International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1205

(04/2008)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Telecommunication security

Overview of cybersecurity

Recommendation ITU-T X.1205

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	
Services and facilities	X.1–X.19
Interfaces	X.20–X.49
Transmission, signalling and switching	X.50–X.89
Network aspects	X.90–X.149
Maintenance	X.150–X.179
Administrative arrangements	X.180–X.199
OPEN SYSTEMS INTERCONNECTION	
Model and notation	X.200–X.209
Service definitions	X.210–X.219
Connection-mode protocol specifications	X.220–X.229
Connectionless-mode protocol specifications	X.230–X.239
PICS proformas	X.240–X.259
Protocol Identification	X.260–X.269
Security Protocols	X.270–X.279
Layer Managed Objects	X.280–X.289
Conformance testing	X.290–X.299
INTERWORKING BETWEEN NETWORKS	
General	X.300–X.349
Satellite data transmission systems	X.350–X.369
IP-based networks	X.370–X.379
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	
Networking	X.600–X.629
Efficiency	X.630–X.639
Quality of service	X.640–X.649
Naming, Addressing and Registration	X.650–X.679
Abstract Syntax Notation One (ASN.1)	X.680–X.699
OSI MANAGEMENT	
Systems Management framework and architecture	X.700–X.709
Management Communication Service and Protocol	X.710–X.719
Structure of Management Information	X.720–X.729
Management functions and ODMA functions	X.730–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	
Commitment, Concurrency and Recovery	X.850–X.859
Transaction processing	X.860–X.879
Remote operations	X.880–X.889
Generic applications of ASN.1	X.890–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
TELECOMMUNICATION SECURITY	**X.1000–**

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

Recommendation ITU-T X.1205

Overview of cybersecurity

Summary

Recommendation ITU-T X.1205 provides a definition for cybersecurity. This Recommendation provides a taxonomy of the security threats from an organization point of view. Cybersecurity threats and vulnerabilities including the most common hacker's tools of the trade are presented. Threats are discussed at various network layers.

Various cybersecurity technologies that are available to remedy the threats are discussed, including: routers, firewalls, antivirus protection, intrusion detection systems, intrusion protection systems, secure computing and audit and monitoring. Network protection principles, such as defence in depth, access management with application to cybersecurity are discussed. Risk management strategies and techniques are discussed including the value of training and education in protecting the network. Examples for securing various networks, based on the discussed technologies, are also discussed.

Source

Recommendation ITU-T X.1205 was approved on 18 April 2008 by ITU-T Study Group 17 (2005-2008) under the WTSA Resolution 1 procedure.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). 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, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

CONTENTS

Recommendation ITU-T X.1205

Overview of cybersecurity

1 Scope

This Recommendation develops a definition of cybersecurity in clause 7. This Recommendation provides a taxonomy of security threats from an organization point of view.

NOTE – The use of the term "identity" in this Recommendation does not indicate its absolute meaning. In particular, it does not constitute any positive validation.

Clause 7 discusses the nature of enterprise cybersecurity environment, cybersecurity risks and end-to-end communications security. Clause 8 discusses possible network protection strategies, including: closed loop policy management, uniform access management. Clause 8 also discusses secure communications techniques, variable depth security, securing the management plane, layered security and network survivability even under attack.

Appendix I discusses taxonomy of security threats, hackers tools of the trade and security threats.

Appendix II provides a review of the fields of cybersecurity technologies, including: cryptograph, access control technologies, perimeter protection techniques, antivirus and system integrity, audit and monitoring, and management.

Appendix III provides examples of network security. Examples include: securing remote access, securing IP telephony, securing VoIP clients, securing the remote office and securing WLANs.

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 X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

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

[ITU-T X.811] Recommendation ITU-T X.811 (1995) | ISO/IEC 10181-2:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Authentication framework*.

[ITU-T X.812] Recommendation ITU-T X.812 (1995) | ISO/IEC 10181-3:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Access control framework*.

[IETF RFC 1918] IETF RFC 1918 (1996), *Address Allocation for Private Internets* <http://www.ietf.org/rfc/rfc1918.txt?number=1918>.

[IETF RFC 2396] IETF RFC 2396 (1998), *Uniform Resource Identifiers (URI): Generic Syntax* <http://www.ietf.org/rfc/rfc2396.txt?number=2396>.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 This Recommendation uses the following terms defined in [ITU-T X.800]:

a) Authorization;

b) Security architecture;

c) Security policy;

d) User.

3.1.2 This Recommendation uses the following terms defined in [ITU-T X.805]:

a) Security dimension;

b) Security service.

3.1.3 This Recommendation uses the following terms defined in [ITU-T X.811]:

a) Authentication;

b) Principle.

3.1.4 This Recommendation uses the following terms defined in [ITU-T X.812]:

a) Access control information;

b) Access;

c) Access control;

d) User.

3.1.5 This Recommendation uses the following terms defined in [IETF RFC 2396]:

a) Uniform resource identifier (URI);

b) URI reference.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 access point: IEEE 802.11 wireless hub, a special kind of station (STA) operating as an access point.

3.2.2 basic service set (BSS): Coverage area served by one access point (AP).

3.2.3 cryptographic algorithm: A cryptographic algorithm is the means by which data are altered and disguised in encryption.

3.2.4 cyber environment: This includes users, networks, devices, all software, processes, information in storage or transit, applications, services, and systems that can be connected directly or indirectly to networks.

3.2.5 cybersecurity: Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following:

- Availability
- Integrity, which may include authenticity and non-repudiation
- Confidentiality.

3.2.6 distributed system: A non-standardized medium for interconnecting BSSs within an ESS.

3.2.7 extensible authentication protocol: This PPP extension providing support for additional authentication methods is part of the [b-IEEE 802.1X] specification.

3.2.8 extended service set: A single wireless LAN with BSSs within a single IP subnet.

3.2.9 firewall: A system or combination of systems that enforces a boundary between two or more networks. A gateway that limits access between networks in accordance with local security policy.

3.2.10 foreign agent: The visited/host network's router that services the mobile node while it is visiting the host network. This foreign agent handles the tunnelling and delivery between the mobile node and others, and between the mobile's home network and the host network.

3.2.11 honeyspot: A software program that emulates a network so as to attract (and maybe confuse) intruders and track their actions. The output of these systems can be used to infer the intruder's intentions and evidence gathering.

3.2.12 home agent: A router that services the mobile node while it is visiting other networks, maintaining current location information on that mobile node.

3.2.13 hot spots: Public places that host mobile IEEE 802.11 users to connect to the Internet.

3.2.14 IP mobility: A mechanism which enables more transparent connectivity for mobile nodes that "visit" different IP sub-networks while travelling. This is a mechanism for mobile management for mobile nodes on both wired networks and wireless networks.

4 Abbreviations

This Recommendation uses the following abbreviations:

3DES	Triple Data Encryption Standard
AAA	Authentication, Authorization and Accounting
ACL	Access Control List
AES	Advanced Encryption Standard
AP	Access Point
ASP	Application Service Provider
BSS	Basic Service Set
CA	Certification Authority
CMP	Certificate Management Protocol
COPS	Common Open Policy Service
CRL	Certificate Revocation List
DISA	Direct Inward System Access
DNS	Domain Name System
EAP	Extensible Authentication Protocol
EMS	Element Management System

ESS	Extended Service Set
ESSID	Extended Service Set Identifier
FTP	File Transfer Protocol
HMAC	Hash function based MACs
HTTP	HyperText Transfer Protocol
IDS	Intrusion Detection System
IKE	Internet Key Exchange
IP	Internet Protocol
IPSec	Internet Protocol Security
ISP	Internet Service Provider
L2TP	Layer 2 Tunnelling Protocol
LAN	Local Area Network
MAC	Message Authentication Code
MD5	Message Digest algorithm 5
MIC	Message Integrity Check
MIME	Multipurpose Internet Mail Extensions
MPLS	MultiProtocol Label Switching
MU	Mobile Unit
NAT	Network Address Translation
NGN	Next Generation Network
NIC	Network Interface Card
NOC	Network Operations Centre
OAM&P	Operations, Administration, Maintenance & Provisioning
OCSP	Online Certificate Status Protocol
OS	Operating System
OSI	Open Systems Interconnection
PDP	Policy Decision Point
PEAP	Protected EAP protocol
PEP	Policy Enforcement Point
PGP	Pretty Good Privacy
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
PoP	Proof of Possession
PPP	Point-to-Point Protocol
PSTN	Public Switched Telephone Network
RADIUS	Remote Authentication Dial-in User Service
RSA	Rivest Shamir Adleman public key algorithm

SHA-1	Secure Hash Algorithm 1
SIP	Session Initiation Protocol
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SP	Service Provider
SSH	Secure Shell
SSID	Service Set Identification
SSO	Single Sign On
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security Protocol
UE	User Equipment
URI	Uniform Resource Identifier
UTC	Coordinated Universal Time
VAR	Value-Added Reseller
VLAN	Virtual LAN
VoIP	Voice-over-IP
VPLS	Virtual Private LAN Service
VPN	Virtual Private Network
VPWS	Virtual Private Wire Service
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WLAN	Wireless LAN
WPA	Wi-fi Protected Access
XML	eXtensible Markup Language

5 Conventions

User equipment (UE) within this Recommendation is understood in a broad sense to encompass all sorts of devices, (hardware- or software based-) entities, mobile and/or stationary, personal computer (PC)s, (multimedia-enabled) terminals, phones, etc., all in the user premises, often out of control of an operator or service provider.

6 Introduction

The use of networks to connect heterogeneous IT systems can result in productivity gains to organizations and new capabilities that are enabled by the networked systems. Nowadays it is relatively easy to obtain information, to communicate, to monitor and control IT systems across vast distances. As such, today's networks play a key role in many nations' critical infrastructure that include: electronic commerce, voice and data communications, utility, financial, health, transportation, and defence.

Network connectivity and ubiquitous access is central to today's IT systems. However, widespread access and the loose coupling of interconnected IT systems can be a primary source of widespread vulnerability. Threats to networked systems such as: denial of service attacks, theft of financial and personal data, network failures and disruption of voice and data telecommunications are increasing.

The network protocols that are in use today were developed in an environment of trust. Most new investments and development are dedicated to building new functionality and not on securing that functionality.

Cybersecurity threats are growing rapidly. Viruses, worms, Trojan horses, spoofing attacks, "identity theft"[1], spam, and cyber attacks are on the rise. An understanding of cybersecurity is needed in order to build a foundation of knowledge that can aid securing the networks of tomorrow.

Corporations and government agencies are encouraged to view security as a process or way of thinking on how to protect systems, networks, applications, and resources. The underlying thinking is that connected networks have inherent risks. However, security should not be an obstacle to business. The objective is on how to offer the necessary services in a secure way.

In today's business environment, the concept of perimeter is disappearing. The boundaries between inside and outside networks are becoming thinner. Applications run on top of networks in a layered fashion. It is assumed that security exists between each of these layers. A layered approach to security enables organizations to create multiple levels of defence against threats.

7 Cybersecurity

Organizations need to devise a comprehensive plan for addressing its security needs. Organizations are encouraged to view security as a process or way of thinking on how to protect systems, networks, applications, and resources.

7.1 What is cybersecurity?

In this Recommendation, the term cybersecurity is defined in clause 3.2.5.

Cybersecurity techniques can be used to ensure system availability, integrity, authenticity, confidentiality, and non-repudiation. Cybersecurity can be used to ensure that user privacy is respected. Cybersecurity techniques can be used to establish the user's trustworthiness.

Technologies, such as wireless networks and voice-over-IP (VoIP), extend the reach and scale of the Internet. In this regard, the cyber environment includes users, the Internet, the computing devices that are connected to it and all applications, services and systems that can be connected directly or indirectly to the Internet, and to the next generation network (NGN) environment, the latter with public and private incarnations. Thus, with VoIP technology, a desk telephone is part of the cyber environment. However, even isolated devices can also be part of cyber environment if they can share information with connected computing devices through removable media.

The cyber environment include the software that runs on computing devices, the stored (also transmitted) information on these devices or information that are generated by these devices. Installations and buildings that house the devices are also part of the cyber environment. Cybersecurity needs to take such elements into consideration.

---

[1] The term "identity theft" refers only to the unauthorized use of the set identifiers and other information which, together, characterize the identity of a specific user. In contrast to the normal concept of theft, where the target item is physically removed from the victim, identity theft generally involves capturing or copying identity details such that the legitimate owner may not even be aware of the theft.

Cybersecurity aims at securing the cyber environment, a system that may involve stakeholders that belong to many public and private organizations, using diverse components and different approaches to security. As such, it is beneficial to think of cybersecurity in the following sense:

– The collection of policies and actions that are used to protect connected networks (including, computers, devices, hardware, stored information and information in transit) from unauthorized access, modification, theft, disruption, interruption or other threats.

– An ongoing evaluation and monitoring of the above policies and actions in order to ensure the continued quality of security in face of the changing nature of threats.

[b-ITU-T Y.2201] places requirements on NGN networks that can be used for enhancing the cybersecurity of these networks. The work calls for the support for authentication with the possibility of authenticating devices and users separately. In NGN, multi-factor bilateral authentication with support of authorization on a service-by-service level reduces the risks of user targeted attacks.

7.2 Nature of enterprise cybersecurity environment

Organizations need to devise a comprehensive plan for addressing its security needs. Security is not one size fit all (see [ITU-T X.805]). Security cannot be achieved by a collection of modules that are interconnected together. Organizations are encouraged to view security as a process or way of thinking on how to protect systems, networks, applications, and network services.

Security has to be comprehensive across all network layers. Adopting a layered approach to security that, when combined with strong policy management and enforcement, provides security professionals a choice of security solutions that could be modular, flexible, and scalable.

Security is difficult to test, predict and implement. Security is not a 'one size fits all' situation. The security needs and the recommended security strategy of each organization is unique and different. For example, an enterprise, a telecommunication provider, a network operator, or service providers each can have a unique set of business needs and may have evolved their networking environment to meet these needs.

A closed enterprise, for example, uses logical (e.g., frame relay) or physical private lines between sites, remote access provided selectively for employees needing access into the Internet. Web presence is achieved through an Internet data centre provided by a service provider (who is responsible for establishing a secure environment). The organization also provides conventional dial access for remote employees (e.g., working from a hotel). The company uses private e-mail among employees with no external access. Wireless LANs are also used.

An extended enterprise or a telecomm provider, network operator or service provider, through various business models, can provide support for remote employee and remote office access over IP VPNs over the Internet, or deliver higher speed, lower cost connectivity including general-purpose access into the Internet, such as interworking between internal e-mail systems and the rest of the world.

In an open enterprise, the business model can leverage the Internet by allowing partner, supplier and customer to have access to a enterprise-managed Internet data centre, even allowing selective access to internal databases and applications (e.g., as part of a supply chain management system). Internal and external users access the enterprise network from home, remote offices or other networks using wired or mobile devices. As such, the security requirement for such an enterprise is different from other enterprises.

A summary of enterprise types is given in Figure 7-1.

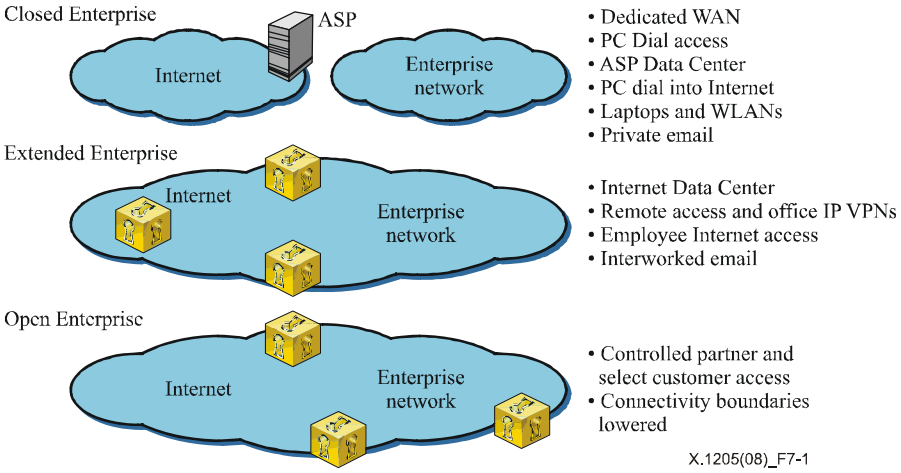

Figure 7-1 – Generic enterprise types

Cybersecurity requires risk management. This process involves the task of identifying the collective set of components that need to be protected. In order to facilitate the risk analysis, it is beneficial to consider attacks as belonging to the following categories:

1) Service interruption attacks: These types of attacks disable user access to the targeted services either temporary or permanently. Examples include lack of access to a web site, or the inability to conduct a financial transaction, or the ability to initiate a voice call. Several types of attacks can lead to service disruption. For example, denial of service (DoS), distributed denial of service attacks (DDoS), or damaging of buildings that host critical infrastructure could result in preventing users from accessing a service.

2) Assets compromise: These types of attacks involve theft or misuse of infrastructure. Attacks of this type can have an impact on cybersecurity if carried on a large scale.

3) Component hijacking: These types of attacks involve taking control of some devices and then using them to launch new attacks against other components of the cyber environment.

Any element of the cyber environment can be viewed as a security risk, which is generally thought of as a combined assessment of threat. Threat analysis includes the task of describing the type of possible attacks, potential attackers and their methods of attack and the consequences of successful attacks. On the other hand, vulnerability in this Recommendation refers to a weakness that could be exploited by an attacker. Risk assessment combined with threat analysis allows an organization to evaluate potential risk to their network.

Attacks can originate in the cyber environment, such as via worms or other malware, by direct attack on critical infrastructure, such as telecommunications cables, or through the actions of a trusted insider. A combination of these attacks is also possible. Risks are often characterized as high, medium, or low. The level of risk varies among different components of the cyber environment.

Security is all about risk management. In order to manage risks, many techniques can be used. For example, the development of a defence strategy that specifies countermeasures to possible attacks may be used; detection, which includes identifying an attack in progress or afterward; formulating a response to an attack that specifies the collection of countermeasures to an attack to either stop it or reduce its impact; formulating a recovery strategy that enables the network to resume operation from a known state.

7.3 Threats to cybersecurity and a methodology to address them

From an X.800 viewpoint, threats to a data communication system include the following:

a) destruction of information and/or other resources;

b) corruption or modification of information;

c) theft, removal or loss of information and/or other resources;

d) disclosure of information; and

e) interruption of services.

According to [ITU-T X.800] threats can be classified as accidental or intentional and may be active or passive. Accidental threats are those that exist with no premeditated intent. Examples of realized accidental threats include system malfunctions, operational blunders and software bugs. Intentional threats may range from casual examination, using easily available monitoring tools, to sophisticated attacks using special system knowledge. An intentional threat, if realized, may be considered to be an "attack". Passive threats are those which, if realized, would not result in any modification to any information contained in the system(s), and where neither the operation nor the state of the system is changed. The use of passive wire tapping to observe information being transmitted over a communications line is a realization of a passive threat. Active threats to a system involve the alteration of information contained in the system, or changes to the state or operation of the system. A malicious change to the routing tables of a system by an unauthorized user is an example of an active threat. Appendix I provides a brief summary of some specific types of attacks.

The X.800 security threats equally apply to the cyber environment. According to [ITU-T X.800], security features usually increase the cost of a system and may make it harder to use. Before designing a secure system, therefore, a recommended practice is to identify the specific threats against which protection is needed. This is known as threat assessment. A system is vulnerable in many ways, but only some of them are exploitable because the attacker lacks the opportunity, or because the result does not justify the effort and risk of detection. Although detailed issues of threat assessment are beyond the scope of this Recommendation, in broad outline they include:

Threats are against assets, so the first step is to list out the assets that require protection. The next step of the assessment is a threat analysis, then a vulnerability analysis (including impact assessment), countermeasures and security mechanisms.

a) identifying the vulnerabilities of the system;

b) analysing the likelihood of threats aimed at exploiting these vulnerabilities;

c) assessing the consequences if each threat were to be successfully carried out;

d) estimating the cost of each attack;

e) costing out potential countermeasures; and

f) selecting the security mechanisms that are justified (possibly by using cost benefit analysis).

In some cases, non-technical measures, such as insurance coverage, may be a cost effective alternative to technical security measures. In general, perfect technical security is not possible. The objective, therefore, should be to make the cost of an attack high enough to reduce the risk to acceptable levels.

7.4 End-to-end communications security

[ITU-T X.805] defines a network security framework for addressing end-to-end network security. [ITU-T X.805] is applicable to various types of networks where the end-to-end security is a concern. The architecture is independent of a network underlying technology.

The security architecture addresses the global security challenges of service providers, enterprises, and consumers and is applicable to wireless, optical and wireline voice, data and converged networks. The architecture addresses security concerns for the management, control, and use of network infrastructure, services and applications. [ITU-T X.805] enables proactive detection and mitigation of security vulnerabilities for the known threats. The security architecture logically divides a complex set of end-to-end network security-related features into separate architectural components. This separation allows for a systematic approach to end-to-end security that can be used for planning of new security solutions, as well as for assessing the security of the existing networks.

In [ITU-T X.805], a security dimension is a set of security measures designed to address a particular aspect of network security. [ITU-T X.805] defines eight dimensions that protect against all major security threats. These dimensions are not limited to the network, but also extend to applications and end user information. The security dimensions apply to service providers or enterprises offering security services to their customers. The security dimensions are:

1) Access control;
2) Authentication;
3) Non-repudiation;
4) Data confidentiality;
5) Communication security;
6) Data integrity;
7) Availability; and
8) Privacy.

In order to provide an end-to-end security solution, the security dimensions are applied to a hierarchy of network equipment and facility groupings, which are referred to as security layers. The following three security layers are addressed:

1) the infrastructure security layer;
2) the services security layer; and
3) the applications security layer.

The security layers identify where security is addressed in products and solutions by providing a sequential perspective of network security. For example, first security vulnerabilities are addressed for the infrastructure layer, then for the services layer and security vulnerabilities are addressed for the applications layer. Figure 7.4-1 depicts how the security dimensions are applied to security layers in order to reduce vulnerabilities that exist at each layer.

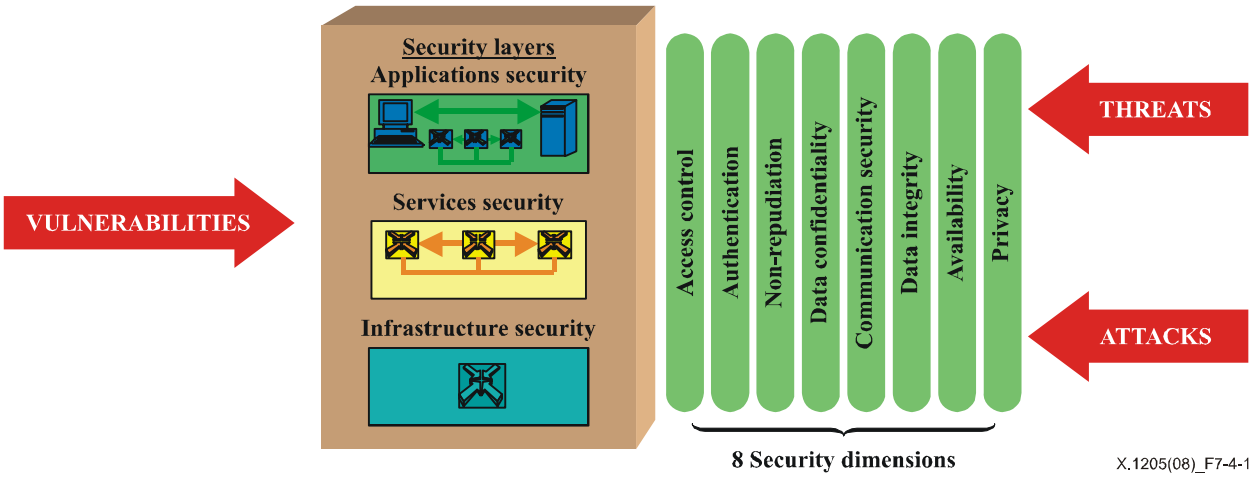

Figure 7-4.1 – Applying security dimensions to security layers

In [ITU-T X.805], a security plane is a certain type of network activity protected by security dimensions. [ITU-T X.805] defines three security planes to represent the three types of protected activities that take place on a network. The security planes are:

1) the management plane;

2) the control plane; and

3) the end-user plane.

These security planes address specific security needs associated with network management activities, network control or signalling activities, and end-user activities correspondingly. [ITU-T X.805] suggests that networks should be designed in such a way that events on one security plane are kept isolated from the other security planes. For example, a flood of DNS lookups on the end-user plane, initiated by end-user requests, should not lock out the OAM&P interface in the management plane that would allow an administrator to correct the problem.

Figure 7.4-2 illustrates the security architecture with the security planes included. The concept of security planes allows the differentiation of the specific security concerns associated with those activities and the ability to address them independently. For example, in a VoIP service, which is addressed by the services security layer, the task of securing the management of the service should be independent of the task of securing the control of the service. The task is independent of the task of securing the end-user data being transported by the service (e.g., the user's voice).

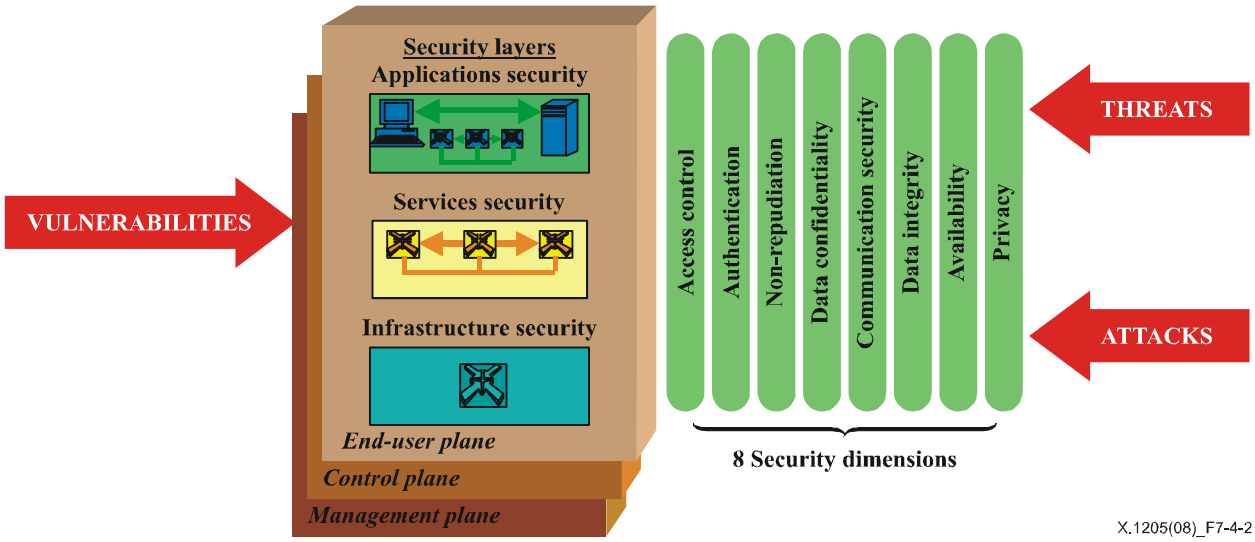

Figure 7-4.2 – Security planes reflect the different types of network activities

8 Possible network protection strategies

Security includes all the architectural layers of a network. This approach provides a good starting point for the design of secure networks. This decomposition enables a higher layer to define their own security requirements at that specific layer, and also enables it to use the security services of the lower levels. The layered security approach allows the development of flexible, scalable security solutions across the network level, application level and management level for all organizations.

8.1 Closed loop policy management

A properly designed and implemented security policy is an absolute requirement for all types of enterprises and organizations. The security policy typically is a living document and process, which is enforced, implemented and updated to reflect the latest changes in the enterprise or organization infrastructure and service requirements.

The security policy clearly identifies the resources in the organization (also the enterprise) that are at risk and resulting threat mitigation methodologies. The security policy provides for performing vulnerability and risk assessment, and defines appropriate access control rules. Risk and vulnerability assessment are performed at all levels of the network. The policy is able to help identify and discover security violations, and states the specified violation responses.

It is recommended that IT and network administrators use tools to perform vulnerability assessment on their networks. The principle of the least privilege access is followed. IT and network administrators tasks include to ensure that audits trails are reviewed, thus closing the loop on policy management. If problems are discovered in the audits, IT and network administrators ensure that the policy is updated to reflect the revised actions.

A security policy that is not enforced is worthless. The enforcement of the security policy is dependent on people. There should be clear responsibility and accountability for policy enforcement.

8.2 Uniform access management

The term access management is used to define systems that may make use of both authentication and authorization services in order to control the use of a resource. Authentication is the process in which a user or entity requests the establishment of an identifier to a network. Authorization determines the level of privileges of that entity based on access control. The control of the level of access is based on a control policy definition and its enforcement. Figure 8-2 depicts the reference model for secure authentication and authorization.

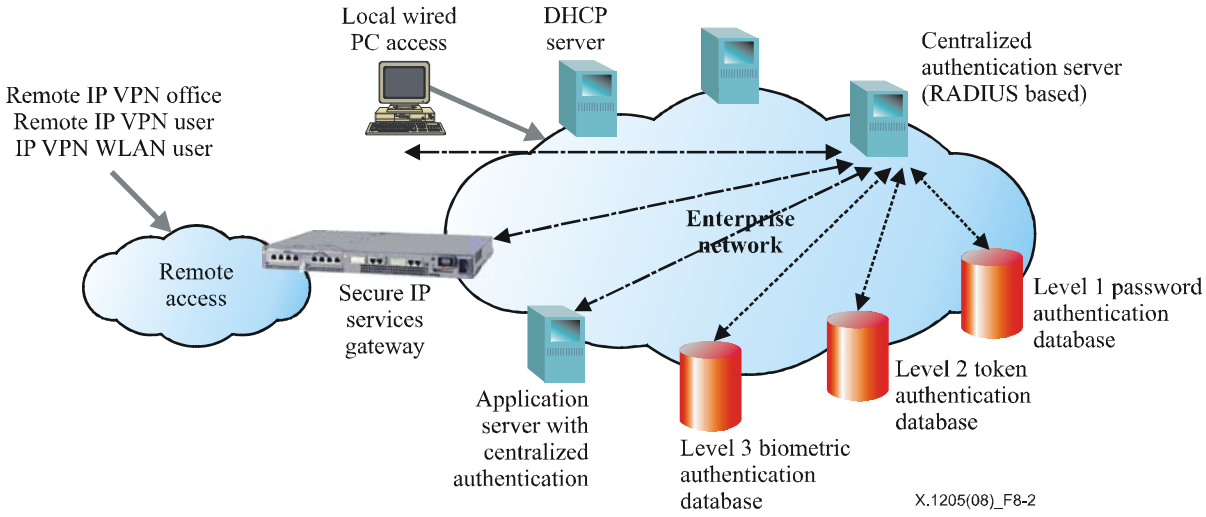

Figure 8-2 – Secure authentication and authorization reference model

From Figure 8-2, the following recommendations are given:

1) The use of a centralized authentication mechanism in order to facilitate administration and remove the need for locally stored passwords. (Locally stored passwords tend to be static and weak.)

2) The use of a centralized authorization system, tightly coupled with authentication system, with appropriate granularity for the particular enterprise.

3) Enforcement of strong (complex) passwords rules for all passwords.

4) Secure storage of all passwords in a one-way encrypted (hashed) format.

5) The principle of simplicity that implies ease of use and ease of administration. A simple system is a secure system since safeguards are much more likely to be followed.

6) Secure logging of all security related events with respect to authentication and authorization.

Approaches to access management include: IP source filtering, proxies and credential-based techniques. Each approach has its advantages and limitations. Depending on the type of the enterprise and within a given type, more than one or a combination of approaches may be used. For example, an enterprise may choose to manage access for workstations using IP source filtering, and may choose to use a credential-based scheme for other users.

Several methods can be used to authenticate a user. Techniques include: passwords, one-time pass, biometric techniques, smart cards, and certificates. Passwords-based authentication must use strong passwords (e.g., that are at least eight characters in length with at least one alphabetic, one numeric and one special character). Password authentication alone may be insufficient. Based on vulnerability assessment, it may be necessary to combine password authentication with other authentication and authorization processes, such as certificates, lightweight directory access

protocol (LDAP), remote authentication dial-in user service (RADIUS), Kerberos, and public key infrastructure (PKI).

All authentication mechanisms have advantages and drawbacks. UserID/password combinations are simple, low cost, and easy to manage; however, remembering a multitude of complex passwords is very difficult for users. Two-factor and three-factor authentication systems add additional authentication strength; however, all are costly, add additional complexity and are difficult to maintain.

A "single password" system with enforced strong passwords can be a good solution for enterprise authentication and authorization. Such system provides high authentication security, granular authorization, and is easier to administer. With this system, a user's strong single password is synchronized with many applications and systems enterprise wide for authentication and authorization. All enterprise systems and applications automatically refer authentication and authorization functions to the single password system. As users only have to remember is one strong password making the system simple to use and not likely to be bypassed. The advantages to single-password system are:

- Single consistent method for setting passwords.
- Single consistent method for authentication and authorization.
- Single method for registration and termination of user accounts.
- Enforcement of corporate password strength guidelines.
- Consistency – users know what to do.
- Standardization – easy to support and adopt.
- Fast – standard interface and APIs.
- Lower costs, lower help calls.

The open and the extended enterprise face the most challenges when designing their access management policy. It is advantageous to consider access management as an integral component of the security policy. These organizations should design of a uniform access management system with fine-grained rules that properly interfaces with:

- Directories and databases holding identity attributes
- Multiple authentication systems such as password, Kerberos, TACACS and RADIUS
- Hosts, applications and application servers.

The uniform access management system performs session management per user after the user is authenticated. The use of flexible configuration and policy enforcement with fine-grained rules that is capable of dealing with specific objects is recommended. Appropriate monitoring, accounting and secure audit trails. The use of unique accounts for each administrator with accountability for actions traceable to individuals is recommended.

8.3 Secure communications

Unified networks can carry voice, data and video packets. The objective of securing network traffic is to ensure the confidentiality, integrity and accuracy of network communications. Security should be available for call and signalling traffic in telephony networks. Encryption technology is used for data and voice and mobile networks.

Encryption can be achieved by:

- VPN techniques using IPSec, with authentication header (AH) and encapsulating security payload (ESP) or tunnelling through the use of layer 2 tunnelling protocol (L2TP).
- Key management based on Internet key exchange (IKE).
- Certificate management based on public key infrastructure [b-ITU-T X.509] (PKIX).

- Certificate management protocol (CMP) (see [b-IETF RFC 2510]) and online certificate status protocol (OCSP) (see [b-IETF RFC 4557]).
- In the application layer, through the use of TLS (see [b-IETF RFC 4366]) with strong keys.

It is important to use standards based encryption algorithms and hashes such as DES, 3DES; AES, RSA and DSA (see [b-IETF RFC 2828]). MD5 (see [b-IETF RFC 1321]) and SHA-1 (see [b-IETF RFC 3174]) could be used for message integrity, and Diffie-Hellman (see [b-IETF RFC 2631]) and RSA (see [b-IETF RFC 2828]) for key exchange.

NOTE – NIST (National Institute of Standards and Technology) now encourages the use of SHA-256 (Secure Hash Algorithm with 256-bit encoded keys) instead of SHA-1.

The wired equivalent privacy (WEP), as defined in [b-IEEE 802.11] standards, defines a technique to protect the over-the-air transmission between wireless LAN (WLAN) access points and network interface card (NIC)s. This protocol has been shown to be insecure. Added measures of protection such as IPSec are necessary to secure WLAN over WEP. Alternatively, the Wi-Fi protected access (WPA) can be used for added protection.

8.4 Variable depth security

A VLAN is a group of network devices, such as servers and other network resources, that is configured to behave as if they were connected to a single, network segment. In a VLAN, the resources and servers of other users in the network will be invisible to each of the other VLAN members. VLANs help meet performance needs by segmenting the network more effectively. VLANs restrict the dissemination of broadcast as well as node-to-node traffic, so the burden of extraneous traffic is reduced throughout the network. In VLANs all packets travelling between VLANs may also pass through a router, as such router-based security measures can be implemented to restrict access to the segment.

Security layering results in the ability to offer variable depth security. Each additional security level builds upon the capabilities of the layer below. Each additional security level provides finer and finer grained security.

For example, basic network compartmentalization and segmentation can be achieved by VLANs. This allows various business functions to be contained and segmented into their own private local area networks with cross-traffic from other VLAN segments controlled or prohibited. There are several benefits derived from the deployment of VLANs across an organization multiple sites. For example, the use of VLAN "tags" allows the segregation of traffic into specific groups such as finance, HR and engineering. Separation of data without "leakage" between the VLANs is an important element for security.

A second layer of security can be achieved through the use of perimeter and distributed firewall-filtering capabilities at strategic points within the network. The firewall layer allows the network to be further segmented into smaller areas, and enables secure connections to the public network. Firewalls limit access to inbound and outbound traffic to those protocols that are explicitly configured within the firewall. Additionally, an authentication capability for incoming or outgoing users can be provided. Those firewalls that support network address translation (NAT) enable optimization of IP addressing within the network as specified in [IETF RFC 1918] (address allocation for private internets).

The use of firewalls provides an extra layer of protection that is useful for access control. The application of policy-based access allows the customization of access based on business needs. The use of a distributed firewall approach affords the additional benefit of scalability as the enterprise needs evolve. Personal firewalls can be deployed on end systems to ensure application integrity.

Layer 3 VPNs can be added as a third layer for enhanced security. VPNs provide a finer granularity of user access control and personalization. VPNs provide very fine grain security down to the individual user level and enables secure remote access for remote sites and business partners. With

VPNs the use of dedicated lines is not necessary. The use of dynamic routing over secure tunnels across the Internet provides a highly secure, reliable and scalable solution. The use of VPNs in conjunction with the use of VLANs and firewalls allow the network administrator to limit the access by a user or user group based upon policy criteria and business needs. VPNs provide stronger assurance of data integrity and confidentiality. Strong data encryption can be enabled at this layer for providing confidentiality and data integrity.

Security solutions based on the layered approach are flexible and scalable. The solution is adaptable to the security needs of enterprise.

8.5 Securing management

Whether considered a "best practice" or an integral part of an organization or enterprise security architecture, a secure management channel or plane is the foundation for all other elements of the network's management, performance and survivability. Figure 8-5 proposes a possible reference model for securing network management for network operations centre (NOC).

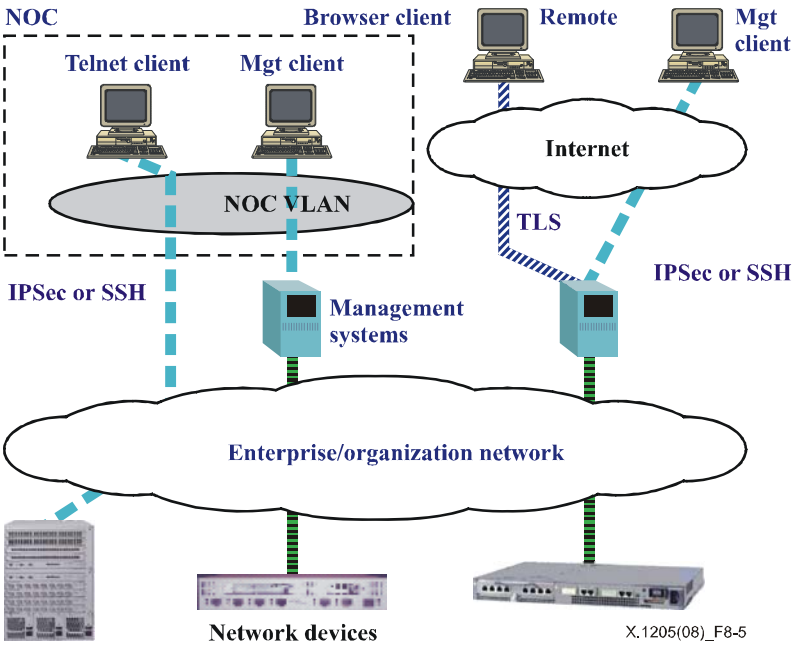

Figure 8-5 – Reference model for securing management

Secure management is a holistic approach rather than a security feature set on a given network element. For that reason, the recommended approach in this Recommendation covers critical areas of network infrastructure and provides specific actions to mitigate potential threats to the network. Each of the subject areas below represents a critical component that requires security attention to ensure a cohesive fabric of protection around the network.

There are nine key network management domains that are to be addressed by security before a network's management plane can be considered secure. The domains are:

- Secure activity logs
- Network operator authentication
- Access control for network operators
- Encryption of network management traffic
- Secure remote access for operators
- Firewalls

- Intrusion detection
- OS hardening
- Virus free software

8.5.1 Policy management

Secure logs can be used to maintain an audit trail of user or administrator activities and events generated by the device itself, this being a critical element of closing the loop on policy management. The raw data collected is called the "audit log", and the verifiable path of events through the audit logs is referred to as the "audit trail". In order to be effective, security audit logs have to contain sufficient information for after-the-fact investigation or analysis of security incidents. These audit logs provide a means for accomplishing several security-related objectives, including individual accountability, reconstruction of past events, intrusion detection and problem analysis. Logs can also be used for long-term trend analysis. Audit log information helps identify the root cause of a security problem and prevent future incidents; this information should be securely stored. For instance, audit logs can be used to reconstruct the sequence of events that led up to a problem, such as an intruder gaining unauthorized access to system resources, or a system malfunction caused by an incorrect configuration or a faulty implementation.

8.5.2 Secure access management

Network operator authentication should be based on strong centralized authentication of network operators and administrators. Centralized administration of passwords enables enforcement of password strength and removes the need for local storage of passwords on the network elements and EMS systems. RADIUS is the basic mechanism of choice for automating centralized authentication.

Good practice for access control for network operators should be used. For example, to determine the authorization level, techniques based on RADIUS servers can be used to provide a basic level of access control; with the addition of an LDAP server to provide more fine grained access control should this be necessary.

8.5.3 Encryption of network management traffic

Encryption is recommended for all data traffic used in a network management capacity to ensure data confidentiality and integrity. Corporations are increasingly using in-band network management and thus separation of management traffic through the use of encryption is necessary. Encryption of management traffic provides a high degree of protection against insiders with the exception of the small group of insiders that have legitimate access to the encryption keys. Encryption between network operations centre (NOC) clients and element management system (EMS) servers and/or network elements should be provided. This includes SNMP traffic, because there are known vulnerabilities with SNMP v1 and v2; these are addressed in SNMP v3. Depending on traffic type, the security protocols to use for these links are TLS, IPSec and secure shell (SSH) (see [b-IETF RFC 4252]). SSH is an application level security protocol that directly replaces Telnet (see [b-IETF RFC 854]) and FTP (see [b-IETF RFC 959]), but cannot normally be used to protect other traffic types. IPSec protocol, on the other hand, runs just between the network layer (layer 3) and the transport layer (layer 4) and can be used to protect any type of data traffic independent of applications and protocols used. IPSec is the preferred method to use; however, SSH can be used if the traffic consists of Telnet and FTP only. TLS technology can protect HTTP traffic when used in a network management capacity between the NOC clients and the EMS and/or network elements. External IPSec VPN device can be used in various parts of the network to secure management traffic.

8.5.4 Secure remote access for operators

Security has to be provided for operators and administrators who manage the network from a remote location over a public network. Providing a secure virtual private network using IPSec is the preferred solution, as this will provide strong encryption and authentication of all remote operators. For example, a VPN product could be placed at the management system interface and all operators should be equipped with extranet access clients for their laptop or workstations.

8.5.5 Firewalls

It is a good practice for the application of variable depth security principles to partition the network management environment through the use of VLANs and firewalls. The firewall controls the type (protocol, port number, source and destination address) of traffic used to transit the boundary between different security domains. Depending on the type of firewall (application versus packet filtering), this can also be extended to include filtering of the application content of the data flow. Firewall placement, type, and filtering rules are specific to the particular network implementation.

8.5.6 Intrusion detection

Host-based intrusion detection systems can be incorporated into management servers to provide defence against network intrusions. Intrusion detection systems can be used to warn network administrators of the possibility of a security incident such as a server compromise or denial-of-service attack.

8.5.7 Application security layer

Hardening of all operating systems used in network management capacity is recommended. For this, all operating systems used in a network management capacity are to be hardened whether they are general purpose operating systems or embedded real-time operating systems. For operating systems where no specific hardening guide exists, the operating system manufacturer should be consulted to obtain the latest hardening patches and procedures.

8.5.8 Virus free software

All software, whether developed in-house or bought from a 3rd party, has to be examined and ensured to be virus free to the maximum reasonable extent possible. A process has to be developed for virus checking which will involve scanning all software with a specified virus detection tool before incorporating the software into a product.

8.6 Layered security across the application, network and network management

Every organization or enterprise has a different security threshold and different technology infrastructure. Internet enabled applications represent increased risks and threats to the enterprise. Internet applications can have built-in security at the application level. However, using the security functionality that could be provided by lower network layers can enhance the security of these applications.

Enterprises with Internet presence are cautioned to use extreme care in designing their sites. [b-IETF RFC 2196] (Site Security Handbook) provides a good reference that discusses site security. At the application level, it is recommended that fine-grained security policy be used. Where possible, objects should be addressable at the uniform resource identifiers (URI) level. Unneeded functionality should be disabled. Where possible, TLS should be used. It is recommended to use application level gateways and focus on providing strong authentication and authorization. If the security infrastructure allows, e-mail services should be secured using S/MIME (see [b-IETF RFC 2311]) or techniques such as PGP (see [b-IETF RFC 1991]).

At the network layer, the techniques as discussed in clause 8.7, are recommended for use to ensure acceptable security for the enterprise. The security is achieved through the use of layered architecture that can be customized as per the security requirements for each type of the enterprise.

Securing network management traffic is an essential requirement for securing the network. This can be achieved by first ensuring that the operating system is hardened against known threats. The operating system manufacturer should be consulted to obtain the latest OS hardening patches and procedures. Steps should be performed to check that all installed software is free from known viruses. It is preferable to encrypt all management traffic all the time using IPSec or TLS to protect HTTP traffic. Encryption is a good and recommended practice if the traffic is travelling outside the local LAN. SNMPv3 and RADIUS are recommended for remote access control for network operators, with multiple levels of control mechanisms that include the use of strong passwords and the ability to centrally administer access control system is preferred. Secure logs are essential for logging network management traffic.

8.7 Network survivability even under attack

In today's environment, the enterprise network supports mission-critical operations and is essential for conducting business. The network is assumed to be secure, reliable and available for business partners all the time.

There are many techniques that could be used to ensure network reliability. Network reliability ensures the appropriate operation of a network when software and/or hardware components fail. However, when security threats are present, the concept of survivable networks is the paradigm. A survivable network is a network that continues to fulfil a minimum set of essential functionality in a timely manner in the presence of attacks. Essential functionality consists of delivering in a timely manner essential services, even if parts of the network are unreachable or have failed due to an attack.

The design of survivable networks starts by organizing the network services into two categories, essential services and non-essential services. Survivability means that a network is able to resist an attack. A clear strategy is needed and to state how to deal and recover from an attack. Depending on the type of attacks, there may be several resistance, identification and recovery strategies that the network administrator may want to consider. One characteristic of survivable network is adaptability. For example, the network can re-route traffic from one server to another if an intrusion or an attack is detected on the first server.

During the security policy design phase, it is necessary to determine the essential services that a network is expected to deliver even under attack. This phase identifies how a network will resist an attack, how the network will overcome such attacks and the best approach for recovering from such attacks. Management systems, hosts, applications, routers and switches are all typical elements to be considered in the analysis.

The resistance of survivable network to attacks is increased by the use of access control mechanisms with strong authentication and encryption. The use of message and packet filtering, and network and server segmentation also enhances network resistance to attacks. The use of appropriate intrusion detection techniques can help to identify an attack. Appropriate back-up techniques can be used for system and network recovery.

Appendix I

Attackers techniques

(This appendix does not form an integral part of this Recommendation)

This appendix briefly reviews some of the attacks of particular concern in a data processing and data communications environment.

I.1 Taxonomy of security threats

IT professionals are advised to view their network as a resource that will be accessed from users that, in general, cannot be trusted. There are many tools, techniques and methodologies that are available for attackers to compromise a network. Hackers can use these tools to launch multi-level attacks in order to access the network. In some cases, the attacker will exploit a security compromise and then use secondary attacks to exploit other parts of the network.

This clause describes the techniques, tools and methodologies used by attackers, hackers and intruders to compromise a network.

I.1.1 Authorization threats

Unauthorized access to network resources is usually the result of improper system configuration and usage flaws. Attackers can obtain unauthorized access by taking advantage of insufficient authentication and authorization of users and tasks in corporate systems or sloppy employee practices (e.g., posting of passwords, when the user is forced to remember multiple passwords).

Practices, such as the improper allocation of hidden space, and sharing privileges among applications, represent serious sources of vulnerabilities. Trapdoor attacks can be used to obtain unauthorized access. For example, attackers can obtain unauthorized access by guessing user names and passwords using a dictionary of common strings. Attackers can derive passwords by algorithmic means. Passwords can be captured in transit if they are sent in the clear.

After guessing the user name and the associated password, the attacker will have access to the organization resources. The level of access is dependent on the privileges that the compromised account has. The amount of damage that the attacker can inflict on the organization is dependent on his or her intent. In most cases, hackers will use the compromised account to install a backdoor entry to the enterprise.

Protocols for remote access to e-mail such as IMAP, POP3 and POP2 use simple username and password authentication techniques. These protocols can be used to facilitate brute force attacks. There are published methods that allow attackers to remotely exploit the services of these protocols.

There are even more sophisticated ways of gaining unauthorized access. Worms can be used to perform system-spoofing attacks whereby one system component masquerades as another. For example, worms can exploit flows in the debug option of sendmail and in .rhosts (e.g., used in UNIX) due to weak authentication. The debug option of sendmail can be turned OFF. Leaving the option ON is an example of usage flaw.

I.1.2 IP spoofing

IP spoofing is a complex attack that exploits trust relationships. Using masquerade techniques, the attacker hijacks the identifiers of a host in order to sabotage the security of the target host. As far as the target host knows, it is carrying on a conversation with a trusted host.

In this assault, the attacker first identifies a trusted host whose identifier will be hijacked. This could be accomplished by first determining the patterns of trust for the host. This usually involves the determination of the range of IP addresses that the host trusts. The next step involves the disabling of the host, since the attacker will hijack its identifiers. This could be achieved by the use of techniques such as TCP SYN flooding attacks.

IP Spoofing attacks can succeed because it is easy to forge IP addresses and due to the limitations of network-based address authentication techniques. The IP spoofing attack is blind, since the attacker may not have access to the responses from the target host. However, the attacker can obtain a two-way communication if the routing tables are manipulated to use the spoofed source IP address. IP spoofing attacks are often used as a first step for other assaults such as denial of service (DoS) and flooding attacks.

It would be reasonable to note that most (but certainly not all) ISPs, and many of the more-responsible enterprise networks, are now doing outgoing address filtering, which precludes straight IP spoofing attacks. In response to this, attackers have been busy accumulating "bot nets" in order to maintain their anonymity.

I.1.3 Network sniffers

Network sniffers were originally designed as an aid tool to network managers to allow them to diagnose problems, perform analysis or improve the performance of their networks. Network sniffers work in a network segment that is not switched, such as segments that are connected through a hub. In this way, the sniffer can see all traffic on that segment.

Older sniffers read packet headers of the network traffic and focused on identifying low-level packet characteristics, such as source and destination address. However, current sniffers can decode data from packets across all layers of the OSI model.

Attackers can use sniffers to view user information and passwords from packets across public or private networks. By using sniffers, attackers can obtain valuable information about user names and passwords, in particular from applications such as FTP, telnet and others that send passwords in the clear. Protocols for remote access to e-mail such as IMAP, POP3 and POP2 use simple username and password authentication techniques and are susceptible to sniffer attacks.

Since users tend to reuse passwords across multiple applications and platforms, attackers can use the acquired information to obtain access to various resources on the network, where their confidentiality could be compromised. Moreover, these resources could also be used as launch pads for other attacks.

In general, attackers are able to use networks sniffers by compromising the physical security of the corporation. This is equivalent to someone walking into the enterprise and plugging his or her laptop to the network. The risks are also applicable to wireless networks, whereby someone in the parking lot can acquire access to the corporation local network. Gaining access to the core packet network allows the attacker to determine configurations and modes of operation for further exploitation.

I.1.4 Denial of service

DoS attacks focus on preventing legitimate users of a service from the ability to use the service. DoS attacks are easy to implement and can cause significant damage. DoS attacks can disrupt the operation of the enterprise and effectively disconnect from the rest of the world. Distributed denial of service attacks uses the resources of more than one machine to launch synchronized DoS attacks on a resource.

DoS attacks can take various forms and target a variety of services. DoS attacks focus on exhausting network, servers, host and application resources. Some DoS attacks focus on disrupting network connectivity. For, example, the SYN flooding attack uses bogus half-open TCP connection requests that exhaust memory capacity of the targeted resource. These types of attacks can prevent legitimate users from accessing hosts, web applications and other network resources. DoS attacks can:

- Deny network connectivity to the Internet
- Deny network element availability to legitimate users
- Deny application availability to legitimate users

DoS attacks exploit weaknesses in the architecture of the system that is under attack. In some cases, it exploits the weakness of many common Internet protocols, such as the Internet control message protocol (ICMP). For example, some DoS attacks send large number of ICMP echo (ping) packets to an IP broadcast address. The packets use a spoofed IP address of a potential target. The replies coming back to the target can cripple it. These types of attacks are called smurf attacks. Another form of attacks uses UDP packets but work on the same concept.

I.1.5 Bucket brigade attacks

Bucket brigade attacks are also known as man-in-the-middle attacks. In this kind of assault, the attacker intercepts messages in a public key exchange between a server and a client. The attacker retransmits the messages, substituting their public key for the requested one. The original parties will think that they are communicating with each other. The attacker may just have access to the messages or may modify them. Network sniffers can be used to launch such attacks.

I.1.6 Back door traps

Back doors are quick methods of access network resources that could:

- Have been deliberately placed by system developers to allow quick access during development and have not been turned off upon delivery
- Have been placed by employees to facilitate performance of their duties
- Be part of standard operating system installs, that have not been eliminated by hardening such as default user logon ID and password combinations
- Be placed by disgruntled employees to allow access after termination
- Have been created by the execution of malicious code, such as viruses.

I.1.7 Masquerading

This entails pretending to be either a valid maintenance or engineering personal, in order to access the network, and is just the tip of the iceberg of a range of threats that build on physical security holes and human vulnerabilities. For example, the intruder can modify data relating to configuration management and signalling layers of network, as well as to billing and usage data.

I.1.8 Replay attacks

This attack occurs when a message, or part of a message, is repeated to produce an unauthorized effect. For example, an entity replies a valid message containing authentication information in order to authenticate itself.

I.1.9 Modification of messages

Modification of a message occurs when the content of a data transmission is altered without detection and results in an unauthorized effect.

I.1.10 Insider attacks

Insider attacks occur when legitimate users of a system behave in unintended or unauthorized ways. Many known computer crimes involve insiders that compromise the security of the system. Careful screening of staff and continued securitization of hardware, software and security policy can help to reduce risks of insider attacks. Having good audit trails to increase the likelihood of detecting such attacks is also a good practice to follow.

I.2 Security threats

All types of organizations such as enterprises face a wide range of threats. The security needs and the recommended security strategy of each organization is unique and different. The most demanding environment from a security perspective is that of the open enterprise. In this case, security needs to be addressed across the enterprise to control employee, partner and even customer access to enterprise databases and applications.

I.2.1 Application layer attacks

Application layer attacks can take various forms and use various methods. Since web hosts are accessible by the public at large at known ports addresses as specified by protocols such as HTTP (port 80), hackers can use this knowledge to launch attacks that are capable of bypassing firewalls.

Application layer attacks exploit vulnerabilities in the operating system and applications to gain access to resources. Improper configuration and authorization can lead to security holes. For example, a host might be a web server, and should provide anyone with requested web pages. Security policy could specify that hosts restrict shell command access to authorized administrators.

Account harvesting targets the authentication process when an application requests a user logon ID and a password. Applications that generate different error messages for wrong user logon ID and wrong password are vulnerable to this type of attack. Based on the type of error message, an intruder can customize an attack that first determines a valid user logon ID and then uses other form of password cracking techniques to obtain the password.

Application layer attacks can be based on viruses, worms, buffer overflow and password harvesting among others. The advent of web services and single sign-on technologies only aggravate the problem, since they tend to web-enable legacy-based applications. These applications were not designed with web connectivity and security in mind.

Some application layer attacks are aimed at just dismantling the web site. Other attacks poison a web site's cookies to gain illegitimate information about a particular server. Applications in general do not check the validity of cookies, and can become the victims of executing malicious code that is hidden in the cookies. There are known vulnerabilities in current browsers that allow cookies based attacks.

An attacker may also use cross-site scripting technique to insert malicious code in the form of a script tag that is added to a URL. The code will be executed when an unsuspected user clicks on that URL. The use of TLS can solve some of the problems of the security at the application layer. However, SSL does not fully protect web applications. Attacks, such as account harvesting, password cracking, can still be launched even if SSL is used.

To reduce the threats of application layer attacks, it is recommended to harden all operating systems used in a network management capacity whether they are general purpose operating systems or embedded real-time operating systems. Specific and up-to-date hardening guides that are available from the manufacturer should be followed. For some legacy systems using older operating systems, no security patches might be available from the manufacturer. It is also recommended to use secure e-mail, application layer firewalls, host intrusion prevention and detection systems, strong authentication techniques, strong passwords, and proper exit control in web sites that prevent displaying of unauthorized modifications web content.

I.2.2 Network layer threats

An attacker may use the tools of the trade to launch network layer attacks of various severities. Extended and open enterprise is particularly vulnerable to network layer attacks. A number of serious security threats are commonly associated with the network infrastructure. These threats include sabotage, vandalism, bad system configuration, and denial of service, snooping, industrial espionage and theft of service. Attacks may be launched from inside the network by insiders and also from external sources such as hackers.

Recent developments in hacker technology, such as mobile terminal based port scanners, demonstrate that attacks on network infrastructure can originate from the mobile terminal as well. It is recommended that a good security policy and a well-understood security process be developed to protect the network infrastructure. Switches, routers, access points, remote access servers, wireless access points, hosts and other resources are typical assets that deserve protection.

Network infrastructure threats and vulnerabilities, which are typical to IP packet networks:

1) Proliferation of insecure protocols: Some networks still use protocols that are known to have security vulnerabilities. Such protocols include: ICMP, TELNET, SNMPv1&2, DHCP, TFTP, RIPv1, NTP, DNS, and HTTP.

2) Use of weak, locally managed, static passwords: Some networks still allow the use of weak passwords that are based on short, common dictionary words that are easy to guess. Some administrators may use one password across network elements, which may be shared and would be known by all administrators.

3) Unprotected security information: In some networks, critical information such as password files is not encrypted. Other information, such as passwords, is sent in the clear across the network. Firewall rule sets are improperly set and weak cryptographic keys are used.

4) Unauthenticated software loads and configuration files: Threats to networks can come from loading incorrect or malicious software, or configuration files can cause loss of service and may result in poor performance. This practice open security holes such as the installation of Trojan horses or other malicious code by insiders or outsiders. The practice also leads to incorrect configurations on devices.

5) Non-hardened network elements and operating systems: Threats to networks can arise from factory default operating system loads that are not hardened against common attacks. This includes the running of unnecessary services, with default accounts and passwords left enabled.

6) Management ports and interfaces unnecessarily exposed to the public network: Threats to networks can arise from in-band management interfaces that are left accessible to the public Internet. Additional threats can arise from support mechanism abuse, such as access to core network in a support mode via dial-up, ISDN or other connection.

I.2.3 Unauthorized access

Unauthorized access is a term that can refer to a number of different kinds of attacks. The ultimate goal of the attacker is to gain access to some resource illegitimately. This is a security problem for all types of enterprises. Any enterprise that enables Internet access or remote LAN access capabilities is susceptible for unauthorized access attacks.

Remote access services that enable travelling employees to dial in for e-mail access, remote offices connected via dial-up lines, intranets, and extranets that connect outside parties to the enterprise network can cause the network to be vulnerable to hackers, viruses, and other attackers. Hackers can use the tools of the trade to acquire access to the enterprise network where sensitive information can be jeopardized, or the network can be used to launch attacks against other networks.

Protecting the network at various levels can help to prevent unauthorized access. At the network layer, the use of firewalls, proxy servers, and user-to-session filtering can add additional protection, but hackers seem to get smarter all the time. Using user access control at the network and application level with appropriate authentication and authorization can also minimize the risks of unauthorized access.

I.2.4 Eavesdropping

Eavesdropping is a difficult threat to detect. The aim of the attacker here is to listen and most properly record raw data on the enterprise LAN. This attack uses "promiscuous mode" of the off-the-shelf Ethernet adaptors that are sold in the market. This mode allows an attacker to capture every packet on the network. There are plenty of free network sniffers on the web today that an attacker can use for eavesdropping.

Any type of enterprise that allows remote access is vulnerable to such an attack. The open and the extended enterprise are at the highest risk. Ethernet switching is completely ineffective against eavesdropping threats, since ARP spoofing can completely subvert the switching mechanism. Only the "lazy eavesdropper" would be hampered by Ethernet switching. The use of strong access management techniques and encryption can minimize the threat of such attacks.

Appendix II

Fields of cybersecurity technologies

(This appendix does not form an integral part of this Recommendation)

The sophistication and effectiveness of attack technology is always advancing. Nowadays, intruders can quickly develop attacks to exploit vulnerabilities discovered in products. Attackers can automate these attacks and make them available for use for the general public. Examples of available field of technologies to combat cyber threats are provided in Table II.1.

Table II.1 – Cybersecurity technologies

Techniques	Category	Technology	Purpose
Cryptography	Certificate and public key architecture	Digital signatures	Used to enable the issuance and maintenance of certificates to be used in digital communications
		Encryption	Used encryption of data during transmission or storage
		Key exchange	Establish either a session key or a transaction key to be used to secure a connection
	Assurance	Encryption	Insures data authenticity
Access control	Perimeter protection	Firewalls	Control access to and from a network
		Content management	Monitors traffic for non-compliant information
	Authentication	Single factor	A system that uses user ID/password combinations to verify an identifier
		Two factor	A system that requires two components in order to grant a user system access, such as the possession of a physical token plus the knowledge of a secret
		Three factor	Adds another identification factor such as a biometric or measurement of a human body characteristic
		Smart tokens	Establish trusted identifiers for users through a specific circuitry in a device, such as a smart-card
	Authorization	Role based	Authorization mechanisms that control user access to appropriate system resources based on its assigned role
		Rule based	Authorization mechanisms that control user access to appropriate system resources based on specific rules associated with each user independent of their role within an organization

Table II.1 – Cybersecurity technologies

Techniques	Category	Technology	Purpose
System integrity	Antivirus	Signature methods	Protect against malicious computer code, such as viruses, worms, and Trojan horses using their code signatures
		Behaviour methods	Checks running programs for unauthorized behaviour
	Integrity	Intrusion detection	Can be used to warn network administrators of the possibility of a security incident, such as files on a server are compromised
Audit and Monitoring	Detection	Intrusion detection	Compare network traffic and host log entries to match data signatures that are indicative of hackers
	Prevention	Intrusion prevention	Detect attacks on a network and take actions as specified by the organization to mitigate the attacks. Suspicious activities trigger administrator alarms and other configurable responses
	Logging	Logging tools	Monitor and compare network traffic and host log entries to match data signatures and host address profiles indicative of hackers
Management	Network management	Configuration management	Allows for the control and configuration of networks, and fault management
		Patch management	Install latest updates, fixes to network devices
	Policy	Enforcement	Allow administrators to monitoring and enforce security policies

II.1 Cryptography

Cryptography is the act of applying transformations on plain data to encipher into secret code. Deciphering of the secret data can recover the original plain text. Current available cryptography techniques can be used to encipher/decipher data. It can also be used for the authentication of a message originator and non-repudiation.

Cryptography plays an important role in protecting information while in storage within a device, or a storage medium and during its transmission over a communication link.

In cryptography, the task of enciphering data into secret code through the use of mathematical algorithms is known as data encryption. Data decryption, on the other hand, performs the inverse function, such that when applied on the encrypted data it reproduces the original data. Cryptography uses secret keys to perform the encryption and the decryption process.

Cryptographic techniques can be divided into two basic types: symmetric key and asymmetric key.

1) Symmetric key cryptography uses algorithms in which the encryption key and the decryption key are the same. The security of the model depends on the difficulty of guessing the key. Communicating parties agree on a key and keep the key secret from others. Examples of symmetric key algorithms include the triple data encryption standard (3DES) and the advanced encryption standard (AES).

2) Asymmetric key cryptography uses algorithms that use a key to encrypt the data and a different one to decrypt the ciphered text. In this type of cryptography, the user will have a private key that is only known to the user and a public key that can be known by others. The public key is used by others to encrypt plaintext. Only the holder of the corresponding private key will be able to decrypt the enciphered text.

Symmetric key cryptography techniques are, in general, faster to compute than asymmetric ones. However, the main complication with symmetric key cryptography is the key distribution problem. As such, they usually do not scale for large deployments. On the other hand, asymmetric key cryptography (also known as public key cryptography) solves some of the key management limitations of symmetric key cryptography. Public key cryptography relies on the use of digital certificates in order to solve public keys management and revocation. In order to improve on the computation speed, public key cryptography techniques can be used as a means of exchanging in a secure fashion a symmetric key for use in a session or a transaction.

Digital signatures are an example of practical implementation of public key cryptography technology. A digital certificate provides assurance of the association between a public key and a holder of the certificate. Digital signatures can provide authentication, data integrity, and non-repudiation for transactions. Digital signatures can be used to confirm corroboration of the claimed identifier of the sender of a message. Digital signatures are often used in conjunction with digital certificates. Digital certificates are used as the vehicle that carries the information that is needed in public key cryptography and digital signatures. Digital certificates can be issued to users through an approved or trusted authority.

Message authentication code (MAC) is an authentication checksum derived by applying an authentication scheme, together with a secret key, to a message. In contrast to digital signatures techniques, a MAC is computed and verified using the same key. This way MACs can only be verified by the intended recipient. In hash function based MACs (HMACs) (see [b-IETF RFC 2104]), a key (or keys) is used in conjunction with a hash function to produce a checksum that is appended to the message.

II.2 Access control technologies

Access control focuses on ensuring that only authorized users can access a network device or an attached system. In effect, access control enables IT professionals to better analyse and understand the type and nature of attacks that occur on their network. There are many techniques that can be used to implement access control. These methods are discussed in the following subclauses.

II.2.1 Perimeter protection

Perimeter protection technology prevents access to the network or computer by untrusted or unauthorized outside users. Perimeter protection technologies install a logical or physical boundary between protected areas and areas that are open to the public and untrusted outside users (this does not cover untrusted insiders). Perimeter protection technology can be applied to protect a network or a single device. Examples of perimeter protection technologies include:

1) Content filtering or content management software restricts the type of data that can be accessed or distributed in a network (see [b-ISO/IEC 10828-3]). It restricts the ability of users to access content outside their boundary. This minimizes the chances of downloading viruses and other malicious code from untrusted locations. Content filtering can take the form of URI (see [IETF RFC 2396]) filters, whereby they can deny access to users to web pages with questionable content. Content filtering can be used to scan application messages, such as e-mail for spam viruses or unapproved content.

2) Firewalls: This technology (see [b-ISO/IEC 10828-3]) can be divided into four broad categories: packet filters, circuit level gateways, application level gateways and stateful multilayer inspection firewalls.

- Packet filtering firewalls operate at the IP layer. They are usually part of a router firewall. They compare each IP packet to a defined rule set before it is forwarded to the next route or its final destination. Depending on the comparison results, the firewall can drop the packet, forward it, or send a message to the originator. Rules can include source and destination IP address, source and destination port number and protocol used. Network address translation (NAT) routers offer the advantages of packet filtering firewalls, and additionally can also hide the IP addresses of devices behind the firewall. Packet filtering firewalls can have low impact on network performance and provide some degree of security at the network layer.
- Circuit level gateways work at the TCP layer of TCP/IP to monitor TCP handshaking between packets to find out whether a requested session is legitimate or not. Furthermore, requests issued to a remote computer through the circuit level gateway will appear to the receiver as if it did originate from the gateway. This technique helps to hide information about a protected network. Circuit level gateways do not filter individual packets.
- Proxies or application level gateways can filter packets at the application layer of the OSI model. Incoming or outgoing requests cannot access services that do not have a proxy. Proxies examine packets at the application layer to filter application-specific commands such as HTTP POST (see [b-IETF RFC 2616]). A proxy will not allow un-configured traffic to reach the application. Proxies can also be used to log user activity and logins. Proxies can provide high level of security at a significant impact on network performance.
- Stateful multilayer inspection firewalls combine the aspects of the above types of firewalls. Multilayer firewalls filter packets at the network layer, establish if the session packets are valid and filter packets contents at the application layer. Multilayer firewalls are transparent to connections between the sender and the receiver.

3) Network address translation (NAT): This technology provides the ability of hiding the network addressing schema behind a firewall environment. In NAT, the IP address of a system on the internal network is mapped to a different corresponding external, routable IP address. In NAT, it is possible for many systems behind a firewall to share the same external IP address. Resources behind a firewall are still accessible to external users by forwarding inbound connections on certain port numbers. NAT can be implemented on most network devices, such as switches, routers and firewalls.

4) Application level gateways: These systems (see [b-ISO/IEC 10828-3]) consist of hardware and software-based device or set of devices. They are designed to restrict access between two separate networks. These systems use stateful packet inspection and application proxy techniques to restrict access between networks. Combinations and variations (e.g., circuit-level firewalls) of these techniques may also be used. Furthermore, NAT can be performed by application level gateways.

5) Application proxy: These systems (see [b-ISO/IEC 10828-3]) provide application level awareness of attempted connections by examining packets at the highest layer of the protocol stack. Application proxies have full visibility of data exchanges at the application layer. This capability allows them to easily see the granular details of each attempted connection upfront and implement security policies as a result. Application proxies can have the ability of terminating client connections and initiating a new connection to an internal protected network. This ability provides added security since it separates the external and internal systems.

II.2.2 Virtual private network (VPN)

[b-ISO/IEC 18028-5] provides a comprehensive overview of using VPN for securing communications across networks.

VPNs are currently used for the task of interconnecting networks, and as a method of connecting remote users to networks. VPNs in their simplest form provide a mechanism for establishing a secure data channel or channels over an existing network or point-to-point connection. VPNs can be established and removed dynamically. The hosting network may be private or public.

Remote access using a VPN is implemented on top of a normal point-to-point connection that is already established between the local user and the remote location (see [b-ISO/IEC 18028-5]). VPNs can be provided as a managed service, where a secure, reliable connectivity, management and addressing, equivalent to that on a private network, are provided on a shared infrastructure.

There are multiple ways of representing types of VPNs (see [b-ISO/IEC 18028-5]). In principle, a VPN can be:

– a single point-to-point connection (for example, a client device remotely accessing an enterprise network over a site gateway); or
– a point-to-cloud connection (by using MPLS techniques).

There are three main types of VPN (see [b-ISO/IEC 18028-5]):

– Layer 2 VPNs emulate a LAN facility, by using VPN connections running over a hosting network to link sites of an enterprise together, or to provide a remote connection to an organization. Typical provider offerings include virtual private wire service (VPWS) that provides a simulated wires-only connection, or virtual private LAN service (VPLS) that provides a more complete emulated LAN service.
– Layer 3 VPNs emulate a WAN facility, by using VPNs running over a network infrastructure. They offer the ability to use private IP addressing schemes over a public infrastructure, a practice that would not be allowed over public IP connections. However, the use of private addresses over public networks via NAT can complicate IPSec (see [b-IETF RFC 2411]) VPN establishment and use.
– Layer 4 VPNs are used for securing transactions over public networks. In this type, VPN connections are usually established over TCP which is a layer 4 protocol. This type of VPNs provides a secure channel between communicating applications to ensure data confidentiality and integrity for the duration of the transaction.

VPNs can be implemented within a private network under the control of the owning business, or they can be implemented across networks in the public domain. Implementations that use combinations of these two schemes are also possible. On the other hand, channels can be established by employing secure channels through the use of tunnels running through Internet service provider networks. In this regard, the public Internet is in effect the underlying transport system. As such, there are greater risks to the confidentiality of the data carried by the VPN.

A tunnel is a data path between networked devices that is established across an existing network infrastructure. The tunnel is transparent to network operations. A VPN created with tunnels is, in general, more flexible than a network based on physical links. Tunnels can be created through the use of virtual circuits, or label switching, or protocol encapsulation.

Security aspects of various types of VPNs are provided in Table II.2.2 (see [b-ISO/IEC 18028-5]).

Table II.2.2 – VPN security aspects

VPN	Technology	User authentication	Data encryption	Key management	Integrity checking
Layer 2 VPN	Frame relay, ATM, MPLS, PPP, L2F	N/A	N/A	N/A	N/A
	L2TP (see [b-IETF RFC 2661])	CHAP-like	N/A	N/A	N/A
Layer 3 VPN	IPSec	Certificate based (packet) pre-shared secret keys	Negotiable several algorithms (packet)	IKE	Negotiable
	IPSec with L2TP	Certificate based (packet) pre-shared secret keys	Negotiable several algorithms (packet)	IKE	Negotiable
	MPLS	N/A	N/A	N/A	N/A
Layer 4 VPN	TLS	Certificate-based	Negotiable	Negotiable	Negotiable
	Secure shell	System-generated key pair (not certificated)	Negotiable	Exchange of public keys to data sender	Negotiable

NOTE 1 – SSL can be used instead of TLS.

NOTE 2 – [b-IETF RFC 3031] provides an overview of multiprotocol label switching architecture (MPLS). [b-IETF RFC 1661] describes the point-to-point protocol (PPP). [b-IETF RFC 2427] discusses multi-protocol interconnect over frame relay.

II.2.3 Authentication

Several methods can be used to authenticate a user. Techniques include: passwords, one time pass, biometric techniques, smart cards [b-ISO/IEC 7816-x], and certificates. Passwords-based authentication must use strong passwords (e.g., that are at least eight characters in length, with at least one alphabetic, one numeric and one special character). Password authentication alone may be insufficient. Based on vulnerability assessment, it may be necessary to combine password authentication with other authentication and authorization processes, such as certificates, lightweight directory access protocol (LDAP) (see [b-IETF RFC 3377]), remote authentication dial-in user service (RADIUS) (see [b-IETF RFC 2869], [b-IETF RFC 3579] and [b-IETF RFC 3580]), Kerberos (see [b-IETF RFC 1510]), and public key infrastructure (PKI) (see [b-IETF RFC 2459]).

Authentication systems can be categorized according to the number of identification factors needed. Single factor authentication refers to a system that uses one factor (e.g., userID/password combination). Two-factor authentication describes a process that requires two components in order to gain system access, such as the possession of a physical token plus the knowledge of a secret (e.g., password). A three-factor system adds another identification factor such as a biometric or measurement of a human body characteristic. Employing more authentication factors results in more secure authentication; however, including more factors adds complexity, cost, and management overhead. Finding the optimum trade-off between simplicity and security is the key challenge with any authentication system.

Single factor userID/password authentication is currently the most common authentication system in use today. Password authentication systems are simple, easy to administer, and very familiar to users. If strong passwords are used, single factor authentication systems can provide a high level of security. Legacy password systems have had some challenges, however, since multiple strong passwords are very hard for users to remember. As will be discussed in the recommendations below, these drawbacks can be minimized to provide an optimal solution with a "single strong password" system.

Tokens, such as smartcards, are added as a second factor in many authentication systems. Tokens provide additional authentication security since the user has to prove physical possession of the token in order to be authenticated. An attacker would similarly have to have possession of the user's token in order to gain system access. The higher level of authentication comes with additional system cost, however, due to the necessary tokens and token readers. In addition, tokens can be easily lost which can present a high administration overhead for reissuing.

Strong cryptographically based authentication can be provided through the use of digital certificates issued to users and stored on tokens or within the user's computer memory. Cryptographic algorithms are used to ensure that a particular certificate has been legitimately issued to the user. A public key infrastructure is used to enable the issuance and maintenance of digital certificates. Strong cryptographically based systems provide very strong authentication; however, these systems are expensive and incur additional management overhead, and as such are currently finding adoption only within very secure environments.

II.2.4 Authorization

Once authenticated, authorization mechanisms control user access to appropriate system resources. Authorization can be categorized according to the granularity of control, that is, according to how detailed a division is made between system resources. Fine-grained authorization refers generically to a system where access is controlled to very fine increments, such as to individual applications or services.

Authorization is often "role based", whereby access to system resources is based on a person's assigned role in an organization. The system administrator role may have highly privileged access to all system resources, whereas the general user role would only have access to a subset of these resources. If fine-grained authorization is applied, the human resources administrators' role may have exclusive access to highly confidential HR databases, and the accounting role may have exclusive access to accounting system databases.

Authorization may also be "rule based", whereby access to system resources is based on specific rules associated with each user, independent of her or his role within an organization. For example, rules may be set up to allow read-only access or read/write access all or certain files within a system.

II.2.5 Authentication and authorization protocols

Several protocols have been commonly adopted for authentication services. The RADIUS protocol (remote authentication dial in user service) (see [b-IETF RFC 2865]) is used widely to centralize password authentication services. Originally designed to authenticate remote dial-in users, the RADIUS protocol has been adopted for general user authentication services. LDAP (lightweight directory access protocol) has been finding extensive use in authentication and authorization systems. LDAP provides a convenient method for storing user authentication and authorization credentials.

Often RADIUS authentication servers are coupled with credential storage in LDAP directories to provide a centralized authentication and authorization system. When a user attempts to access a particular application on such a system, the application would query the user for authentication credentials and forward them to the centralized system. The RADIUS server would then check the

presented credentials against those stored in the LDAP database, and also query the LDAP database for authorization rule information. The authentication results (pass or fail) are returned to the application along with authorization rule information for the particular user. Authorization rules would then be enforced at the application to allow the user to access particular data or services. From an end-user perspective, these authentication and authorization systems are expected to be automatic and easy to use.

II.3 Antivirus and system integrity

Worms, malicious code, viruses and Trojan horses can modify a system and its data. Therefore, it is essential to use technologies that scan for viruses and ensure that the integrity of the system is preserved.

A worm is a program that reproduces by replicating itself from one system to another without the need of human involvement. Viruses can attach themselves to user files and can spring into life by replicating themselves into other files when an unsuspected user performs some action such as opening an infected file. A Trojan horse, on the other hand, usually presents itself to the unsuspected user as a useful program that conceals a harmful code.

Antivirus technology helps to protect systems against worms, malicious code and Trojan horses attacks. The software can either be installed on the user's devices, or be provided as a service by the network or the Internet service provider. System integrity techniques use software that checks that only authorized updates are applied to critical system files.

Antivirus software products can use string signatures techniques to identify viruses and malicious code. This technique requires the earlier knowledge of the malicious code before the antivirus software can detect it. As such, their signature database needs to be current for effective protection.

Activity scanners check for unauthorized activities performed by a running code. The software notifies the user of the suspicious activities. Active scanners usually have limited success against viruses, but may be more effective against worms and Trojan horses. Static heuristic scanners scan the code to try to identify activities that could be associated with virus-like behaviour.

System integrity techniques use software that monitors modifications that is done to critical system files. These techniques can be used by IT administrators to perform system checks to determine if hackers have successfully penetrated a system (hackers tend to leave backdoor traps).

II.4 Audit and monitoring

Audit and monitoring techniques allow IT administrators to evaluate overall system security, including instructions detection and prevention software. IT administrators can use this technology to carry out system analysis to determine its weakness after an attack. In some cases, system analysis can be performed during an active attack on the system.

Intrusion detection system (IDS) (see [b-ISO/IEC 18043]) can be used to monitor the network to ensure that no unauthorized users are accessing the network. Most IDS applications compare network traffic and host log entries to match data signatures and host address profiles indicative of hackers. Intrusion detection software identifies traffic patterns that indicate the presence of unauthorized users. Suspicious activities trigger administrator alarms and other configurable responses. Intrusion detection system (IDS)s can be broadly categorized according to the following criteria:

- Incident detection time-frame: Real-time or off-line, depending on whether system logs and network traffic are analysed as events take place or in batch mode during off hours;

- Type of installation: Network-based or host-based. A network-based IDS typically involves multiple monitors (often pre-configured appliances) installed at choke points on the network (where all traffic between two points can be monitored). A host-based IDS requires that software be installed directly on the servers to be protected, and monitors the network connections and user activity on those servers; and
- Type of reaction to incidents: Whether the IDS actively intervenes to head off attacks (such as by modifying firewall rules or router filters) or simply notifies staff or other network systems of the problem.

Most commercial IDS products provide a combination of network- and host-based monitoring capabilities, with a central management host to receive the reports from the various monitors and alert the network support staff. The use of a network-based IDS product is recommended for most network installations depending on particular customer needs.

II.5 Management

Configuration management techniques allow IT administrators to set and verify security settings on devices in their networks. Policy management enables IT administrators to define business-driven security and QoS policies, and enforce these across the organization without having to understand all the device-specific rules and settings that are needed to enforce these policies. Technically, policies are a set of rules to administer, manage, and control access to IT resources; these need to be derived from business policies defined by the organization. In the security space, policy management addresses the complexity and the difficult learning curves associated with these technologies (for example, firewalls, IDS, access lists and filters, authentication techniques), and the lack of a system view across different parts of the network (data centre, remote office, campus).

While there are numerous solutions to address parts of the problem, the ultimate policy management system provides a centralized network configuration, ensuring that security parameters are set consistently across multiple nodes, reducing the risk of network vulnerability. This does not mean that there is only one policy system; in a larger network with multiple administrative domains, there may be a need for multiple policy systems each responsible for controlling a subset of devices and inter-domain consistency.

The major benefit of a fully implemented policy management system is the ease of use and a more secure environment. Ideally, network managers would like to be able to define policies for network operations using a non-technical vocabulary, and then have the policy system automatically translate these terms into the appropriate security mechanisms to be implemented across the network.

II.5.1 Policy management reference model

Figure II.5.1 depicts the IETF's architectural framework for policy management ([b-IETF RFC 2753]). This reference model is used as the blueprint for policy management for both security and QoS management. Thus, policy management, when based on this model, will be implemented across the network and at all layers of the architecture, and will be available to all types of user and applications, including employees, network technicians, partners and even customers.

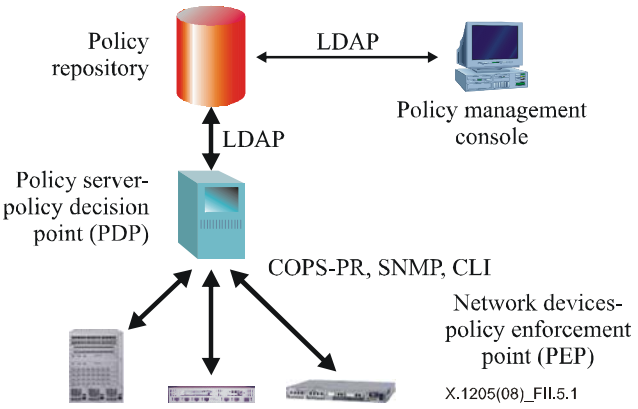

Figure II.5.1 – Policy management reference model

Components of the model include:

- *Policy enforcement point (PEP)*: A network or security device that accepts a policy (configuration rules) from the policy decision point and enforces that policy against the network traffic traversing that device. This enforcement leverages network and network-assisted security mechanisms as appropriate.
- *Policy decision point (PDP)*: PDPs or policy server's abstract network policies into specific device control messages, which are then passed to policy enforcement points. These policy servers are often stand-alone systems controlling all of the switches and routers within a particular administrative domain; they communicate with these devices using a control protocol (e.g., COPS, SNMP set commands, Telnet or the device's specific command line interface (CLI)).
- *Common open policy service (COPS)*: COPS is a simple query and response stateful TCP-based protocol that can be used to exchange policy information between a policy decision point (PDP) and its client's policy enforcement points (PEPs). It is specified in [b-IETF RFC 2748]. COPS relies on the PEP to establish connections to a primary (and a secondary PDP when the primary is unreachable) at all times. Alternatively, a COPS proxy device can be used, which translates COPS messages originating from a policy server into SNMP or CLI commands understood by the network and security devices.

  The COPS protocol supports two different extension models for policy control: a dynamic outsourcing model COPS-RSVP, specified in [b-IETF RFC 2749], and a configuration or provisioning model COPS-PR, specified in [b-IETF RFC 3084]. The provisioning extensions to the COPS protocol allow policies to be installed on the PEP "up front" by the PDP, thus allowing the PEP to make policy decisions for data packets based on this pre-provisioned information. Further communication between the PDP and PEP is necessary to keep policies provisioned in the data repository (i.e., the directory) in synch with those sent to the PEP.
- *Policy repository*: The network directory is the repository for all policy information; it describes network users, applications, computers, and services (i.e., objects and attributes), and the relationships between these entities. There is a tight integration between IP address and the end user (via dynamic host control protocol – DHCP and a domain name system – DNS). A directory is usually implemented on a special-purpose database machine. The lightweight directory access protocol is the mechanism that policy servers use to access the directory.

The policy repository is used to store relatively static information about the network (e.g., device configurations), whereas policy servers store more dynamic network state information (e.g., bandwidth allocation, or information about established connections). The policy server retrieves policy information from the directory, and deploys it to the appropriate network elements.

There is no established standard to describe the structure of the directory database, i.e., how network objects and their attributes are defined and represented. A common directory *schema* is needed if multiple vendor applications are to share the same directory information; for example, all vendors need a common way to interpret and store configuration information about routers. The forthcoming directory-enabled networking (DEN) standard, now being developed by the DMTF (Desktop Management Task Force), addresses this need. DEN includes an information model that provides an abstraction of profiles and policies, devices, protocols, and services. This provides a unified model for integrating users, applications, and networking services, and an extensible service-oriented framework.

- *Lightweight directory access protocol* (LDAP version 3) is specified in [b-IETF RFC 3377]: LDAP is a client-server protocol for accessing a directory service. The LDAP information model is based on the entry, which contains information about some object (e.g., a person), and is composed of attributes, which have a type and one or more values. Each attribute has a syntax that determines what kinds of values are allowed in the attribute, and how those values behave during directory operations.
- *Policy management console*: Human beings interact with the policy management system through a management console, generally running on a personal computer or workstation. Alternatively, a web browser can be used to provide manager access from virtually anywhere, with policy object-level security used to limit which policies can be modified by a specific individual. It is through the management console that policies get instantiated in the directory. The console provides a graphical user interface and the tools needed for managers to define network policies as business rules. It may also give the operator access to lower-level security configurations in individual switches and routers.

The elements of the policy management reference model interoperate to deliver closed loop policy management. This includes configuration of edge devices, enforcement of policies in the network and verification of network functionality as seen by the end-user application. Enforcement of policies in the network includes admission controls of applications or users vying for access to network resources. Policy management can go some way towards simplifying the configuration management environment inside enterprises, minimizing opportunities for human error.

II.5.2 Hardening server OS

Hardening the operating systems (OS) is a key element of securing information systems within the application security layer. A typical enterprise may have multiple different operating systems for various applications in the data world (including network management), but also for application servers supporting IP telephony and communication intensive applications. It is quite frequent to find multiple versions of the same OS breed deployed in the IT infrastructure, rendering the security task even more challenging.

The most common operating system in the data world is also used extensively for application servers supporting IP telephony and communication intensive applications. Vendors offer a hardened version of these systems with off-the-shelf security software for functions, such as anti-virus protection, intrusion detection and login audits. Hardening an OS starts with the requirements to avoid server cloning and to trust the media from which the operating system is downloaded, and goes from there. For operating systems where no specific hardening guide exists, the OS vendor should be consulted to obtain the latest OS hardening patches and procedures.

Appendix III

Example of network security

(This appendix does not form an integral part of this Recommendation)

This appendix provides examples of securing various aspects of an organization or a large enterprise using the techniques that have been discussed in this Recommendation.

In particular, the principles of building layered security solutions for securing the campus include gateways to the Internet, the data centre, the remote office, remote access and IP telephony. The techniques that are discussed in this Recommendation are used to illustrate that security for the enterprise does not fall into "one-size-fits-all" model. Table III.1 provides an example of relevant security aspects that are needed for example enterprise 1, which is a small size enterprise that uses limited physical private lines between sites, provides limited remote access to employees, and Web presence is achieved through an Internet data centre provided by a service provider (who is responsible for establishing a secure environment). Example enterprise 2, is an open enterprise with a business model that leverage the Internet by allowing partner, supplier and customer to have limited access to enterprise-managed applications. In example enterprise 2, internal and external users access the enterprise network from home, remote offices or other networks using wired or mobile devices.

Table III.1 – A guide to relevant enterprise security aspects

Network area	Example enterprise 1	Example enterprise 2
Securing the campus	Yes	Yes, representing most stringent security requirements
Securing the remote office	Encryption option over virtual or physical private lines	Yes, including remote office Internet access
Securing remote access	Yes, but only for private dial access	Yes, including partners and customers
Securing the data centre	Yes, for internal data centres	Yes, including Internet data centres
Securing IP telephony	Yes	Yes, leveraging VPNs

III.1 Securing remote access

Remote access technologies enable the enterprise or an organization to make efficient use of people and resources located almost anywhere. However, these technologies also have the potential to introduce security problems for the enterprise. Individual enterprise employees who are travelling or working from home comprise the majority of remote access users, but this category also includes small offices, which connect on-demand to the enterprise network. The key challenges are met through network security and secure access management. Network management security is implemented at the central site. Application security is relevant in that the remote device needs to be protected through antivirus scanning software and personal firewalls.

One important threat specific to remote users is the theft of UE. Theft of the remote user's equipment should not be allowed to lead to intrusion into other areas of the enterprise network, nor to access of the information, which may be stored in the system. On the other hand, mobile users want to carry around their devices or their terminals for access to the network from anywhere. This makes it necessary to encrypt sensitive information stored on systems used for remote access, preferably using a system, which integrates seamlessly into normal use of applications. Currently,

available encryption systems allow the user to operate normally, not requiring manual or individual encryption/decryption of files. For example, entire file systems or "folders" can be stored in encrypted form, with decryption being integrated in the normal file system access. Another form of threat can occur when the remote access user is operating on a wireless LAN, perhaps at home or in a hotel. In this case, having an up-to-date personal firewall and antivirus is important.

The most common forms of remote access for data communications are dial access, either directly to the enterprise or to an ISP, and Internet-based direct access using digital subscriber line (DSL), cable modems, native Ethernet (e.g., in hotels), and wireless LANs (e.g., in airports). Public wireless data services supporting Internet access are also a high growth area providing increased mobility for laptops and handheld computers. The increasing availability and economies of the Internet are contributing to its rapid growth for remote access VPNs, using both dial up and direct access. Figure III.1 provides an example of securing remote access.

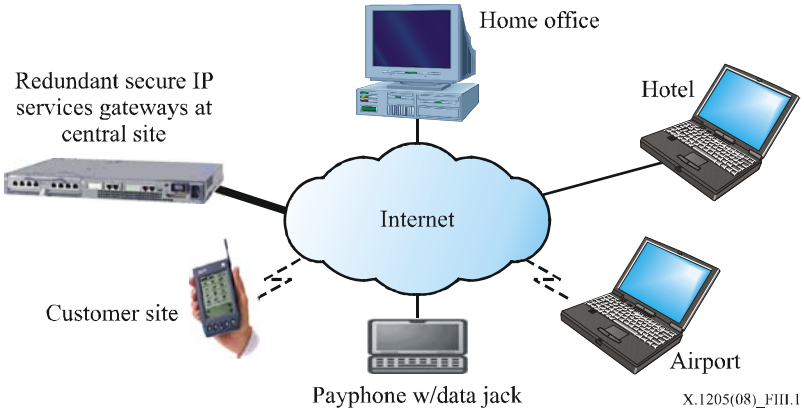

Figure III.1 – Securing remote access

Using the techniques that are presented in this Recommendation, the following steps can be taken to secure remote access:

1) *Dial access to a centralized enterprise site*

A remote access dial-up user establishes a telephone call from a modem attached to his computer system to a modem pool (also called a remote access switch) located at a central or regional enterprise site. Dial access systems should be configured to use a secure access management system providing access authentication and authorization, as described previously. Direct switched access, while widely used in the 80's and early 90's, is rapidly being replaced by Internet-based remote access VPNs.

2) *Remote access VPNs*

Internet-based remote access provides tremendous flexibility and high bandwidth. There are two approaches: IPSec-based VPNs using remote access VPN clients, or SSL-based VPNs based on the SSL capability of the user's browser.

3) *IPSec-based VPNs*

IPSec is a network layer approach that can be used across applications (e.g., if an IPSec-based VPN connection is established, the user can get to e-mail, self-serve applications and browse the internal network and access authorized applications). An IPSec client needs to be loaded on the UE to be used for remote access. Clients are also available for handheld computers. The UE should also be loaded with antivirus detection software.

Whether based on dial access to an ISP POP or on wired or wireless direct access, the VPN client authenticates the user, verifies the integrity of the user's own computer system, and establishes a secure link (or tunnel) to the enterprise. The VPN client provides capabilities

(e.g., firewalls) to ensure that the remote system is itself secure, in particular, during the connection set-up to the enterprise. Session set-up phase uses encrypted and authenticated traffic to the enterprise.

It is assumed that remote access VPNs are able to detect and, if possible, to bypass common Internet obstacles such as NAT and outbound firewalls (i.e., to establish a link to the enterprise network from within another firewall-protected network), or at least to provide the remote user with information on the nature of the obstacles encountered.

At the enterprise edge, remote access connections from the Internet are handled by IPSec gateway system. The enterprise edge should provide protection against a single point of failure by employing multiple gateways with multiple paths to the Internet. Depending on the scope of the enterprise, geographic separation of gateways is also recommended. The gateway should provide a number of features to support effective enterprise-scale remote access. Recommended features include: simple client configuration, capability to pass connections through to the internal enterprise network as opposed to session termination, and be able to provide stateful firewall functionality to avoid the need for a separate firewall. Furthermore, it is recommended that the gateway use a variety of authentication mechanisms, such as RADIUS, PKI and LDAP for added flexibility in choosing user authentication level. The gateway should allow the enterprise the flexibility to integrate other schemes, such as RADIUS, directory-based userID/passwords, or even smart or token-card authentication on user's laptops that may already be in use. Support for L2TP and PPTP is beneficial.

III.2 Securing IP telephony

Organizations and enterprises are starting to roll-out IP telephony solutions, aiming to reap the benefits of convergence in the LAN and the WAN, and of converged applications. Every VoIP system is a hardware/software solution that is made up of a set of four logical functions:

- IP telephones and PC soft clients.
- Communications servers (also called call management servers or gatekeepers).
- Media gateways providing flexible network access (e.g., via traditional PBXs and the public switched telephone network (PSTN) and the public wireless network and beyond).
- Application servers (e.g., unified messaging, conferencing and SIP-enabled collaborative applications).

These functions, as well as related communications application servers, such as those supporting contact centre and unified messaging, are distributed across a telephony- or business-grade IP network that delivers the needed levels of reliability, voice quality and congestion management. Extended reach and mobility are provided over wireless LANs and over the Internet via IP VPNs.

Figure III.2 depicts a typical organization approach to securing IP telephony.

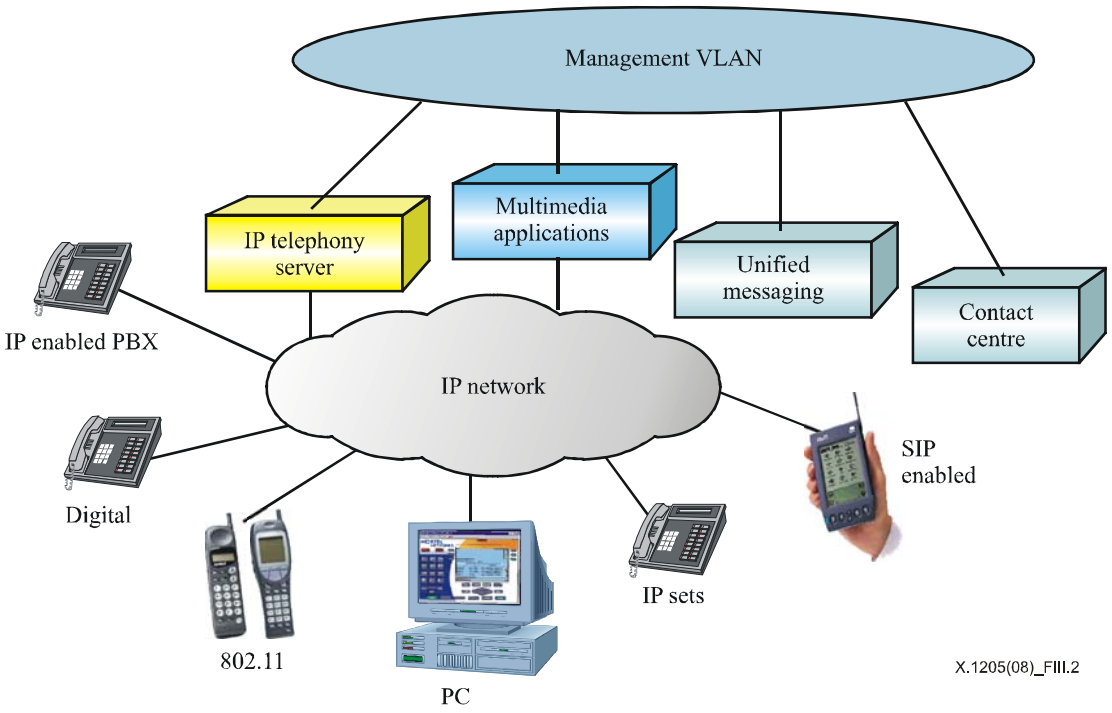

Figure III.2 – Securing IP telephony

IP telephony is an application that runs on the IP network and leverages the security functionality provided by a network. Unlike most data applications, IP telephony is time-sensitive and is critical to the running of the business. Just like other data applications, IP telephony systems can be subjected to a number of attacks. For example:

- Attacks on the router can bring down both voice and data services in an organization;
- Denial of service can overload an IP telephony communications server or client;
- Ping of death can disrupt VoIP operations by sending multiple pings to VoIP devices;
- Port scanning can find vulnerabilities in VoIP clients and servers;
- Packet sniffing can record and/or intercept conversations;
- IP spoofing can misrepresent the source or destination of the media or signalling stream;
- Viruses, worms, Trojan horses, and time-triggered bombs can attack servers and clients.

IP telephony can be compromised. For example, there have been cases of hackers taking over IP clients, due to slack of administration of passwords in one case and due to vulnerabilities associated with running XML (see [b-W3C XML 1.0]) in another. These attacks can be primarily a threat when running VoIP natively across the Internet, and a lesser of a threat when IP telephony is used strictly within the enterprise and over tunnelled connections over the Internet.

Like any applications, a risk assessment of IP telephony needs to be done to evaluate its intrinsic value, the implications of loss understood within an organization and a security policy formulated. Telephony is a critical business function, and therefore, like the network itself, the telephony system as a whole will have to be protected from security threats and attacks.

Generally, telephony users authenticate themselves for off-net access using a feature set called direct inward system access (DISA). On the other hand, it is not uncommon to require data users to use multiple user identities and passwords for network and application access. This complexity runs counter to securing the enterprise environment. Simplicity will be even more important with VoIP, since the expectation is instant dial tone. Needless to say, any VoIP security mechanisms cannot impede necessary connectivity and voice quality.

Key guidelines in securing IP telephony include:

1) Enterprise IP telephony solutions operate within the confines of the enterprise, inter-working with the public network over circuit switched connections.
2) Enterprise IP telephony systems rely on the IP networking infrastructure to be secured from a data perspective, and to be engineered and designed to meet the latency and reliability requirements of telephony.
3) Enterprise IP telephony communications servers are business critical and are physically secured, and protected from internal and external attack.
4) Secure authentication of VoIP clients is provided.
5) Encryption of voice is only a requirement when traversing a shared media LAN or over the Internet.
6) A holistic approach to security is taken across the entire telephony environment including VoIP clients and servers, application servers (e.g., for unified messaging and contact centres) and traditional PBXs.

Securing IP telephony solutions require a coordinated approach across all network layers. Policy management and secure access management ensure user authentication and control IP telephony feature and calling capabilities. Secure management techniques should be used to protect VoIP devices, such as communications servers and media gateways. Security mechanisms that have been put in place for data can be leveraged for VoIP, for example, using IPSec for secure remote access, branch connectivity and for wireless LAN access. Additional security through policy management can be achieved by adding VoIP stateful inspection to firewalls and network address translation functionality. Application security can be achieved in a number of ways, including OS hardening, and virus protection installed on the UE.

III.2.1 Securing application and IP telephony communications servers

The heart of the IP telephony system is the communications server, which can be a stand-alone server or integrated with an IP enabled PBX business communications manager. Equally important are application servers delivering contact centre, multimedia applications, unified messaging and self-serve interactive voice response systems. Securing these servers starts with the hardening of the operating systems as described.

III.2.2 Securing VoIP clients

VoIP solutions support a broad range of clients and access configurations, including IP wired and wireless telephones and PC-based soft clients. When connected to an IP network, these are vulnerable to attack.

There is a number of different telephony signalling protocols such as SIP. Signalling traffic generally uses TCP at the transport level. In the future, the ability to secure signalling traffic at the VoIP client will be generally available. In IP telephony systems, the voice signal is packetized using a standard such as [b-ITU-T G.729] (at 8 kbit/s) and a speech activity detection algorithm, and uses the real-time protocol (RTP) with UDP at the transport level.

There are significant differences in how risk is minimized for IP telephones and for PC-based soft telephony clients. IP telephones are custom-built appliances for telephony only. There is no storage or asset on the phone itself to protect (other than its presence on the network as a trusted device). The identification of the caller and the call itself are the only assets to be protected. These telephony appliances most commonly use a proprietary thin client protocol which relies on the communications server for feature/functionality and security. This approach contrasts with implementations, which rely on XML in the VoIP set for feature operation which can be a vulnerability point.

VoIP soft-clients reside on user equipment with other applications and other assets, and running widely available operating systems. A successful attack can be costly, since there are many valuable assets on the UE including applications and business, financial and personal data. The common practice is to use one or a number of security applications written for UE platforms, providing personal firewalls, antivirus detection and IP VPN clients. For VoIP soft clients, the same mechanisms that apply for data can be used.

III.2.3 Securing VoIP in the wiring closet and across the campus

There are two ways of wiring IP devices into a campus network: shared media and dedicated switched Ethernet. The general industry direction is towards dedicated switched Ethernet, this is driven by traffic growth and manageability requirements. In addition, security and manageability are also driving the deployment of VLANs (see [b-ISO/IEC 18028-5]) in enterprise networks. Wireless LANs offer a third alternative, which are exploding in environments, such as in education and healthcare.

With the introduction of IP telephony, it is highly recommended that VoIP soft clients and VoIP appliances be connected to switched Ethernet environments right to the desktop. This meets the following requirements:

– VoIP latency variation is minimized by eliminating CDMA operation of shared media Ethernet operation;

– VoIP security is enhanced by prohibiting the potential of other desktops eavesdropping on VoIP calls.

In addition, enterprises may choose to logically group VoIP telephones in their own VLANs, in order to ease manageability.

IP telephony can significantly enhance the productivity of users using wireless LANs within the enterprise extending telephony feature/functionality from the desktop to, for example, the conference room or classroom. Because of the hostile nature of these WLANs, the recommended architecture is to secure both the signalling and voice planes over the wireless segment. This can be done by configuring soft client's co-resident with an IP VPN client on a laptop. Alternatively, with some WLAN IP phones, encryption and authentication is built in. Both approaches provide robust user authentication and encryption for WLAN environments.

III.2.4 Securing branches for IP telephony

There are a number of approaches to supporting remote office and branch VoIP solutions. These include VoIP telephones and soft clients supported of office-in-a-box solutions. Other approaches fully leverage the distributed nature of VoIP by deploying clients off a centralized server. In all cases, it is recommended that VoIP traffic in the branch run securely over an IP VPN established for data.

III.2.5 Securing remote access for IP telephony

IP telephony can significantly enhance the productivity of remote users, whether working at home, in a hotel or on the road, in all cases extending telephony feature/functionality from the desktop to the remote location. VoIP soft clients would be co-resident with an IP VPN client on a laptop for highly mobile employees. This same configuration would be used to take advantage of WLAN access points in hotels, airports and convention centres. VoIP telephones would provide feature-rich communications for telecommuters and contact centre agents with security provided by a home office IP VPN.

III.2.6 Network management security for IP telephony

From a management perspective, a physically dedicated Ethernet port should be configured. This should be part of a management VLAN with all non-management traffic blocked at the routing level via access lists and perimeter security. Off-net access for suppliers, system integrators and/or VARs can be provided via IP VPNs. Unused ports (e.g., for consoles or remote modem access) should be turned off. Only authorized application software should be run on these servers. Multi-level security should be used with various levels of privileges (monitor, configure, control) for authenticated operational personnel. User passwords are securely stored and password formatting and change management strictly controlled. Management traffic (such as billing information) can be optionally encrypted even for internal transmission through IP VPN technology.

III.3 Securing the remote office

A remote office can be of any size, from a home worker's desktop to a major corporate campus. Although there are many elements in common between a "remote office" and "remote access", they are distinguished by the persistence of capabilities for bidirectional communication between the remote location and the rest of the enterprise. That is, a remote office is a workplace, which is constantly connected to the rest of the enterprise, and is able to exchange messages with the rest of the enterprise during working hours. On the other hand, remote access is a temporary connection to the enterprise established on-demand by the remote access user(s).

Branch networking is the most significant cost-intensive service delivery vehicle in many industries, such as retail banking, health care and government. Traditional branch networking environments are based on various LAN technologies, and on multi-protocol routers, working into frame relay networks with ISDN circuit switched backup. Four major developments have created major opportunities to transform branch networking: 1) the convergence on Ethernet as the LAN standard, 2) universal acceptance of IP as the protocol of choice, 3) the Internet, and 4) a growing list of layer 2 and 3 VPN services. However, these developments also introduce a variety of security challenges particularly for larger organizations enterprises. This is depicted in Figure III.3.

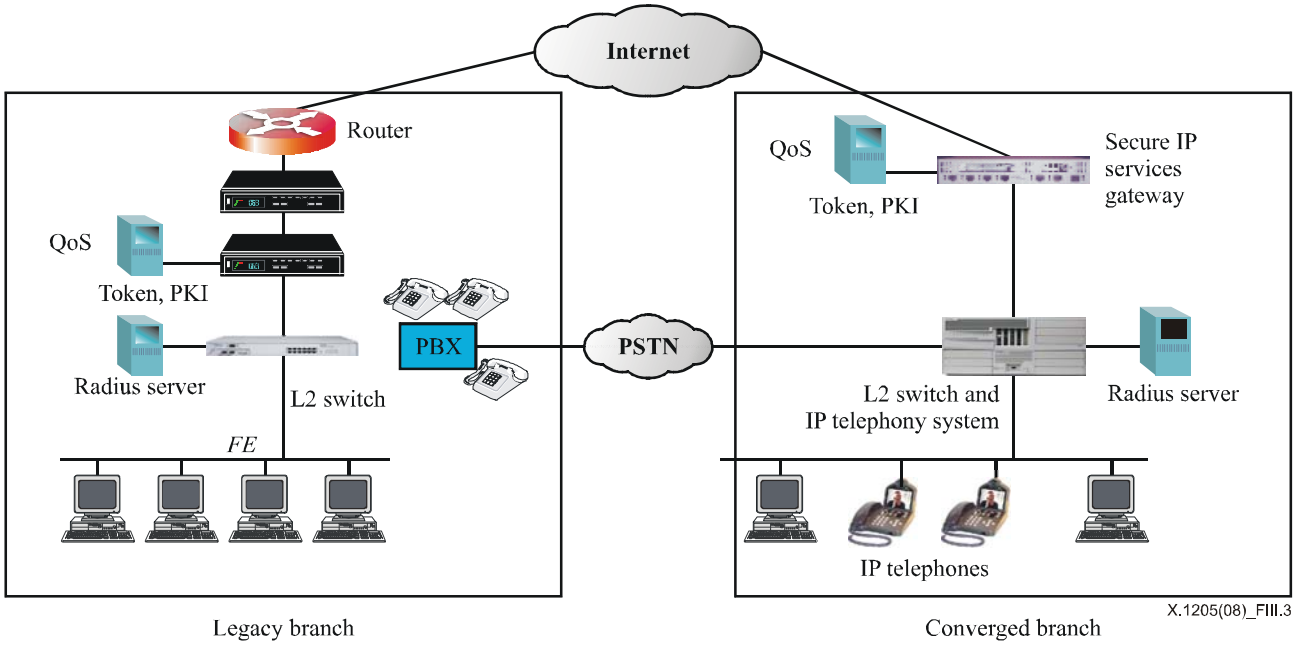

Figure III.3 – Securing remote office

The WAN edge requirements at the branch level include routing between VLANs locally and into the network, QoS and bandwidth management and scalable interfacing into the WAN network. This includes supporting encapsulation scheme over the WAN and whatever level of reliability is appropriate. Cost effective security over the Internet (and even over frame relay) is a key requirement. Managing the transition from legacy relatively secure WAN technologies to IP VPNs is also a challenge. Some enterprises want to have direct Internet access from every remote office opening up the need for remote firewalls. Others want highly reliable dynamically routed connectivity between branches and the enterprise backbone, with centralized firewalls into the Internet, in some cases using frame relay as the primary path and the Internet as a backup, or moving towards IP VPNs as a primary configuration. Dynamic routing is used to enhance scalability and reliability by:

- Automatically learning the network topology;
- Automatically learning the addresses of end users across the enterprise;
- Automatically adapting to changes in network topology.

However, security in routed networks has been an afterthought, not a day-one requirement. For example, there has been no effective way of running dynamic routing over VPN-encrypted tunnels, and management of these has been very difficult.

Generally, the above has led enterprises to purchase, install, maintain and manage multiple security and networking devices for remote office and branch networks, which have made these complex and costly to manage.

With the move to IP VPNs over the Internet, a complete set of security requirements have to be met as cost effectively as possible. This includes network security functions such as IP routing over secure tunnels, virtual private networking (VPN), and encryption, stateful firewall inspection at the network-assisted layer, and remote office authentication and directory services at the secure access management layer, all to be provided in a highly integrated fashion. Security policy management enforcement needs to be integrated into this solution, allowing each user to be provisioned with a unique security profile, which remains with the individual regardless of whether he/she logs in from his UE at home across the public Internet or connects locally within the branch office. Network

management security also needs to be extended to the remote office, without backdoors that might compromise network security. Finally, application security needs to be provided if data servers and/or IP telephony are deployed at the remote office.

III.4 Securing WLAN

The opportunities for communicating among corporate headquarters, branch offices, remote employees, consultants, and business partners are evolving. Companies can now leverage the new wireless IEEE 802.11 (see [b-IEEE 802.11]) technologies to conduct business anytime, anywhere. With these solutions, however, comes a need to centrally and effectively manage the user's access while securing the resources of an organization.

WLANs are particularly vulnerable to security breaches. Intercepting communications on a standard LAN requires physical access to the cabling infrastructure. Wireless transmissions, on the other hand, are subject to interception over the air and expose the network to intrusions from anyone with a standard wireless LAN card.

WLANs extend the corporate network by using wireless devices and the IEEE 802.11 protocol. Equipment in WLANs includes wireless network interface cards (NICs) for mobile equipment such as laptops and desktops, all of which are referred to as the mobile unit (MU) or station (STA). The NICs enable network signals to be carried from the connecting device through an intermediary device, the wireless LAN gateway, or hub known as the wireless access point (AP), which converts the wireless signals to wireline signals to be carried on the wired network.

Using an Ethernet hub or switch, companies can connect wireless LAN access points to the wired LAN as easily as adding a wired user. By connecting the access points to a switch, the access point is assured a dedicated 10/100 Mbit/s, thereby allowing all available access points to behave like a switch without having to contend for a portion of the wired hub's bandwidth.

The original [b-IEEE 802.11] standard is a family of specifications, of which IEEE 802.11a, IEEE 802.11b, IEEE 802.11g and IEEE 802.11i are available today and which are used based on the network's signal environment, with trade-offs between distance and bandwidth.

III.4.1 WLAN security issues

Regardless of WLAN security mechanisms, WLAN signals still broadcast and receive over the air via radio waves and therefore have no physical barrier to an unauthorized user. These signals are unfortunately subject to interception and to the possibility of intrusions into the corporate network. Therefore, adding a wireless node to the corporate network implies to include the appropriate security precautions and good security practices for protecting all WLAN network assets.

The infrastructure layer of WLAN networks consists of all components of the network, cables, interconnections and transmissions media (coverage space), e.g., access points, mobile stations, gateways and servers hosting associated services like RADIUS, DNS, etc.

The service layer is composed of wireless LAN access services and other services enabling wireless access, e.g., authentication, authorization, accounting (AAA), key management services, etc.

The security threats posed by WLANs include:

- Breaches of confidentiality and integrity of wireless traffic. It may be possible for an attacker to intercept communications between a mobile computer and a wireless AP, and thereby capture sensitive or classified information not intended for a third party. Conversely, it may be possible for an attacker to insert information into an authentic transaction, without the knowledge of the legitimate users.

- Exposure of corporate LAN. Unless mobile platforms are securely authenticated, an attacker may simply connect the WLAN using an IEEE 802.11 compliant device and become an "authorized" station on the WLAN, thereby gaining access to the corporate LAN.

Using the X.800 threat model, the attacks can be summarized as follows:

X.800 threat model	Methods of attack
Destruction of information and/or other resources	AP intrusion
Corruption or modification of information	WEP key cracking, man-in-middle
Theft, removal, or loss of information and/or other resources	AP intrusion, WEP key cracking, man-in-middle, MAC address spoofing, rogue devices, war driving, layer 3 hijacking, ad hoc networks
Disclosure of information	AP intrusion, WEP key cracking, man-in-middle, MAC address spoofing, rogue devices, war driving, layer 3 hijacking, ad hoc networks
Interruption of service	RF jamming, data flooding, layer 2 hijacking, fake AP, spoofed de-authenticate frame, FATA-Jack DoS

Similar to the wired network, WLANs require confidentiality, integrity, and access controls. The main security problem with wireless is that outsiders can easily receive or transmit to and from the WLAN, regardless of whether the outsider is considered out of range.

This allows attackers to eavesdrop and insert unauthorized APs (referred to as rogue APs) to launch attacks, such as man-in-the-middle attacks and session hijacking, and easily attack WLAN users from within the WLAN. Thus, an attacker can fool a user into connecting to the attacker's AP, posing as a legitimate node on the network and, therefore, freely and unwittingly share user IDs, passwords, and other private information.

The following techniques can be leveraged for securing the wireless environment:

- Network names: service set identifications (SSID)
- Card registration: MAC access control lists (ACL)
- Shared key encryption: through the use of security protocols (such as WPA/WPA2)

In addition, the following authentication types can be used:

- Open system authentication: enables anyone with the AP's SSID to receive access.
- Shared key authentication: the user possesses a shared secret in order to be authenticated.

In the original [b-IEEE 802.11] specification, secure roaming happens through the pre-authentication of the mobile unit (MU) to surrounding APs. There is no handoff message between APs, as all APs and MUs use the same shared key, enabling the new AP to presume the validity of the MU's authentication. Thus handoff is fast, but authentication is less secure because the management frames are unauthenticated.

III.4.2 Security requirements and mechanisms within and in front of the wireless access point

The only way to really protect the open nature of the wireless environment is with cryptographic solutions and appropriate authentication measures that validate the end user. Traffic gets encrypted to a gateway whose identifier can be cryptographically validated.

The two main requirements for a secure WLAN are secure traffic and secure roaming. For secure communications, the most basic requirement is the use of encryption for the traffic from the mobile device to the AP, to a gateway behind the AP (for example using an IPSec gateway), or to the application server (secure web site). For secure roaming, mobile users have to be able to move from one AP to another without losing their active sessions and without having to re-authenticate to the new AP. Roaming has tight time constraints such that there is minimal impact caused to the user's application. Users expect and assume that their credentials are suitably protected when being passed between domains.

III.4.3 Security enhancements to the IEEE 802.11 specification

The above security risks lead to enhancements to the original [b-IEEE 802.11] standard to provide more effective means of security wireless LANs. IEEE 802.11i introduces IEEE 802.1X (see [b-IEEE 802.1X]) access control, dynamic re-keying, per-session key distribution mechanisms, and strong cryptographic algorithms. [b-IEEE 802.1X] introduces more authentication/access control for the APs through the use of the extensible authentication protocol (EAP), which is a set of messages for authentication negotiation and authentication transport method between client and server (see [b-IETF RFC 2716], [b-IETF RFC 3748] and [b-IETF RFC 4017]). EAP supports several authentication methods, including MD5, transport layer security (TLS) with MD5 being the most widely supported and available. Regardless of EAP choice, all three IEEE 802.1X (see [b-IEEE 802.1X]) components have to support the same method (see Figure III.4.3).

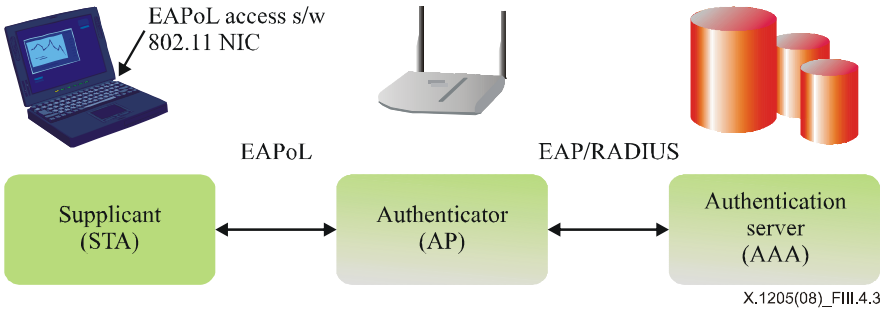

Figure III.4.3 – IEEE 802.1X components

The task of securing IEEE 802.1X roaming requires the user to always re-authenticate to the new AP to which it is roaming. Per-session keys and slow public key infrastructure (PKI) operations make fast re-authentication difficult. Therefore, there will be some difficulty with these authentication options for the hand-offs between APs while roaming.

For [b-IEEE 802.1X], EAP-TTLS and PEAP provide fast re-authentication for roaming. This can be accomplished by taking advantage of the connection re-establishment mechanism provided in the TLS handshake protocol. Full authentication is not required with the presumption that the knowledge of the master secret as evidenced by the ability to resume the TLS session is authentication enough.

III.4.4 Layered approach to securing wireless LANs

Good WLAN secure architectures require a layered approach applying multiple technologies, just as in regular LAN environments. The end solution should be an integrated WLAN/LAN security architecture. Wherever possible, existing LAN security mechanisms should be extended to serve the WLAN.

III.4.4.1 Access point

ESSID and MAC ACL may be used, even though they provide very weak security. All mobile units (MUs) and APs configured with the same ESSID can freely associate. [b-IEEE 802.11] supports a "broadcast ESSID," which permits an MU to associate to an AP without knowing the ESSID. Security can be enhanced if this feature is disabled. The MAC ACL contains a list of allowed MAC addresses and may contain a list of prohibited addresses, keeping in mind that this becomes difficult to manage when a large number of computers is involved.

Presently, AP products featuring pre-standard and proprietary security mechanisms including: WPA, WPA2, dynamic WEP advanced encryption standard (AES), temporal key integrity protocol (TKIP), and 128-bit encryption can be easily applied. Dynamic WEP is a means of changing the WEP key more often, at a predetermined interval. AES is the new FIPS-approved standard for replacement of the DES encryption algorithm. TKIP strengthens the key-scheduling algorithm to guard against key recovery attacks for classic WEP. Because of its weakness, [b-IEEE 802.11] recommends not using TKIP except as a patch to old equipment.

NOTE – The Wi-Fi protected access (WPA) started as an industry initiative that specifies improvements to wireless local area networking (LAN) security. WPA-PSK is a special mode of WPA for home users without an enterprise authentication server, and provides strong encryption protection. In WPA-PSK encryption, keys are automatically changed (re-keying) and authenticated between devices after a specified period of time, or after a specified number of packets has been transmitted. WPA-PSK uses a shared secret that is entered in both the wireless access point outer and the WPA clients. The shared secret can be between 8 and 63 characters long. The temporal key integrity protocol (TKIP) is used after the initial shared secret is entered in the wireless devices and handles the encryption and automatic re-keying. WPA is designed to be a software upgrade. Wireless vendors and security professionals expect today's WPA and WPA-PSK to be useful for a very long time. WPA defines the use of advanced encryption standard (AES) as an additional optional replacement for WEP encryption.

III.4.4.2 Air space

With a high-gain directional antenna, an outsider who wishes to gain unauthorized access to the WLAN can reach a WLAN from many miles away. It would be preferable to block the outsider from doing this. A method of blocking unauthorized outsiders from taking advantage of the open-air availability of the signal using a high-gain directional antenna may be to surround the perimeter of the corporate grounds or WLAN network with APs that are not connected to the internal network (see Figure III.4.4.2). An outsider is blocked from seeing the internal WLAN because the outside APs operate at the same carrier frequency as the internal ones, and offer a higher signal strength to the outsider, in effect, "jamming" the internal signal for the outsider. This set-up can be enhanced by connecting these external APs to an isolated network and adding an intrusion detection system (IDS) and honeypot for intrusion-detection and evidence gathering.

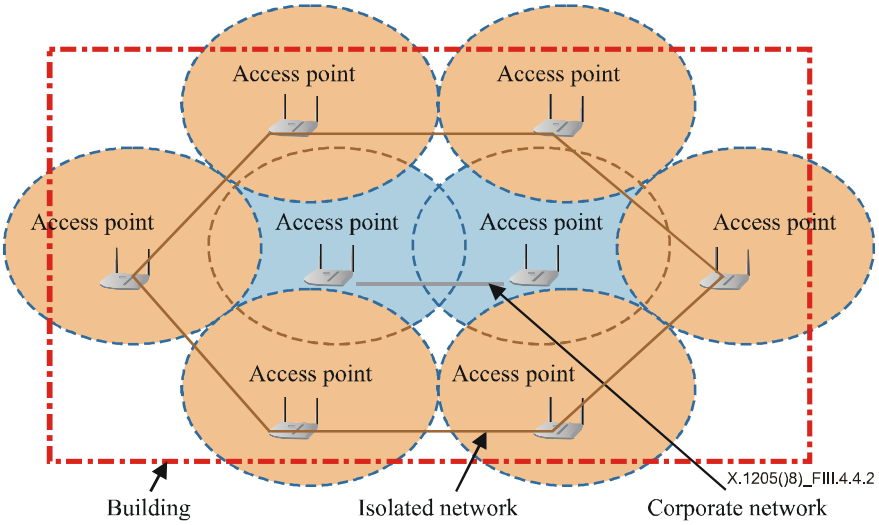

Figure III.4.4.2 – Sentry APs for perimeter security

III.4.4.3 Segmentation

Wherever possible, existing LAN security mechanisms should be extended to serve the WLAN. Additional mechanisms such as encryption through VPNs and TLS, segmentation of wireless segments through virtual LANs (VLANs), and perimeter defence through a firewall are effective regardless of the additional enhancements to [b-IEEE 802.1X]. Figure III.4.4.3 shows generic WLAN IEEE 802.11 APs with a common SSID or subnet connected to a layer 2 switch. The layer 2 switch can intelligently limit traffic going to other APs and some are capable of VLANs. For those APs residing on another subnet or SSID, connection could be made via a layer 2/3 routing switch. To this architecture, secure communications, secure roaming and hand-offs, and perimeter defence are considered as part of the secured and integrated WLAN/LAN network environment.

IPSec is a proven and trusted protocol for securing communications. For environments which can leverage IPSec clients on mobile devices or have applications with more than Web-based front ends, IPSec is the most appropriate means for securing communications. The main benefit of an IPSec VPN is that the corporation has complete control of the robust security policy such that someone attaching to a LAN has all the privileges of a local LAN user.

The same technique works for a "hot spot", WLAN. For example, for a remote employee accessing the network from a hotel's ISP, the employee could connect via DSL using a PPPoE client and a user ID/password provided by the hotel to access the ISP. The employee can then connect to their corporate network using an IPSec client.

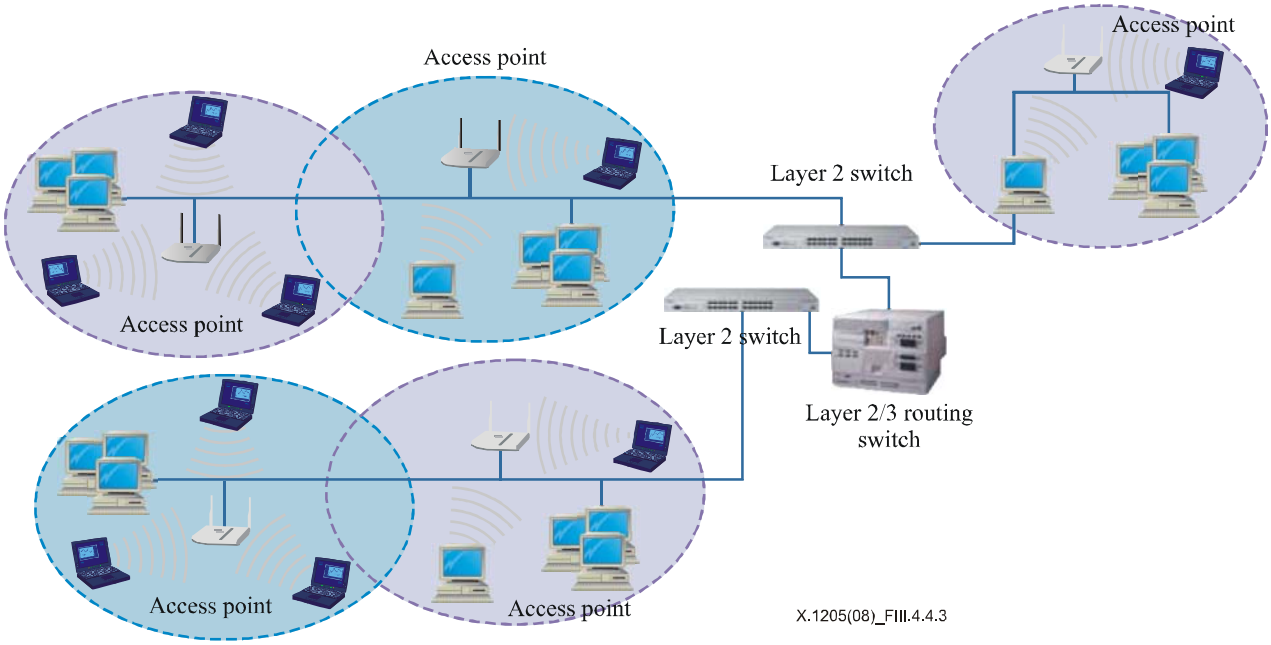

Figure III.4.4.3 – Generic WLAN IEEE 802.11 APs with a common SSID

III.4.4.4 Management layer

Managerial and operational countermeasures should also be used to secure WLANs, for example, by extending an organization security policy to include the WLAN. Wherever possible, existing LAN security mechanisms should be extended to serve the WLAN; otherwise, new mechanisms need to be integrated with existing mechanisms. For example, leveraging the IPSec solutions gives the enterprise centralized management of WLAN users, remote users, and firewall rules, and does not require an additional management application if it is already being used for extranet access. Vendors are adding WLAN awareness to mechanisms, such as network discovery, vulnerability scanners, and IDS.

III.4.4.5 Analysing WLAN access protocols

The relative strengths and weaknesses of the various Wi-Fi protocols discussed in the clauses above, namely IEEE 802.11i, WPA2[2], WPA and WEP can be analysed using the ITU-T X.805 dimensions. The analysis is illustrated for a couple of the dimensions, and can be extended to all eight dimensions.

The qualitative results for each Dimension are tabulated using the following legends:

√	Satisfactory
P	Partial
X	Not addressed by the standard

Access control

The original [b-IEEE 802.11] specifications, including WEP, had no built-in access control mechanism, thus larger WLAN deployments used a WLAN gateway for service level access control. Based on this assumption, access control for the WLAN service to the end-users has been rated as partially adequate.

---

2 Though the WPA2 and IEEE 802.11i have similar security features, the fact that WPA2 can interoperate with less secure WPA, weaknesses of WPA reflect on the security of WPA2.

[b-IEEE 802.1X] is the end-user access control mechanism for Wi-Fi service for IEEE 802.11i, WPA, and WPA2.

Table III.2 – Coverage for access control dimension

Access control security dimension								
Security planes	**Security layers**							
	Infrastructure				**Services**			
	IEEE 802.11i	**WPA2**	**WPA**	**WEP**	**IEEE 802.11i**	**WPA2**	**WPA**	**WEP**
End-user	√	√	√	X	√	√	√	P
Control	√	X	X	X	√	√	√	X
Management	X	X	X	X	X	X	X	X

Authentication

IEEE 802.11i, WPA2, and WPA use IEEE 802.1X/EAP for authentication. In contrast, WEP employs either "open" or "shared secret" authentication, which uses the same static key used for encryption. Thus, WEP authentication is rated "partial". Authentication in other standards could also receive the same rating if a weak EAP protocol like MD5 is selected for [b-IEEE 802.1X].

Authentication of control information across access points and other network elements (to support roaming) is only addressed in IEEE 802.11i. APs supporting other standards normally use proprietary mechanisms to exchange this information, while roaming and validating the security of such implementations is out of the scope.

Table III.3 – Coverage for authentication dimension

Authentication security dimension								
Security planes	**Security layers**							
	Infrastructure				**Services**			
	IEEE 802.11i	**WPA2**	**WPA**	**WEP**	**IEEE 802.11i**	**WPA2**	**WPA**	**WEP**
End-user	√	√	√	P	√	√	√	P
Control	√	X	X	X	√	√	√	X
Management	X	X	X	X	X	X	X	X

Availability

DoS attacks like RF jamming, data flooding, and layer 2 session hijacking, are all attacks against availability. None of the WLAN security standards can prevent attacks on the physical layer simply because they operate on layer 2 and above. Similarly, none of the standards can deal with an AP failure.

Table III.4 – Coverage for availability dimension

Availability security dimension								
Security planes	**Security layers**							
	Infrastructure				**Services**			
	IEEE 802.11i	**WPA2**	**WPA**	**WEP**	**IEEE 802.11i**	**WPA2**	**WPA**	**WEP**
End-user	P	P	P	X	P	P	P	X
Control	P	P	P	X	P	P	P	X
Management	X	X	X	X	X	X	X	X

It is apparent that relatively secure WLAN networks can be designed, implemented, and maintained using either IEEE 802.11i or WPA2. Simply implementing these standards, however, will not ensure end-to-end security for WLANs. As illustrated in this case study, the availability dimension is not addressed.

Bibliography

[b-ITU-T G.729] Recommendation ITU-T G.729 (2007), *Coding of speech at 8 kbit/s using conjugate-structure algebraic-code-excited linear prediction (CS-ACELP)*.

[b-ITU-T X.509] Recommendation ITU-T X.509 (2005), *Information technology – Open Systems Interconnection – The Directory – Public-key and attribute certificate frameworks*.

[b-ITU-T Y.2201] Recommendation ITU-T Y.2201 (2007), *NGN release 1 requirements*.

[b-IETF RFC 854] IETF RFC 854 (1983), *TELNET Protocol Specification* <http://www.ietf.org/rfc/rfc0854.txt?number=854>.

[b-IETF RFC 959] IETF RFC 959 (1985), *File Transfer Protocol (FTP)* <http://www.ietf.org/rfc/rfc0959.txt?number=959>.

[b-IETF RFC 1321] IETF RFC 1321 (1992), *The MD5 Message-Digest Algorithm* <http://www.ietf.org/rfc/rfc1321.txt?number=1321>.

[b-IETF RFC 1510] IETF RFC 1510 (1993), *The Kerberos Network Authentication Service (V5)* <http://www.ietf.org/rfc/rfc1510.txt?number=1510>.

[b-IETF RFC 1661] IETF RFC 1661 (1994), *The Point-to-Point Protocol (PPP)* <http://www.ietf.org/rfc/rfc1661.txt?number=1661>.

[b-IETF RFC 1991] IETF RFC 1991 (1996), *PGP Message Exchange Formats* <http://www.ietf.org/rfc/rfc1991.txt?number=1991>.

[b-IETF RFC 2104] IETF RFC 2104 (1997), *HMAC: Keyed-Hashing for Message Authentication* <http://www.ietf.org/rfc/rfc2104.txt?number=2104>.

[b-IETF RFC 2196] IETF RFC 2196 (1997), *Site Security Handbook* <http://www.ietf.org/rfc/rfc2196.txt?number=2196>.

[b-IETF RFC 2311] IETF RFC 2311 (1998), *S/MIME Version 2 Message Specification* <http://www.ietf.org/rfc/rfc2311.txt?number=2311>.

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

[b-IETF RFC 2427] IETF RFC 2427 (1998), *Multiprotocol Interconnect over Frame Relay* <http://www.ietf.org/rfc/rfc2427.txt?number=2427>.

[b-IETF RFC 2459] IETF RFC 2459 (1999), *Internet X.509 Public Key Infrastructure Certificate and CRL Profile* <http://www.ietf.org/rfc/rfc2459.txt?number=2459>.

[b-IETF RFC 2510] IETF RFC 2510 (1999), *Internet X.509 Public Key Infrastructure Certificate Management Protocols* <http://www.ietf.org/rfc/rfc2510.txt?number=2510>.

[b-IETF RFC 2616] IETF RFC 2616 (1999), *Hypertext Transfer Protocol -- HTTP/1.1* <http://www.ietf.org/rfc/rfc2616.txt?number=2616>.

[b-IETF RFC 2631] IETF RFC 2631 (1999), *Diffie-Hellman Key Agreement Method* <http://www.ietf.org/rfc/rfc2631.txt?number=2631>.

[b-IETF RFC 2661] IETF RFC 2661 (1999), *Layer Two Tunnelling Protocol "L2TP"* <http://www.ietf.org/rfc/rfc2661.txt?number=2661>.

[b-IETF RFC 2716] IETF RFC 2716 (1999), *PPP EAP TLS Authentication Protocol* <http://www.ietf.org/rfc/rfc2716.txt?number=2716>.

[b-IETF RFC 2748] IETF RFC 2748 (2000), *The COPS (Common Open Policy Service) Protocol* <http://www.ietf.org/rfc/rfc2748.txt?number=2748>.

[b-IETF RFC 2749] IETF RFC 2749 (2000), *COPS usage for RSVP* <http://www.ietf.org/rfc/rfc2749.txt?number=2749>.

[b-IETF RFC 2753] IETF RFC 2753 (2000), *A Framework for Policy-based Admission Control* <http://www.ietf.org/rfc/rfc2753.txt?number=2753>.

[b-IETF RFC 2828] IETF RFC 2828 (2000), *Internet Security Glossary* <http://www.ietf.org/rfc/rfc2828.txt?number=2828>.

[b-IETF RFC 2865] IETF RFC 2865 (2000), *Remote Authentication Dial In User Service (RADIUS)* <http://www.ietf.org/rfc/rfc2865.txt?number=2865>.

[b-IETF RFC 2869] IETF RFC 2869 (2000), *RADIUS Extensions* <http://www.ietf.org/rfc/rfc2869.txt?number=2869>.

[b-IETF RFC 3031] IETF RFC 3031 (2001), *Multiprotocol Label Switching Architecture* <http://www.ietf.org/rfc/rfc3031.txt?number=3031>.

[b-IETF RFC 3084] IETF RFC 3084 (2001), *COPS Usage for Policy Provisioning (COPS-PR)* <http://www.ietf.org/rfc/rfc3084.txt?number=3084>.

[b-IETF RFC 3174] IETF RFC 3174 (2001), *US Secure Hash Algorithm 1 (SHA1)* <http://www.ietf.org/rfc/rfc3174.txt?number=3174>.

[b-IETF RFC 3377] IETF RFC 3377 (2002), *Lightweight Directory Access Protocol (v3): Technical Specification* <http://www.ietf.org/rfc/rfc3377.txt?number=3377>.

[b-IETF RFC 3579] IETF RFC 3579 (2003), *RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)* <http://www.ietf.org/rfc/rfc3579.txt?number=3579>.

[b-IETF RFC 3580] IETF RFC 3580 (2003), *IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines* <http://www.ietf.org/rfc/rfc3580.txt?number=3580>.

[b-IETF RFC 3748] IETF RFC 3748 (2004), *Extensible Authentication Protocol (EAP)* <http://www.ietf.org/rfc/rfc3748.txt?number=3748>.

[b-IETF RFC 4017] IETF RFC 4017 (2005), *Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs* <http://www.ietf.org/rfc/rfc4017.txt?number=4017>.

[b-IETF RFC 4252] IETF RFC 4252 (2006), *The Secure Shell (SSH) Authentication Protocol* <http://www.ietf.org/rfc/rfc4252.txt?number=4252>.

[b-IETF RFC 4366] IETF RFC 4366 (2006), *Transport Layer Security (TLS) Extensions* <http://www.ietf.org/rfc/rfc4366.txt?number=4366>.

[b-IETF RFC 4557] IETF RFC 4557 (2006), *Online Certificate Status Protocol (OCSP) Support for Public Key Cryptography for Initial Authentication in Kerberos (PKINIT)* <http://www.ietf.org/rfc/rfc4557.txt?number=4557>.

[b-ISO/IEC 7816-x] ISO/IEC 7816-x, *Identification cards – Integrated circuit(s) cards with contacts* <http://www.iso.org/iso/search.htm?qt=7816&searchSubmit=Search&sort=rel&type=simple&published=on>.

[b-ISO/IEC 18028-2] ISO/IEC 18028-2:2006, *Information technology – Security techniques – IT network security – Part 2: Network security architecture.* <http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=40009>

[b-ISO/IEC 18028-3] ISO/IEC 18028-3:2005, *Information technology – Security techniques – IT network security – Part 3: Securing communications between networks using security gateways*.
<http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=40010>

[b-ISO/IEC 18028-5] ISO/IEC 18028-5:2006, *Information technology – Security techniques – IT network security – Part 5: Securing communications across networks using virtual private networks.*
<http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=40012>

[b-ISO/IEC 18043] ISO/IEC 18043:2006, *Information technology – Security techniques – Selection, deployment and operations of intrusion detection systems*.
<http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=35394>

[b-IEEE 802.11] IEEE 802.11-2007, *IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*.
<http://standards.ieee.org/getieee802/download/802.11-2007.pdf>

[b-IEEE 802.1X] IEEE 802.1X-2004, *IEEE Standard for Local and metropolitan area networks: Port-Based Network Access Control*
<http://www.ieee802.org/1/pages/802.1x.html>.

[b-W3C XML 1.0] W3C XML 1.0 (2004), *Extensible Markup Language (XML) 1.0 (Third Edition),* W3C Recommendation, Copyright © [4 February 2004] World Wide Web Consortium, (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University), <http://www.w3.org/TR/REC-xml/>.

[b-SSL3] The SSL Protocol Version 3.0, <http://wp.netscape.com/eng/ssl3/draft302.txt>

[b-WPA] Wi-Fi Alliance, *Wi-Fi Protected Access*, <http://www.wi-fi.org/white_papers/whitepaper-022705-deployingwpawpa2enterprise/>

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, 2009