.323 and SIP logging options for call logs, setup message logs, registration logs, and reject logs with detailed description.

6.18 VoIP and NAT

Network Address Translation (NAT) may break the end-to-end model of IP routability, encryption, etc., because traditional NATs only modify the Layer 3 addressing (i.e., the source /destination IP address) and do not modify Layer 4-7 addresses embedded within the IP payload. VoIP signaling protocols and RTP/RTCP embed IP addresses at higher layers that traditional NATs do not modify. Therefore, the VoIP signaling and RTP/RTCP may become unreachable after NAT translation (for example, one way signaling and audio) due to the embedded IP address and port which is specified within the IP payload.

For enterprise-hosted VoIP service, NAT may not come into play for trusted enterprise branch sites if all branch sites are part of the organizations intranet or VPN and use the same addressing scheme. However, if an enterprise is making use of NATs for reasons other than VoIP (i.e., , address overlap), ALGs with NAT support must be implemented on the NAT appliance.

With the VoIP NAT ALG enabled, the firewall/NAT will have the ability to look into the Layer 4-7 information within the IP payload and make all the necessary changes to the embedded IP addresses and ports used. This will solve most of the problems associated with VoIP and NAT/Firewall.

However, if there is encryption involved such as IPSec or Transport Layer Security (TLS), and the media and/or the signaling is encrypted, then the ALG feature will not be able to look into the Layer 4-7 information and will not be able to perform the necessary changes to the embedded IP address and ports unless there is decryption and re-encryption performed at the ALGs by sharing/distributing the encryption keys.

7 Concluding Remarks

This TR provides the industry with the description of a set of tools with which a network can secure the user plane traffic over NGNs. It is meant to be a first step to achieving a comprehensive security approach that will include all aspects of IT security. Future standards and TRs are expected to be developed by appropriate SDOs both inside and outside of ATIS and should be consistent with this approach.