International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

M.3016.3

(04/2005)

SERIES M: TELECOMMUNICATION MANAGEMENT, INCLUDING TMN AND NETWORK MAINTENANCE

Telecommunications management network

Security for the management plane: Security mechanism

ITU-T Recommendation M.3016.3

ITU-T M-SERIES RECOMMENDATIONS

TELECOMMUNICATION MANAGEMENT, INCLUDING TMN AND NETWORK MAINTENANCE

Introduction and general principles of maintenance and maintenance organization	M.10–M.299
International transmission systems	M.300–M.559
International telephone circuits	M.560–M.759
Common channel signalling systems	M.760–M.799
International telegraph systems and phototelegraph transmission	M.800–M.899
International leased group and supergroup links	M.900–M.999
International leased circuits	M.1000–M.1099
Mobile telecommunication systems and services	M.1100–M.1199
International public telephone network	M.1200–M.1299
International data transmission systems	M.1300–M.1399
Designations and information exchange	M.1400–M.1999
International transport network	M.2000–M.2999
Telecommunications management network	**M.3000–M.3599**
Integrated services digital networks	M.3600–M.3999
Common channel signalling systems	M.4000–M.4999

For further details, please refer to the list of ITU-T Recommendations.

ITU-T Recommendation M.3016.3

Security for the management plane: Security mechanism

Summary

This Recommendation identifies the security mechanisms for the management plane in the Telecommunications management network. This Recommendation focuses specifically on the security aspect of the management plane for network elements (NE) and management systems (MS), which are part of the Telecommunication infrastructure.

Source

ITU-T Recommendation M.3016.3 was approved on 13 April 2005 by ITU-T Study Group 4 (2005-2008) under the ITU-T Recommendation A.8 procedure.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementors are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database.

© ITU 2005

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

CONTENTS

Introduction

Telecommunications is a critical infrastructure for global communication and economy. Appropriate security for the management functions controlling this infrastructure is essential. Many standards for Telecommunications network management security exist. However, compliance is low and implementations are inconsistent across the various telecommunications equipment and software components. This Recommendation identifies the security mechanisms to allow vendors, agencies, and service providers to implement a secure Telecommunications management infrastructure. Although the present set of security mechanisms represents the current understanding of the state of the art, technologies will advance and conditions will change. To be successful, this Recommendation must evolve as conditions warrant. This Recommendation is intended as a foundation. Service providers may include additional security mechanisms to meet their specific needs over and above those in this Recommendation.

This Recommendation is part of the M.3016.x series of ITU-T Recommendations intended to provide guidance and recommendations for securing the management plane of evolving networks:

ITU-T Rec. M.3016.0 – *Security for the management plane: Overview*.

ITU-T Rec. M.3016.1 – *Security for the management plane: Security requirements*.

ITU-T Rec. M.3016.2 – *Security for the management plane: Security services*.

ITU-T Rec. M.3016.3 – *Security for the management plane: Security mechanism*.

ITU-T Rec. M.3016.4 – *Security for the management plane: Profile proforma*.

ITU-T Recommendation M.3016.3

Security for the management plane: Security mechanism

1 Scope

ITU-T Recs M.3016.1-M.3016.3 specify a set of requirements, services and mechanisms for the appropriate security of the management functions necessary to support the telecommunications infrastructure. Because different administrations and organizations require varying levels of security support, the ITU-T Recs M.3016.1-M.3016.3 do not specify whether a requirement/service/mechanism is mandatory or optional.

This Recommendation identifies the security mechanisms for the management plane in the Telecommunications management network. This Recommendation focuses specifically on the security aspect of the management plane for network elements (NE) and management systems (MS), which are part of the Telecommunication infrastructure.

This Recommendation is generic in nature and does not identify or address the security mechanisms for a specific Telecommunications Management Network (TMN) interface.

The proforma defined in ITU-T Rec. M.3016.4 is provided to assist the organizations, administrations and other national/international organizations, in specifying the mandatory and optional support of the requirements as well as value ranges, values etc., to help implement their security policies.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

– ITU-T Recommendation G.8080/Y.1304 (2001), *Architecture for the Automatically Switched Optical Network (ASON)*, plus Amendment 2 (2005).

– ITU-T Recommendation M.3010 (2000), *Principles for a telecommunications management network*.

– ITU-T Recommendation M.3016.0 (2005), *Security for the management plane: Overview*.

– ITU-T Recommendation M.3016.2 (2005), *Security for the management plane: Security services*.

– ITU-T Recommendation M.3016.3 (2005), *Security for the management plane: Security mechanism*.

– ITU-T Recommendation M.3016.4 (2005), *Security for the management plane: Profile proforma*.

– ITU-T Recommendation X.509 (2000), *Information technology – Open Systems Interconnection: The Directory: Public-key and attribute certificate frameworks,* plus Corrigendum 1 (2001), Corrigendum 2 (2002), and Corrigendum 3 (2004).

– ITU-T Recommendation X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT Applications*, plus Amendment 1 (1996).

– ITU-T Recommendation X.805 (2003), *Security architecture for systems providing end-to-end communications*.

3 Definitions

This Recommendation does not define any new terms.

4 Abbreviations

This Recommendation uses the following abbreviations:

CORBA	Common Object Request Broker Architecture
DoS	Denial of Service
EMS	Element Management System
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPSec	Internet Protocol Security
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
ITU-T	International Telecommunication Union – Telecommunication Standardization Sector
MS	Management System; any EMS, NMS, or OSS[1]
NE	Network Element
NE/MS	NE or MS
NMS	Network Management System
NTP	Network Time Protocol
NTPv3	NTP version 3
OAM&P	Operations, Administration, Maintenance and Provisioning
OS	Operating System
OSS	Operations Support System
RFC	Request for Comments
SAML	Security Assertion Markup Language
SNMP	Simple Network Management Protocol
SNMPv3	Simple Network Management Protocol version 3
SOAP	Simple Object Access Protocol
SSH	Secure Shell
SSL	Secure Socket Layer

[1] OSSs generally can be used in the same context as MSs on any layer of the telecommunications management network hierarchy.

TCP	Transmission Control Protocol
TLS	Transport Layer Security
TMN	Telecommunications Management Network
XML	Extensible Markup Language

5 Conventions

In ITU-T Recs M.3016.1, M.3016.2 and M.3016.3, a descriptor is used to identify the different requirements, services and mechanisms. The descriptor consists of one of the following three-letter label followed by a number:

– REQ for requirement;

– SER for service;

– MEC for mechanism.

6 Security mechanisms

This clause contains the specific security mechanisms for operations, administration, maintenance, and provisioning (OAM&P) and operations support system (OSS) security as they specifically apply to Management Plane security for infrastructure, services, and applications.

Table 1 below is reproduced from ITU-T Rec. M.3016.0 (Table 4 in ITU-T Rec. M.3016.0). This table gives an overview of the relationship between Requirements and Security services, and is used as the basis for organization of the other Recommendations in the series. For example, ITU-T Rec. M.3016.1 discusses the security Functional Requirements, ITU-T Rec. M.3016.2 discusses the Security Services, and this Recommendation (ITU-T Rec. M.3016.3) discusses specific security mechanisms corresponding to the Security Services.

This clause only defines the security services which are covered by standard solutions; other possible services (e.g., detection of denial of service) are left out.

Table 1/M.3016.3 – Mapping of security requirements and security services

Security functional requirement	Security service
Verification of identities	user authentication peer entity authentication data origin authentication
Controlled access and authorization	access control
Protection of confidentiality – stored data	access control confidentiality
Protection of confidentiality – transferred data	confidentiality
Protection of data integrity – stored data	access control
Protection of data integrity – transferred data	integrity
Accountability	non-repudiation
Activity logging	audit trail
Security alarm reporting	security alarm
Security audit	audit trail
Protection of the DCN	packet inspection

Table 2 below outlines the organization of this clause:

Table 2/M.3016.3 – Organization of this clause

Clause	Contents
6.1	Discusses authentication security mechanisms including user authentication, peer entity authentication.
6.2	Discusses data origin authentication.
6.3	Discusses access control security mechanisms.
6.4	Discusses data confidentiality security mechanisms.
6.5	Discusses data integrity security mechanisms.
6.6	Discusses audit trail security mechanisms.

6.1 User authentication

User authentication is the act of verifying a claimed identity of a person. User authentication may be based on security mechanisms which include:

– User ID and password combination (with suitably complex passwords) where the password may be a one time password (e.g., SecureID).

– Multi-factor authentication.

– Single sign-on authentication.

A discussion of user authentication security mechanisms is given in this clause.

6.1.1 User ID and Passwords authentication

User ID and static passwords may be used for user authentication. User authentication involves proving the true identity of the legitimate system user and preventing masquerading by illegitimate imposters. With proper authentication, it is possible to track activities and apply access control to restrict users to pre-authorized activities or roles as discussed in 6.2.

User ID and password authentication involves assigning a unique User ID to each user, and then assigning a suitably complex secret password which is used in combination with the User ID to prove identity.

Passwords should contain enough characters and other randomness to prevent guessing by persons or by machine automated techniques. Examples of characteristics of complex passwords may include such requirements as the following:

MEC 1: Passwords may be required to be a minimum number of characters long (e.g., eight characters).

MEC 2: Passwords may be prevented containing certain characters.

MEC 2a: Passwords may be prevented from including a repeat or the reverse of the associated user ID.

MEC 2b: Passwords may be required not to contain a set of configured character sequences anywhere within them (e.g., words from a dictionary or product names).

MEC 3: Passwords may be required to have no more than a certain number of the same characters used consecutively.

MEC 4: Passwords may be required to contain at least a certain number of lower case and/or upper case alpha characters.

MEC 5: Passwords may be required to contain at least a certain number of numeric characters.

MEC 6: Passwords may be required to contain at least a certain number of special characters.

Administration of passwords is also very important to ensure a secure authentication system. For example the following password system administration capabilities may be desired:

MEC 7: The password administration system may require the entry of the old password to prevent another user from changing a logged-on user's password without their knowledge.

MEC 8: The system may automatically check to ensure that each new login password differs from the previous password. (Because passwords are typically stored via one-way encryption, the entry of the old password may also be required to allow the system to determine the degree of difference between the old and new passwords[2]).

MEC 9: The system may support a password history list to prevent password reuse.

MEC 10: The system may enforce the changing of passwords after certain time intervals.

MEC 11: After a certain number of invalid password attempts, the system may restrict further password attempts for a certain amount of time (e.g., 60 minutes) or force a lock out of users. Locked out users may need to contact security administration personnel to clear the locked out condition.

6.1.2 Multi-factor authentication

Multi-factor authentication refers to an authentication process that requires two or more different types of information or factors to prove identity for user authentication. Requiring multiple factors increases the security of the authentication system by not relying on only a single factor which may be more easily spoofed.

Authentication factors typically used in multi-factor user authentication systems include:

Something the user **knows**:	e.g., knowledge of a secret password or pass phrase.
Something the user **has**:	e.g., token, smart-card, one-time password generator.
Something the user **is**:	e.g., Fingerprint or other biometric measurement.

A common multi-factor authentication mechanism is two-factor authentication, which requires two credentials for authentication. A typical example of two-factor authentication is a bank card system whereby the user must have the card in their possession and also prove knowledge of the secret PIN number associated with the card.

MEC 12: Multi-factor authentication with a specified number of factors.

6.1.3 Single sign-on user authentication

User authentication may support methods for secure single sign-on and X.509 certificate public key infrastructure. In secure single sign-on, the protocol still challenges the entity(s) for credentials; however, a user may not have to enter the credentials because they are securely cached in some way (e.g., Kerberos). Secure single sign-on techniques are used to reduce the necessity of the user having to authenticate to the system multiple times which may become inconvenient.

MEC 13: Single sign-on authentication.

6.2 Peer entity and data origin authentication

Peer entity authentication mechanisms are used to verify claimed identity between peer systems. Data origin authentication security mechanisms are used to ensure that messages are received from

[2] As an exception to one-way encryption, symmetrically encrypted passwords may be used for passwords that need to be decrypted for internal, transient use in trusted system-to-system communication or single sign-on.

the system that claims to have sent them. Peer entity authentication and data origin authentication are closely related, and may be based on security mechanisms which include:

– Cryptographic authentication mechanisms.

– Trusted path authentication mechanisms.

A discussion of these authentication security mechanisms is given in this clause.

6.2.1 Cryptographic authentication

Cryptographic authentication mechanisms provide authentication during data communications between systems (e.g., system-to-system, application-to-application), and is the basis for setting up private communications with full data integrity. During data communications, cryptographic authentication of the sending entity allows the receiver of a message to authenticate the sender's identity (peer entity authentication) and ascertain the origin of the message (data origin authentication). Within a secure communication channel, peer entity and data origin authentication may be based on cryptographic information associated with each message to bind the sending entity's identity to the message. The receiver will check the cryptographic information supplied with the message to verify the true identity of the sending entity.

Cryptographic techniques that can be used for peer entity and data origin authentication include public key encryption, symmetric key encryption, digital signatures, and digital hashing techniques).[3] Cryptographic authentication may be unidirectional where only one end of the conversation is authenticated, or can be bidirectional where both ends are authenticated. Bidirectional authentication is more secure and can be used to help prevent active attacks.

MEC 14: Peer entity and data origin authentication based on public key encryption.

MEC 15: Peer entity and data origin authentication based on symmetric key encryption.

MEC 16: Peer entity and data origin authentication based on digital signatures.

MEC 17: Peer entity and data origin authentication based on digital hashing techniques.

MEC 18: Bidirectional cryptographic authentication.

6.2.2 Trusted path user authentication

Trusted path authentication is a security mechanism whereby any system-to-system authentication interactions are secured over a secure communication path. This mechanism can be activated only by the system and cannot be imitated. A Trusted Path can either be a dedicated physical path (i.e., a terminal directly connected to the system) or an encrypted pathway which includes integrity and replay protection (e.g., IPsec virtual private network, Secure Socket Layer/Transport Layer Security (SSL/TLS) tunnel, or Secure Shell (SSH)).[4] See Appendix I for a discussion of IPsec, SSL/TLS and SSH security protocols.

MEC 19: Peer entity and data origin authentication based on a trusted path.

6.3 Access control

A TMN may provide capabilities to ensure that actors are prevented from gaining access to information or resources that they are not authorized to access. Access control security mechanisms ensure that only authorized users are allowed to manage system security resources.

[3] American National Standards Institute T1.243-1995, *Operations, Administration, Maintenance*.

[4] Adapted from National Computer Security Centre, NCSC-TG-004-88, *Glossary of Computer Security Terms*, October 1998 (available at http://csrc.nist.gov/SBC/PDF/NCSC-TG-004_COMPUSEC_Glossary.pdf).

Access control security mechanisms may be provided by a centralized system, often in conjunction with the authentication system. For example, a centralized Remote Access Dial-In User System (RADIUS) server may be used in conjunction with an Lightweight Directory Access Protocol (LDAP) database to provide a centralized system for authentication and access control.

Access control security mechanisms may have some of the following characteristics:

MEC 20: All administrative actions may be linked to specific individuals.

MEC 21: The access control security mechanism may support the concept of "least privilege" (i.e., a person will have a role and will have authorization to view data, modify data, or initiate Management Actions only for those functions allowed by that role).

MEC 22: At least some administrator accounts may not be allowed to be locked out due to password related activities such as login failures or timeouts.

MEC 23: A number of administrator roles may be defined, each with varying degrees of privilege with respect to critical security management actions. For example, a system may define five administrator user roles. Another system may define three administrator user roles. In either case, the roles may be defined to allow different privileges with respect to the following security actions:

MEC 23a: Define and assign user privileges.

MEC 23b: Add and delete user IDs.

MEC 23c: Initialize and reset login passwords.

MEC 23d: Initialize and change cryptographic keys.

MEC 23e: Set the system's aging threshold for login passwords.

MEC 23f: Set the system's limit on the number of failed logins for each user ID.

MEC 23g: Remove a lockout or change the system's Lockout timer value.

MEC 23h: Set the system's inactivity timer value.

MEC 23i: Set system security logging and alarm configuration.

MEC 23j: Manage system security logging processes.

MEC 23k: Upgrade security software.

MEC 23l: Terminate any user or system session.

MEC 23m: Define and assign new user and group privileges at the application level.

MEC 23n: Maintain a record of all requests for access to the application.

MEC 23o: Add and delete users at the application level.

MEC 23p: Monitor all application security logs.

MEC 23q: Configure application security logging and alarms.

MEC 23r: Manage application security logging processes.

MEC 23s: Terminate any user application session.

6.4 Data confidentiality

Data confidentiality security mechanisms are used to prevent unauthorized reception of communicated data. Cryptographic security mechanisms to provide data confidentiality are discussed in this clause.

Data confidentiality is based on cryptographic foundations. Cryptography uses special algorithms that are standards-based and publicly available thereby allowing for widespread scrutiny and ease of implementation. Cryptographic "strength" is based on the cryptographic algorithm used, as well as the key size used (i.e., strength refers to the amount of time required to reverse engineer (i.e., find or guess) the key value(s) being used with a specific algorithm).

Security protocols (e.g., IPsec, SSL/TLS, SSH) typically provide data origin authentication, data integrity, and data confidentiality. (See Annex A for a discussion of IPsec, SSL/TLS and SSH security protocols). Security extensions to other protocols such as Simple Network Management Protocol Version 3 (SNMPv3)[5], Common Object Request Broker Architecture (CORBA), Border Gateway Protocol, and Open Shortest Path First are designed to provide data origin authentication and data integrity.

The methods used to generate, store, distribute, destroy, and revoke cryptographic keys for data confidentiality are of very important. In addition, factors such as key length, key selection, and algorithm selection have a direct bearing on the security strength of a specific cryptosystem.

6.4.1 Symmetric data confidentiality

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 (e.g., the encryption key). The key must be distributed to the individuals via a secure means, or internally generated (e.g., based on a shared secret root key) because knowledge of the enciphering key implies knowledge of the deciphering key and vice-versa.

Data confidentiality security mechanisms may be based on symmetric cryptographic algorithms such as Data Encryption Standard (DES), Advanced Encryption Standard (AES), Triple Data Encryption Algorithm (3DES), and other algorithms.

DES is a 56-bit symmetric encryption algorithm that has been in use for many years. Due to its short key length, DES is vulnerable to key exhaustion using massive parallel computations, and is now considered weak. DES has been depreciated by the US National Institute of Standards and Technology (NIST).

AES has been chosen by NIST as the standard symmetric encryption algorithm to replace DES for US government applications. AES has key lengths of 128, 192 and 256 bits.

3DES is essentially the DES algorithm run three times with either two 56-bit keys or three 56-bit keys. 3DES is specified in Federal Information Processing Standard (FIPS) Publication 46-3, *Data Encryption Standard*, October 1999, Appendix 2, Page 22 (available at http://csirc.nist.gov/publications/fips/fips46-3/fips46-3.pdf).

3DES can be performed using either two independent 56-bit keys or three independent 56-bit keys, which could be expected to have strength of 112 bits and 168 bits, respectively. However, 3DES is subject to the "meet in the middle" attack, which can reduce two key 3DES strength to only 57 bits rather than the expected 112 bits. The same attack can render three key 3DES strength to only 112 bits rather than the expected 168 bits. Thus for higher security 3DES should be used with three independent keys and the worst case strength should be assumed to be 112 bits.

The DES algorithm may be performed relatively quickly due to its short 56-bit key, whereas 3DES must essentially perform DES three times and is, hence, much slower. AES, which has a minimum key length of 128 bits, is cryptographically stronger than 3DES and yet may be performed very quickly in both hardware and software. For example, a software implementation of AES may be processed approximately as fast as DES on the same platform, but with far greater cryptographic strength than DES.

MEC 24: Symmetric data confidentiality based on DES cryptographic algorithm.

[5] SNMPv3 may also provide confidentiality.

MEC 25: Symmetric data confidentiality based on AES cryptographic algorithm.

MEC 26: Symmetric data confidentiality based on 3DES cryptographic algorithm.

6.4.2 Asymmetric data confidentiality

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.

Data confidentiality security mechanisms may be based on asymmetric cryptographic algorithms such as Rivest Shamir Adleman (RSA), Elliptic Curve Cryptography (ECC), and others.

The RSA algorithm is a commonly used asymmetric algorithm which may be used for encryption and digital signatures. RSA is based on the mathematical difficulty of factoring large prime numbers. Common key lengths for the RSA algorithm are 1024 bits and 2048 bits. Note that RSA with a key length of 2048 bits is approximately equivalent in cryptographic strength to 128-bit symmetric encryption.

Elliptic Curve Cryptography (ECC) is a new method of performing public key cryptography (i.e., comparable to the RSA algorithm). With ECC, an elliptic curve is defined over a certain field; then, the elliptic curve discrete logarithm problem is solved over this field. The main advantage of ECC as compared to other public-key algorithms is the key size. A 160-bit ECC key is approximately equivalent in security to a 1024-bit RSA algorithm key, and a 210-bit ECC key is approximately equivalent to a 2048-bit RSA algorithm. The smaller ECC key results in less computational overhead and a more efficient cryptosystem.[6]

MEC 27: Asymmetric data confidentiality based on RSA cryptographic algorithm with specified key length.

MEC 28: Asymmetric data confidentiality based on ECC cryptographic algorithm with specified key length.

6.4.3 Data confidentiality – Summary

Examples of algorithms which may be used to provide data confidentiality are presented in tabular format in Table 3. Issues such as formatting, padding, handling error conditions, and choosing appropriate primes and the size of the public exponent, and in the case of ECC, base field and curve must also be considered; however, these issues are outside the scope of this Recommendation.

Table 3/M.3016.3 – Example cryptographic algorithms for data confidentiality

Category	Algorithm	Comments
Symmetric encryption algorithms	AES	Advanced Encryption Standard
	3-DES	Triple Data Encryption Algorithm
	DES	Data Encryption Standard
Asymmetric encryption algorithms	RSA	Rivest, Shamir, Adleman
	ECC	Elliptic Curve Cryptography

[6] See *Digital Signature Standard*, November 2002, (available at http://csrc.nist.gov/cryptval/dss.htm) for additional details on RSA, Diffie-Hellman, and ECC algorithms.

6.5 Data integrity

Data integrity security mechanisms are used to guarantee communicated data has not been modified.

Data integrity is based on cryptographic foundations. Cryptography uses special algorithms that are standards-based and publicly available, thereby allowing for widespread scrutiny and ease of implementation. Security protocols (e.g., IPsec, SSL/TLS, SSH) typically provide data integrity services based on underlying cryptographic algorithms in addition to other security services such as data confidentiality and data origin authentication. (See Appendix I for a discussion of IPsec, SSL/TLS and SSH security protocols.)

The methods used to generate, store, distribute, destroy, and revoke cryptographic keys for data integrity are of paramount importance. In addition, factors such as key length, key selection, and algorithm selection have a direct bearing on the security strength of a specific cryptosystem.

6.5.1 Symmetric data integrity

Symmetric, or secret key data integrity, refers to a cryptographic system where keys used for data integrity are the same for both the information sender and receiver. Symmetric cryptosystems require that initial arrangements be made for the individuals to share a unique secret key (e.g., the verification key). The key must be distributed to the individuals via a secure means, or internally generated (e.g., based on a shared secret root key).

Symmetric data integrity security mechanisms for arbitrary length messages may be based on keyed message digest algorithms combined with hashing functions. Examples of keyed message digest algorithms include the Hashed Message Authentication Code with Message Digest 5 (HMAC-MD5-96)[7] algorithm and the Hashed Message Authentication Code with Secure Hash Algorithm 1 (HMAC-SHA-1-96)[8].

MEC 29: Symmetric data integrity based on HMAC-MD5-96 cryptographic algorithm.

MEC 30: Symmetric data integrity based on HMAC-SHA-1-96 cryptographic algorithm.

6.5.2 Asymmetric data integrity

An asymmetric data integrity system is one in which the signing and verification keys are related but different. The verification key is made public, whereas the signing key is kept secret. The signing key is different from the verification key, and no feasible way is known for deriving the signing key from the verification key. Verification keys are distributed widely; however, the signing key is always kept secret.

Data integrity security mechanisms may be based on asymmetric cryptographic algorithms such as the Digital Signature Algorithm (DSA) and the Rivest Shamir Adleman (RSA) algorithm.

With asymmetric data integrity security mechanisms, the sender signs a message digest with a signing (private) key and the verification (public) key is used by the receiver to verify that the message digest was signed by the claimed originator.

MEC 31: Asymmetric data integrity based on DSA cryptographic algorithm with specified key length.

MEC 32: Asymmetric data integrity based on RSA cryptographic algorithm with specified key length.

[7] Internet Engineering Task Force Request for Comment 2403, *The Use of HMAC-MD5-96 within ESP and AH*, C. Madson, R. Glenn, November 1998.

[8] Internet Engineering Task Force Request for Comment 2404, *The Use of HMAC-SHA-1-96 within ESP and AH*, C. Madson, R. Glenn, November 1998.

6.5.3 Data integrity – Summary

Examples of algorithms which may be used to provide data integrity are presented in tabular format in Table 4. Issues such as formatting, padding, handling error conditions, and choosing appropriate primes must also be considered; however, these issues are outside the scope of this Recommendation.

Table 4/M.3016.3 – Example cryptographic algorithms for data confidentiality

Category	Algorithm	Comments
Asymmetric message verification algorithms	DSA	Digital Signature Algorithm.
Symmetric message verification algorithms	HMAC-MD5-96	Hashed Message Authentication Code with Message Digest 5.
	HMAC-SHA-1-96	Hashed Message Authentication Code with Secure Hash Algorithm 1.

6.6 Audit trail

Network elements and management systems should provide adequate capabilities to allow investigation, audit, and real-time detection, analysis and protection activities, so that proper remedial actions can be taken. This clause considers security mechanisms used for such security audit logs. The specific details of the content and format of the security audit logs are beyond the scope of this Recommendation.

Security audit logs may be kept by network element and management systems. These security audit logs may be kept locally, and may be transmitted to a centralized log repository and/or log analysis device.

Syslog is one common mechanism used for transmitting security audit logs from local storage to a centralized log repository.

In general, a device may be able to log any action that changes the security attributes and services, access controls, or other configuration parameters of the devices; each login attempt and its result; and each logout or session termination, whether remote or console. Logging of non-security related OAM&P messages, sometimes referred to as "recent change" messages, is required for any actions that are auditable.

Audit log entries may be sent to an unalterable audit server after being sequence labelled and cryptographically authenticated (signed) by the network element or management system. Security audit logs may be sent to a central repository over a trusted path. To ensure accurate analysis of actions, the date and time of numerous log sources must be synchronized accurately and securely (e.g., NTPv3).

MEC 33: Security audit logs based on Syslog.

MEC 34: Security audit log entry containing the following information:

MEC 34a: A description of the action or the actual action that is being logged.

MEC 34b: The identity and security level of the user or process that initiated the action.

MEC 34c: The date and time the action occurred.

MEC 34d: Network source and destination information, if applicable (e.g., when logging in).

MEC 34e: An indication of the success or failure of the activity.

MEC 34f: Any action that requires auditing.

MEC 35: Security audit logs sent to an unalterable audit server.

MEC 36: Security audit logs cryptographically signed.

MEC 37: Security audit logs sent to a central repository over a trusted path.

6.7 Key exchange

For symmetric data confidentiality and symmetric data integrity applications, cryptographic keys must be securely exchanged between endpoints. The keys for such symmetric algorithms should normally be exchanged in a process tightly bound to authentication, lest an attacker gets between the authentication and key distribution processes.

The methods used to generate, store, distribute, destroy, and revoke these cryptographic keys are of paramount importance. In addition, factors such as key length, key selection, and algorithm selection have a direct bearing on the amount of security a cryptosystem provides.

Various methods can be used for provisioning and/or exchanging cryptographic keys. One conceptually simple method is pre-shared key exchange whereby keys are sent out-of-band and provisioned into each endpoint as necessary. For example, keys can be selected and configured into endpoints by network administrators upon commissioning. Pre-shared key exchange may be acceptable for a small number of endpoints however this does not scale well for a large numbers since it becomes very cumbersome to generate and configure large numbers of keys.

Asymmetric algorithms such as the Rivest, Shamir, Adleman (RSA) can be used in support of key exchange services. Using RSA, one endpoint selects symmetric cryptographic keys and distributes these to other endpoints under protection of the RSA encryption algorithm. Using this method, the asymmetric algorithm should have an appropriate key length in order to protect the symmetric keys being sent. To protect a 128-bit symmetric key, for example, the RSA algorithm should use a key length 2048 bits or greater to be roughly equivalent in cryptographic strength to the 128-bit symmetric key encryption.

The Diffie-Hellman key agreement algorithm is a common method of key distribution. Using the Diffie-Hellman algorithm, endpoints independently derive secret symmetric cryptographic keys over a public network. Only intermediate results are sent between endpoints during the Diffie-Hellman process, and the secret key is never revealed. With appropriate Diffie-Hellman prime number selection, it is computationally unfeasible for attackers to derive the secret key from the intermediate results.

For RSA and Diffie-Hellman algorithms, issues such as choosing appropriate primes, choosing public exponents, and handling error conditions must also be considered.

MEC 38: Cryptographic key exchange based on pre-shared keys.

MEC 39: Cryptographic key exchange based on asymmetric RSA algorithm, with a specified RSA key length.

MEC 40: Cryptographic key exchange based on the Diffie-Hellman key agreement algorithm with a specified Diffie-Hellman prime group.

6.8 Alarm reporting

Security alarms should be sent to administrators on the detection of any security violation or the inability to continue to write audit logs.

MEC 41: Security alarms reporting mechanisms such as X.736.

6.9 Packet filtering

In order to protect the DCN from attack and the loss of information about the DCN, packet filtering should be used for devices with packet-based connectivity.

MEC 42: Packet filtering based on one or more of the following inspection criteria:

MEC 42a: Source IP Address.

MEC 42b: Destination IP Address.

MEC 42c: Protocol.

MEC 42d: Source Port.

MEC 42e: Destination Port,

and providing one or more of the following actions:

MEC 42f: Pass.

MEC 42g: Drop.

MEC 42h: Modify.

MEC 42i: Forward.

potentially with the capability to consider previous decisions (i.e., stateful).

Appendix I

IPsec, SSL/TLS and SSH security mechanisms

I.1 IPsec

IPsec addresses security at the IP layer, provided through the use of a combination of cryptographic and protocol security mechanisms. IPSec protocol runs between the Network layer (Layer 3) and the Transport layer (Layer 4) and can be used to protect any type of data traffic (TCP or UDP) and is independent of applications. IPsec is designed to provide interoperable, high quality, cryptographically-based security for IPv4 and IPv6. The set of security services offered by IPsec includes:

a) Data integrity;

b) Data origin authentication based on IP address;

c) Machine-to-machine authentication;

d) Anti-Replay Protection;

e) Data confidentiality;

f) Cryptographic key exchange.

These objectives are met through the use of two traffic security services, the Authentication Header (AH) and the Encapsulating Security Payload (ESP), and through the use of cryptographic key management procedures and protocols. AH service provides data origin authentication, machine-to-machine authentication and data integrity for IP packets. ESP service provides data confidentiality service in addition to data origin authentication, machine-to-machine authentication and data integrity for IP packets. IPsec mechanisms also designed to be cryptographic algorithm-independent to permit selection of different sets of algorithms without affecting the other parts of the implementation.

Key Management is provided by the Internet Key Exchange (IKE) protocol. Both manual and automatic mechanisms for key negotiation between endpoints are provided. Automatic key negotiation can be based on pre-shared keys (e.g., passwords) or X.509 certificates.

References [RFC 2401], [RFC 2402], [RFC 2403], [RFC 2404], [RFC 2405], [RFC 2406], [RFC 2407], [RFC 2408], [RFC 2409], [RFC 2410], [RFC 2411], [RFC 2412], [RFC 3602], [RFC 2451], [FIPS-197].

I.2 SSL/TLS

The Secure Socket Layer (SSL) security protocol provides data encryption, server authentication, message integrity, and optional client authentication for a TCP/IP connection at the transport layer (Layer 4). SSL is currently at revision 3.0. Transport Layer Security (TLS) is the IETF standardized version of SSL which includes security enhancements over SSL including:

- Required Diffie-Hellman and DSA digital signatures algorithm (DSA) support, with optional RSA support.
- Use of stronger hashed message authentication algorithm (HMAC) instead of a non-standard SSL defined MAC algorithm.
- Modified key generation algorithm which uses MD5 (Message Digest 5) and SHA-1 (Secure Hash Algorithm 1) with the HMAC.

The SSL/TLS protocol runs above the Network Layer (Layer 4) and works with Transport Control Protocol (TCP) protocol only and cannot work with User Datagram Protocol (UDP). The application layer protocols that commonly run on top of SSL/TLS include, but are not limited to, Hypertext Transport Protocol (HTTP), the Lightweight Directory Access Protocol (LDAP), and the Internet Messaging Access Protocol. Higher application-level protocol can work above SSL/TLS without any regard for SSL/TLS; however, the application level must be linked to SSL/TLS through the use of I/O callbacks.

The SSL/TLS protocol provides three security functions for TCP traffic: data confidentiality, data integrity and authentication.

The SSL/TLS security protocol architecture provides two layers which run over TCP:

- The SSL/TLS Upper Layer Protocols;
- SSL/TLS Record Protocol.

The SSL/TLS Upper Layer Protocols include the SSL/TLS Handshake Protocol, SSL/TLS Cipher Change Protocol, and the SSL/TLS Alert Protocol for notifications. SSL/TLS sessions are initially created by the SSL/TLS handshake protocol which provides:

a) Negotiation of authentication and security mechanisms.

b) Authentication of client and server. (Using the server and client public/private keys.)

c) Establishment of security keys.

Once the SSL/TLS session is established, the SSL/TLS Record Protocol is used for bulk data transport services. The SSL/TLS Record Protocol provides:

a) Data origin authentication based on the server keys.

b) Data integrity.

c) Confidentiality.

Note that SSL is now at version 3 (SSLv3), and TLS is at version 1. Earlier versions of SSL and TLS are not recommended.

SSL/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. Unidirectional authentication is the usual method used in the public internet. For network management applications, bidirectional authentication is recommended to allow both parties to know they are communicating with the desired endpoint.

References [RFC 2246], [RFC 3546], [SSL V3].

I.3 SSH

SSH is an Application Layer (Layer 7) security protocol commonly used to directly replace insecure protocols Telnet and File Transfer Protocol (FTP) protocols. Telnet and FTP are insecure protocols which transmit passwords and all other data in the clear. SSH can also be used to protect other protocols through the use of port forwarding, so it can be used as a general network security protocol.

There are two versions of SSH: SSHv1 and SSHv2. SSHv1 was developed in 1998 and is now considered insecure/obsolete.

Secure Shell 2 features are:

- Full replacement for Telnet, Rlogin, Rsh, Rcp, and FTP protocols to provide secure file transfer and file copying.
- Automatic authentication of users. (No passwords sent in clear-text.)
- Bidirectional authentication (both the server and the client are authenticated).
- Tunnelling of arbitrary TCP/IP-based applications through the use of port forwarding.
- Encryption of data for data confidentiality.
- Multiple authentication options including passwords, public key, and SecureID authentication.
- Multiple ciphers suites available.

The SSHv2 architecture consists of three major components:

- The Transport Layer Protocol [SSH-TRANS] provides server authentication, data confidentiality, and data integrity. It may optionally also provide compression.
- The User Authentication Protocol [SSH-USERAUTH] authenticates the client-side user to the server.
- The Connection Protocol [SSH-CONNECT] multiplexes the encrypted tunnel into several logical channels.

The connection protocol provides channels that can be used for a wide range of purposes. Standard methods are provided for setting up secure interactive shell sessions and for forwarding ("tunnelling") arbitrary TCP/IP ports and connections.

Port number 22 has been registered with the IANA as the standard port to use for SSHv2 applications.

References [SSH-ARCH], [SSH-TRANS], [SSH-USERAUTH], [SSH-CONNECT].

Appendix II

This appendix describes a mechanism for Packet Filtering to enhance the security of the Data Communications Network (DCN). The Data Communications Network (DCN) is the network used to connect the management applications (usually located in the Network Operations Centre) to the network elements for centralized service provisioning, alarm monitoring, testing, billing, and other network management activities. Sections 2.8–2.10 of RFC 3871 provide a set of requirements for packet filtering for large Internet Service Provider IP network infrastructure. This contribution draws on RFC 3871 to define filtering recommendations for the DCN.

Packet filtering is the process of deciding the disposition of each packet that passes through a network element based on specified match criteria[9]. There could be several dispositions, e.g., Pass, Drop, Forward (direct it to elsewhere), etc. Packet filtering provides the basic protection mechanism determining what traffic passes into or through the network element or management system.

The main concern is filtering traffic from other networks (e.g., networks carrying customer traffic, peer management networks) onto the DCN. In addition, certain elements of the DCN may need to be segregated from other elements. Therefore, filtering can be used between different sub-networks (or domains) of the DCN.

II.1 Objectives

Broad objectives for the packet filtering mechanism are to:

1) Protect the DCN infrastructure from customer traffic. The protection should include proper sharing of common resources to avoid degradation or denial of service.

2) Protect the DCN infrastructure from peer networks.

3) Prevent traffic on the DCN that is not in compliance with the applicable security policy from propagating any further through the DCN infrastructure.

II.2 Network design considerations affecting packet filtering

This appendix does not imply requirements for design of the DCN; however, the design and deployment of the DCN will affect the deployment of and requirements for packet filtering in the network. Figure II.1 shows a typical DCN design.

[9] This description of packet filtering is very similar to packet routing; however, this appendix focuses on packet filtering and does not address packet routing.

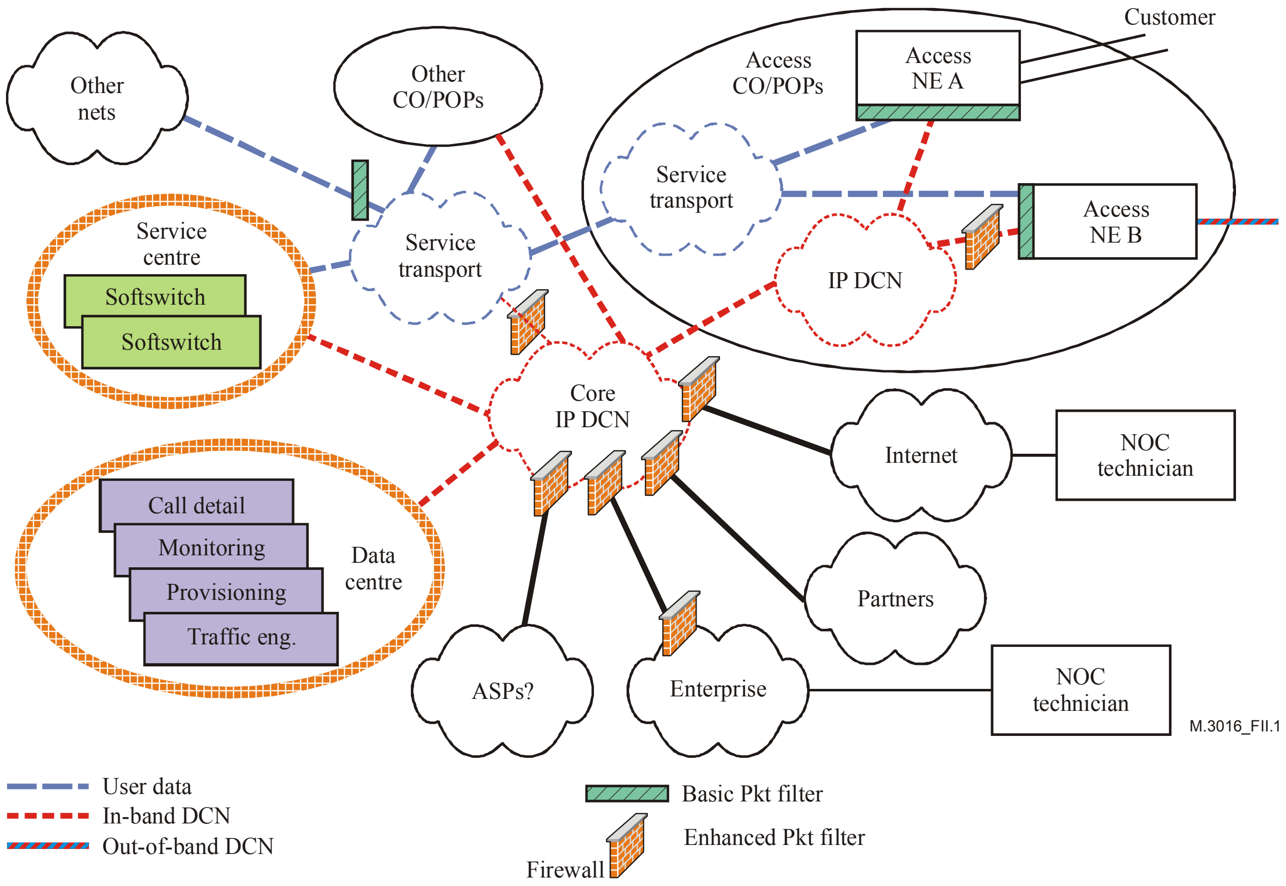

Figure II.1/M.3016.3 – Generic DCN illustration

Three types of DCN design are generally recognized:

- In-band Management: DCN uses reserved bandwidth from the Service Network used to carry customer data. For example, a VLAN on an Ethernet link could be dedicated to management traffic or an IPSec or SSH connection could be used over an Internet connection (e.g., for the NOC Technician in Figure II.1 connected over the Internet).
- Out-of-band Management: The DCN is a completely different network from the Service network carrying customer traffic. This network could be overlaid on top of the same physical network that also carries user data traffic.
- Hybrid: Combines in-band and out-of-band approaches.

  The comparison & general discussion of these types of management architectures are beyond the scope of this Recommendation (see section 2.2 of RFC 3871); however, utilization of one or the other will affect filtering requirements.

The rationale used to create DCNs will vary based on the type of network elements supported, operational procedures and preferences, network topologies, economics, etc. Network capacity, resiliency, and security are issues that are considered for each approach.

Next-generation managed service offerings will be implemented using packet-based (e.g., frame-relay, ATM, IP, MPLS, Ethernet) transport equipment. The advent of such services makes it necessary to manage the access equipment (CPE).

It may be necessary to use a hybrid model using out-of-band management to the points-of-presence (POP) and in-band management from the POP to the CPE access devices, as it may not be economically feasible to extend the out-of-band management all the way to the CPE access device. Access NE B illustrates the latter in Figure II.1. In this case, enhanced filtering (e.g., firewall) can be used to protect the DCN from the CPE. Other examples of the use of an in-band connection are the management of a remote, isolated POP where it is infeasible to build out a separate network and the use of the service network as a backup to the DCN.

The use of packet filtering also assumes the address space used by the DCN is separate from that assigned to customers and there is no need for the traffic to flow between these two domains. Separation of address space simplifies development of packet filters to block customer traffic from accessing management resources. The easiest approach is to block all traffic destined to the DCN that originates from outside the DCN to protect the management infrastructure from customer traffic. However, some traffic may need to be exchanged between outside networks and the DCN in some cases, e.g., management information exchange between two Service Providers (e.g., the DCC at a mid-point meet between two SPs).

Thus provision needs to be made to allow some restricted traffic to flow between domains and more controls (e.g., enhanced packet filtering) are needed to provide adequate security for the DCN.

Figure II.1 illustrates a DCN design based on the assumptions above. The Service Transport (blue) carries the customer traffic. The DCN (red) carries the management traffic. The Service Centre contains servers, etc., that provide services to the customers and that the customers have access to (e.g., soft switches). The Data Centre contains servers and other operations systems used to manage and monitor the network and is not directly accessible to customers. The connection from the DCN to the Network Elements can use IP, X.25, async or ISO CLNS.

Providing ingress packet filtering on DCN/Service network boundary is a basic requirement for providing DCN security at the Access NE. However, such basic packet filtering may not be sufficient since attacks could also come from a compromised NE or host within the DCN. Therefore, suitable packet filtering mechanisms may need to be strategically implemented at multiple points in the DCN to ensure compliance with the applicable security policy. In addition, enhanced packet filtering may be needed where the DCN connects to external networks (e.g., Internet, SP's enterprise network, partners, etc.).

While packet filtering is a component of a network security strategy, it must be used within the context of overall network security principles and strategies including, e.g., compartmentalization and defense-in-depth. So, while a good security strategy will include security requirements on the hosts themselves (e.g., soft switches) and compartmentalization of the network, these are outside the scope of this Recommendation.

To protect the management infrastructure, and the DCN in general, it is useful for the network operator to discard certain packets received from outside the perimeter of the DCN (i.e., from peers and customers). For example, packets with invalid source IP addresses and packets destined for IP addresses used exclusively on the DCN should not be permitted inside the perimeter of the DCN. This function is called ingress filtering. These requirements are derived from [RFC 3871] and [RFC 2827].

There are two categories of packet filtering:

- Basic Packet Filtering based on the packet header information including the capability to detect and block packets with spoofed source address.
- Enhanced Packet Filtering, including:
  - Stateful examination of packets where the context or state information is also used in making the filtering decisions.
  - Dynamic filtering for specific protocols where filters are opened dynamically based on the information carried in the protocol payload.
  - Deep packet inspection where the application level protocols are examined for any protocol anomaly, unusual or suspicious contents.

II.3 Basic packet filtering

Equipment connecting to the DCN should have an option to drop packets received from external-facing interfaces (e.g., customers and peers) containing invalid source IP addresses. Invalid source IP addresses can consist of:

- Bogon addresses (see Section 1.8 of RFC 3871).
- Martians (see Section 1.8 of RFC 3871).
- IP addresses not assigned to the customer (or not valid for the peer to send).

The packet filtering mechanism should be able to filter traffic addressed to the address blocks allocated to the DCN and originated from outside (e.g., from customers) based on the attributes specified in MEC 42.

The packet filtering mechanism should provide accurate per-interface traffic statistics. The level of granularity of statistics may vary depending on packet filtering mechanism.

Equipment should be able to filter traffic from outside the DCN (e.g., from customers), that is, addressed directly to a Network Element via any of its interfaces, including loopback interfaces, based on attributes specified in MEC 42.

The packet filtering mechanism may support the multiple security domains concept of the TMN model where all elements in a security domain are mandated to follow a common security policy.

Equipment may have the capability to generate suitable alarms based on the traffic, exceptions and its operating conditions.

II.4 Enhanced packet filtering

These recommendations should be considered where a high degree of overlap exists between the user and management traffic, i.e., the user and management traffic are not segregated right at the edge of the network, and where the DCN connects directly to other networks. In addition, these filtering capabilities should be used at the boundaries of protected sub-networks (e.g., between the DCN and Data Centre).

The mechanism should examine the application protocols used on the DCN for any protocol anomaly or abnormal behavior and should suitably block such traffic.

The mechanism should examine the content of the traffic on the DCN for malicious content like viruses, worms, Trojans, etc., wherever applicable.

The mechanism should provide protection for applicable types of Denial of Service (DoS) attacks.

The mechanism should be capable of stateful filtering, i.e., the session information is used for packet filtering. Return traffic for a session should always be allowed to pass.

The mechanism should support dynamic pinhole capability for all protocols used in the network carrying the port information in their payload, e.g., FTP, SIP, etc. The packet filtering mechanism should examine the port information in the payload and open the communication on the specified port (dynamic pinhole) for the life of the session. In case of abrupt termination of the session, a suitable time-out mechanism shall exist to close the port.

The mechanism should support protocol enforcement including dropping of malformed packets or improper session establishment, etc.

Other recommended filtering capabilities can be found in sections 2.7–2.10 of RFC 3871.

BIBLIOGRAPHY

[RFC 2827] IETF RFC 2827 (2000), *Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing.*

[RFC 2401] IETF RFC 2401 (1998), *Security Architecture for the Internet Protocol*, http://www.ietf.org/rfc/rfc2401.txt?number=2401

[RFC 3704] IETF RFC 3704 (2004), *Ingress Filtering for Multihomed Networks.*

[RFC 3871] IETF RFC 3871 (2004), *Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure.*

[NDS/IP] 3GPP TS 33.210 (2001), *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Network Domain Security; IP network layer security.*

[RFC 2402] IETF RFC 2402 (1998), *IP Authentication Header*, http://www.ietf.org/rfc/rfc2402.txt?number=2402

[RFC 2403] IETF RFC 2403 (1998), *The Use of HMAC-MD5-96 within ESP and AH*, http://www.ietf.org/rfc/rfc2403.txt?number=2403

[RFC 2404] IETF RFC 2404 (1998), *The Use of HMAC-SHA-1-96 within ESP and AH*, http://www.ietf.org/rfc/rfc2404.txt?number=2404

[RFC 2405] IETF RFC 2405 (1998), *The ESP DES-CBC Cipher Algorithm with Explicit IV*, http://www.ietf.org/rfc/rfc2405.txt?number=2405

[RFC 2406] IETF RFC 2406 (1998), *IP Encapsulating Security Payload (ESP)*, http://www.ietf.org/rfc/rfc2406.txt?number=2406

[RFC 2407] IETF RFC 2407 (1998), *The Internet IP Security Domain of Interpretation for ISAKMP*, http://www.ietf.org/rfc/rfc2407.txt?number=2407

[RFC 2408] IETF RFC 2408 (1998), *Internet Security Association and Key Management Protocol (ISAKMP)*, http://www.ietf.org/rfc/rfc2408.txt?number=2408

[RFC 2409] IETF RFC 2409 (1998), *The Internet Key Exchange (IKE)*, http://www.ietf.org/rfc/rfc2409.txt?number=2409

[RFC 2410] IETF RFC 2410 (1998), *The NULL Encryption Algorithm and Its Use with IPsec*, http://www.ietf.org/rfc/rfc2410.txt?number=2410

[RFC 2411] IETF RFC 2411 (1998), *IP Security Document Roadmap*, http://www.ietf.org/rfc/rfc2411.txt?number=2411

[RFC 2412] IETF RFC 2412 (1998), *The OAKLEY Key Determination Protocol*, http://www.ietf.org/rfc/rfc2412.txt?number=2412

[RFC 3602] IETF RFC 3602 (2003), *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 2451] IETF RFC 2451 (1998), *The ESP CBC-Mode Cipher Algorithms*, http://www.ietf.org/rfc/rfc2451.txt

[RFC 2246] IETF RFC 2246 (1999), *The TLS Protocol, Version 1.0*, ftp://ftp.rfc-editor.org/in-notes/rfc2246.txt

[RFC 3546] IETF RFC 3546 (2003), *Transport Layer Security (TLS) Extensions*, ftp://ftp.rfc-editor.org/in-notes/rfc3546.txt

[SSL V3] *Secure Socket Layer Version 3.0 Specification*, Netscape Communications. http://wp.netscape.com/eng/ssl3/

[SSH-ARCH] YLONEN (T.): *SSH Protocol Architecture*, I-D draft-ietf-architecture-15.txt, October 2003. http://www.ietf.org/internet-drafts/draft-ietf-secsh-architecture-15.txt

[SSH-TRANS] YLONEN (T.): *SSH Transport Layer Protocol*, I-D draft-ietf-transport-17.txt, October 2003. http://www.ietf.org/internet-drafts/draft-ietf-secsh-transport-17.txt

[SSH-USERAUTH] YLONEN (T.): *SSH Authentication Protocol*, I-D draft-ietf-userauth-18.txt, September 2002. http://www.ietf.org/internet-drafts/draft-ietf-secsh-userauth-18.txt

[SSH-CONNECT] YLONEN (T.): *SSH Connection Protocol*, I-D draft-ietf-connect-18.txt, October 2003. http://www.ietf.org/internet-drafts/draft-ietf-secsh-connect-18.txt

[FIPS-46-3] Data Encryption Standard. (Describes both DES and 3DES). http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf

[FIPS-197] Advanced Encryption Standard (AES), FIPS Publication 197, National Institute of Standards and Technology, November 2001. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[RFC 2437] IETF RFC 2437 (1998), *PKCS #1: RSA Cryptography Specifications Version 2.0*, http://www.ietf.org/rfc/rfc2437.txt?number=2437

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	**Telecommunication management, including TMN and network maintenance**
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2005