International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1039

(10/2016)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Information and network security – Network security

Technical security measures for implementation of ITU-T X.805 security dimensions

Recommendation ITU-T X.1039

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	**X.1030–X.1049**
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1339
PKI related Recommendations	X.1340–X.1349
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699

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

Recommendation ITU-T X.1039

Technical security measures for implementation of ITU-T X.805 security dimensions

Summary

Many organizations in developing countries as well as developed countries may have difficulties in implementing the high-level dimensions described in Recommendation ITU-T X.805. Recommendation ITU-T X.1039 is aimed at providing a set of security measures to implement the high-level dimensions. It also provides technical implementation guidance for security measures that can be used to improve organizations' security response capabilities. A set of security measures described in this Recommendation could assist organizations in managing information security risks and implementing technical dimensions. The audience of this Recommendation includes, but is not limited to, those individuals responsible for implementing an organization's information security dimensions.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1039	2016-10-14	17	11.1002/1000/13059

Keywords

Security dimension, security measures, technical implementation guidance.

---

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

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/.

Table of Contents

Recommendation ITU-T X.1039

Technical security measures for implementation of ITU-T X.805 security dimensions

1 Scope

This Recommendation provides technical security measures for the implementation of [ITU-T X.805] security dimensions, which includes access control, communication security, authentications, and data confidentiality. It also provides examples for applying the set of technical security measures to the organizations with practical levels of information security dimensions, etc. in the appendices. It is not intended to cover all security measures, but to focus on several technical issues.

This Recommendation is applicable to all type of telecommunication organizations, including those in the developing countries.

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

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 access control [b-ITU-T X.800]: The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner.

3.1.2 authentication [b-ITU-T X.1254]: Provision of assurance in the identity of an entity.

3.1.3 authorization [b-ITU-T X.1254]: The granting of rights, which includes the granting of access based on access rights.

3.1.4 availability [b-ITU-T X.800]: The property of being accessible and useable upon demand by an authorized entity.

3.1.5 confidentiality [b-ITU-T X.800]: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

3.1.6 data integrity [b-ITU-T X.800]: The property that data has not been altered or destroyed in an unauthorized manner.

3.1.7 firewall [b-ISO/IEC 27033-1]: Type of security barrier placed between network environments – consisting of a dedicated device or a composite of several components and techniques – through which all traffic from one network environment traverses to another, and vice versa, and only authorized traffic, as defined by the local security policy, is allowed to pass.

3.1.8 intrusion detection [b-ISO/IEC 27039]: Formal process of detecting intrusions, generally characterized by gathering knowledge about abnormal usage patterns, as well as what, how, and which vulnerability has been exploited to include how and when it occurred.

3.1.9 intrusion detection system [b-ISO/IEC 27039]: Information systems used to identify that an intrusion has been attempted, is occurring, or has occurred.

3.1.10 intrusion prevention system [b-ISO/IEC 27039]: Variant on intrusion detection systems that are specifically designed to provide an active response capability.

3.1.11 privacy [b-ITU-T-X.800]: The right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

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

3.1.12 security gateway [b-ISO/IEC 27033-1]: Point of connection between networks, or between subgroups within networks, or between software applications within different security domains intended to protect a network according to a given security policy.

3.1.13 repudiation [b-ITU-T X.800]: Denial by one of the entities involved in a communication of having participated in all or part of the communication.

3.1.14 threat [b-ISO/IEC 27000]: Potential cause of an unwanted incident, which may result in harm to a system or organization.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

2FA Two-Factor Authentication

ACL Access Control Lists

AES Advanced Encryption Standard

ATM Automatic Teller Machine

CEO Chief Executive Officer

DDoS Distributed Denial of Service

DHCP Dynamic Host Configuration Protocol

DMZ Demilitarized Zone

FTP File Transfer Protocol

GGSN Gateway General packet radio service (GPSR) Support Node

GPRS General Packet Radio Service

HIDS Host Based Intrusion Detection System

HTTP Hypertext Transport Protocol

HTTPS Hypertext Transport Protocol Secure

ICT Information Communication Technology

IDPS Intrusion Detection and Prevention System

IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention Systems
IPSec	Internet Protocol Security
IPSG	IP Source Guard
ISP	Internet Service Provider
MFA	Multi-Factor Authentication
NIDS	Network Based Intrusion System
OS	Operating system
OSI	Open System Interconnection
PC	Personal Computer
PII	Personally Identifiable Information
PIN	Personal Identification Number
RPC	Remote Procedure Call
SFA	Single Factor Authentication
SGSN	Serving GPRS Support Node
SMB	Server Message Block
SNMP	Simple Network Management Protocol
TFA	Three-Factor Authentication
TLS	Transport Layer Security
VPN	Virtual Private Network

5 Conventions

None.

6 Overview of information security measures

A security measures is a means of managing risk, and includes policies, procedures, guidelines, practices or organisational structures, which can be of an administrative, technical, management, or legal nature.

A security dimension is a set of security measures designed to address a particular aspect of the network security. The security dimensions, defined in [ITU-T X.805] are:

- access control;
- authentication;
- non-repudiation;
- data confidentiality;
- communication security;
- data integrity;
- availability; and
- privacy.

A set of technical implementation guidance for each dimension should be defined and implemented by organizations.

This Recommendation presents a technical implementation guideline, which provides a set of security measures for each dimension, for mitigating the most common threats.

Deploying these security measures can assist an organisation in protecting against the most common forms of cyber-attack emanating from the external network.

Organisations implementing these security measures can benefit by gaining confidence that basic technical security measures are in place and that important steps are being taken to protect its information and system. The technical implementation guidance can be used to:

- improve organizations' security capabilities and posture;
- allow organizations to effectively and consistently evaluate security capabilities;
- share knowledge, best practices, and relevant documents across organizations as a means to improve security capabilities; and
- allow organizations to prioritize security measures and their associated activities and investment resources to improve security.

7 Information security measures

7.1 Access control

Access control protects against unauthorized use of network resources. User accounts, particularly those with special access privileges (e.g., administrative accounts) should be assigned only to authorized individuals, managed effectively and provide the minimum level of access to applications, computers and networks. User accounts should be managed through robust access control. The following information security measures should be considered regarding access control:

- Organizations should create user account according to a provisioning and approval process.
- Organization should allow special access privileges to a limited number of authorized individuals.
- Organizations should document details about special access privileges (e.g., the individual and purpose), keep them in a secure location and review them on a regular basis (e.g., quarterly).
- Organizations should use administrative accounts to perform authorized administrative activities, and should not grant access to the Internet.
- Organization should change password for administrative accounts on a regular basis (e.g., at least every 60 days).
- Organization should allow each user to be authenticated using a unique username and strong password before being granted access to applications, computers and network devices.
- Organizations should remove or disable user accounts and special access privileges when no longer required (e.g., when an individual changes role or leaves the organization) or after a pre-defined period of inactivity (e.g., 3 months).

7.2 Authentication

The authentication serves to confirm the identities of communicating entities. There are three types of authentication factors:

- knowledge factor ("something only a user knows"), such as passwords;
- possession factor ("something only a user has"), such as automatic teller machine (ATM) cards; and

- inherence factor ("something only a user is"), such as biometrics.

There are three types of authentication methods described in [b-ITU-T X.1158]:

- Single-factor authentication (SFA) is the traditional one that requires only a user name and password before granting access to the user.
- Two-factor authentication – Two-factor authentication (also known as 2FA) is based on using the combination of two different authentication factors. These factors may be something that a user knows, something that a user has or something that a user is. A good example in everyday life is that when a user wants to withdraw money from a cash machine, only the correct combination of a bank card (something that a user has) and a personal identification number (PIN), i.e., something that a user knows) allows the transaction to be conducted.
- Three-factor authentication (TFA) is based on using the combination of three different independent factors: what a user knows (password), what a user has (security token) and what a user is (biometric verification).

Multi-factor authentication (MFA) is based on using the combination of two or more independent different factors. Two-factor authentication and three-factor authentication are a part of multi-factor authentication.

The organizations should determine the authentication methods based on the result of risk assessment. User authentication should be managed through robust authentication. Organizations should consider the following information security measures regarding authentication:

- Organizations should use the methods of authentication which is appropriate for the classification of the information to be accessed.
- Organizations should employ a strong authentication method such as two-factor or three-factor authentication (identity/password, one-time password, public-key certificate) when using privileged access right to information system and applications as an administrator.
- Organizations should provision identities for personnel and other entities (e.g., services, devices) who require access to assets (note that this does not preclude shared identities).
- Organizations should issue credentials for personnel and other entities that require access to assets (e.g., passwords, smart cards, certificates, keys).
- Organizations should de-provision identities when no longer required.
- Organizations should periodically review and update identity repositories to ensure validity (i.e., to ensure that the identities still need access).
- Organizations should periodically review credentials to ensure that they are associated with the correct person or entity.
- Organizations should de-provision identities within organizationally defined time thresholds when no longer required.
- Organizations should inform employees of requirements for credentials according to the organization's risk criteria (e.g., multifactor credentials for higher risk access).

7.3 Non-repudiation

The non-repudiation provides means for preventing an individual or entity from denying having performed a particular action related to data by making available proof of various network-related actions (such as proof of obligation, intent, or commitment; proof of data origin, proof of ownership, proof of resource use). Organizations should consider the following information security measures regarding non-repudiation:

- Organizations should incorporate procedures to ensure non-repudiation.
- Organizations should implement appropriate measures such as using digital signature to guard against later denial that they furnished the signature.

- Organizations should use technical mechanisms for non-repudiation in [b-ITU-T X.813].
- Organizations should use cryptographic techniques to support non-repudiation and to provide evidence of the occurrence or non-occurrence of an event or action.

In addition, the implementation guidance for cryptography from [b-ITU-T X.1051] clause 10 could also be considered.

7.4 Data confidentiality

The data confidentiality protects data from unauthorized disclosure. Sensitive information in transit or at rest should be protected by appropriate measures. Organizations should consider the following information security measures regarding data confidentiality:

- Organizations should implement appropriate measures such as cryptographic technologies and data leakage prevention technologies to prevent unauthorized disclosure of sensitive personal data at rest or in transit.
- Organization should incorporate procedures to ensure data confidentiality.
- Organizations should use technical mechanisms for data confidentiality in [b-ITU-T X.814].
- In addition, the implementation guidance from [b-ITU-T X.1051] clause 10 could also be considered.

7.5 Communication security

Information, applications and computers within the organization's internal networks should be protected against unauthorized access and disclosure from the internet, using boundary firewalls, internet gateways or equivalent network devices.

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

7.5.1 Security gateway

A security gateway is placed at the boundary between two network segments, for example, between the organization's internal network and a public network, to filter the traffic flowing across the boundary in accordance with the documented security gateway service access policy for that boundary.

7.5.2 Firewall

The firewall is a typical implementation of the security gateway that controls the incoming and outgoing network traffic based on an applied rule set. A firewall establishes a barrier between a trusted, secure internal network and another external network (e.g., the Internet) that is assumed not to be secure and trusted. There are two types of firewalls: software-based firewall which is implemented as software to run on general purpose hardware and a hardware-based firewall which exists as hardware appliance. Many hardware-based firewalls also offer other functionality to the internal network they protect, such as acting as a dynamic host configuration protocol (DHCP) server for that network.

7.5.3 Intrusion detection system

An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station. There are two types of IDS: network based intrusion system (NIDS) and host based intrusion detection systems (HIDS).

7.5.4 Intrusion prevention system

Intrusion prevention systems (IPS), also known as intrusion detection and prevention systems (IDPS), are network security appliances that monitor network and/or system activities for malicious activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about this activity, attempt to block/stop it, and report it. Intrusion prevention systems are considered extensions of intrusion detection systems because they both monitor network traffic and/or system activities for malicious activity. The main differences are, unlike intrusion detection systems, intrusion prevention systems that are placed in-line and are able to actively prevent/block intrusions that are detected.

7.5.5 Application firewall

An application firewall is a form of firewall which controls input, output, and/or access from, to, or by an application or service. It operates by monitoring and potentially blocking the input, output, or system service calls which do not meet the configured policy of the firewall. The application firewall is typically built to control all network traffic on any open system interconnection (OSI) layer up to the application layer. It is able to control applications or services specifically, unlike a stateful network firewall which is – without additional software – unable to control network traffic regarding a specific application.

7.5.6 Technical implementation guidance

End points, such as personal computers and notebook computers that are able to access external network and communicate through the wireless access point should be assigned in order to protect unauthorized access from attacks outside.

When wireless access points are deployed, security mechanisms (i.e., Wi-Fi Protected Access II [b-Wi-Fi]) should be used in order to protect communications between the access point and mobile station.

Public network access from personal computers that are able to access the information systems dealing with processing massive personally identifiable information (PII) should be prohibited.

Internal network should be segregated via a firewall to protect internal operation network from attacks outside. Public server such as web server should exist in the demilitarized zone which exists between the internal operation network and external network.

Unauthorized use of wireless access point should be detected and unauthorized access to the internal information system through the wireless access point protected.

One or more firewalls (or equivalent network device) should be installed on the boundary of the organisation's internal network(s). As a minimum:

- The default administrative password for any firewall (or equivalent network device) should be changed to an alternative, strong password.
- Each rule that allows network traffic to pass through the firewall (e.g., each service on a computer that is accessible through the boundary firewall) should be subject to approval by an authorised individual and documented (including an explanation of business need).
- Unapproved services, or services that are typically vulnerable to attack (such as server message block (SMB), NetBIOS, tftp, remote procedure call (RPC), rlogin, rsh or rexec), should be disabled (blocked) at the boundary firewall by default.
- Firewall rules that are no longer required (e.g., because a service is no longer required) should be removed or disabled in a timely manner.
- The administrative interface used to manage boundary firewall configuration should not be accessible from the Internet.

Organizations should install one or more firewalls, intrusion detection systems, application firewall on the boundary of and within the organization's internal network(s) according to risk assessment result. In addition,

- organization should operate network success control functions for end points, such as desktop PC and notebook computers, which can access wireless access point or/and the internal wired network to prevent unauthorized access to the internal network;
- when using wireless access point, organization should have secure access point configuration in place, for example, use of secure transfer mode;
- organization should prevent remote access to information system which processes massive amount of PII, for example, to a database containing user's ID and password;
- organization should operate demilitarized zone (DMZ) to separate internal network with external network and operate public server such as web server in DMZ area;
- organization should operate the wireless intrusion detection system which can detect and prevent any unauthorized use of wireless access points.

7.6 Data integrity

Data integrity ensures the correctness or accuracy of data, and protects against improper information modification or destruction. It includes ensuring information non-repudiation and authenticity. For an asset, integrity is the quality of being in the condition intended by the owner and therefore continuing to be useful for the purposes intended by the owner. Organizations should consider the following information security measures regarding data integrity:

- Organization should evaluate suggested changes to inventoried assets before applying them.
- Organization should log changes to inventoried assets.
- Organization should test changes to assets prior to its deployment, whenever possible.
- Change management practices address the full life cycle of assets (i.e., acquisition, deployment, operation, retirement).
- Organization should test changes to assets for security impact prior to deployment.
- Change logs include information about modifications that impact the security requirements of assets (availability, integrity, confidentiality).

7.7 Availability

Availability ensures that there is no denial of authorized access to network elements, stored information, information flows, services and applications due to events impacting the network.

One of the typical attacks which compromise network availability is a distributed denial of service (DDoS) attack which is an attempt to make an online service unavailable by overwhelming it with massive amount of traffic from multiple sources.

DDoS mitigation system is a hardware that includes purpose-built automated network devices for detecting and mitigating some levels of DDoS attacks. Sometimes perimeter security hardware such as firewalls and intrusion detection systems (IDS) may include features intended to address some types of small DDoS attacks. DDoS mitigation system performs three basic functionalities as follows:

- mitigating DDoS attack, not just detecting;
- distinguishing good traffic from bad traffic to preserve business continuity, not just detecting the overall presence of an attack;
- maintaining reliable and cost-efficient scalability.

A DDoS protection system provided additional protection functionalities as follows:

- enables immediate response to DDoS attacks through integrated detection and blocking mechanisms, even during spoofed attacks when attacker identities and profiles are changing constantly;
- provides more complete verification capabilities than either static router filters or IDS signatures can provide to date;
- delivers behaviour-based anomaly recognition to detect valid packets sent with malicious intents to flood a service;
- identifies and blocks individual spoofed packets to protect legitimate business transactions;
- offers mechanisms designed to handle the huge volume of DDoS attacks without suffering the same fate as protected resources;
- enables timely deployment to protect the network during attacks without introducing a point of failure;
- processes (with built-in intelligence) only contaminated traffic streams, helping ensure maximum reliability and minimum scaling costs;
- avoids reliance on network device resources or configuration changes;
- uses standard protocols for all communications, helping ensure maximum interoperability and reliability.

Organizations should install DDoS protection system on the boundary of and within the organization's internal network(s) according to risk assessment result. To this end:

- Organizations could have a capability to use DDoS protection service provided by the Internet service provider (ISP).
- Organizations should deploy a DDoS protection system on the boundary of and within the organization's internal network(s).

7.8 Privacy

The privacy security dimension provides for the protection of information that might be derived from the observation of network activities.

- Appropriate measures should be implemented to protect personally identifiable information processed.

Additional ISO/IEC guidance for the protection of PII can be found in [b-ISO/IEC 29100]. [b-ISO/IEC 29100] describes basic privacy requirements in terms of three main factors: (1) legal and regulatory requirements for the safeguarding of the individual's privacy and the protection of his/her PII, (2) the particular business and use case requirements, and (3) individual privacy preferences of the PII entity. [b-ISO/IEC 29100] describes the following basic privacy principles: consent and choice, purpose specification, collection limitation, use, retention and disclosure limitation, data minimization, accuracy and quality openness, transparency and notice, individual participation and access, accountability, security controls and compliance.

Annex A

Additional technical implementation guidance

(This annex forms an integral part of this Recommendation.)

This annex provides additional implementation guidance to implement [ITU-T X.805] security domains.

A.1 Secure configuration

Configuration management is the task of tracking and controlling changes in the software.

Computers and network devices should be configured to reduce the level of inherent vulnerabilities and provide only the services required to fulfil their role. Computers and network devices (including wireless access points) should be securely configured. To this end:

- Organizations should remove and disable unnecessary user accounts (e.g., guest accounts and unnecessary administrative accounts).
- Organizations should change any default password for a user account to an alternative, strong password.
- Organizations should remove or disable unnecessary software (including application, system utilities and network services).
- Organizations should disable the auto-run feature to prevent software programs running automatically when removable storage media is connected to a computer or when network folders are accessed.
- Organizations should enable a personal firewall (or equivalent) on desktop personal computers (PCs) and laptops, and configured to disable (block) unapproved connections by default.

A.2 Malware protection

Malware (short for malicious software) is software designed to infiltrate or damage a computer without user's consent. Malware includes computer viruses, worms, Trojan horses, spyware, scareware and more. It can be present on websites and emails or hidden in downloadable files, photos, videos, freeware or shareware. (However, it should be noted that most websites, shareware or freeware applications do not come with malware.)

The best way to avoid getting infected is to run a good anti-virus protection program, do periodic scans for spyware, avoid clicking on suspicious e-mail links or websites. But scammers are sneaky: sometimes malware is cleverly disguised as an email from a friend, or a useful website.

Computers that are exposed to the internet should be protected against malware infection through the use of malware protection software. The organization should implement robust malware protection on exposed computers. To this end:

- Organizations should install malware protection software on all computers that are connected to or capable of connecting to the Internet.
- Organizations should keep malware protection software (including program code and malware signature files) up-to-date (e.g., at least daily, either by configuring it to update automatically or through the use of centrally managed deployment).
- Organizations should configure malware protection software to scan files automatically upon access (including when downloading and opening files, accessing files on removable storage media or a network folder) and scan web pages when being accessed (via a web browser).

- Organizations should configure malware protection software to perform regular scans of all files (e.g., daily).
- Organizations should install malware protection software to prevent connections to malicious websites on the internet (e.g., by using website blacklisting).

A.3 Patch management

A patch is a piece of software designed to update a computer program or its supporting data, to fix or improve it. Patch management is the process of using a strategy and plan of what patches should be applied to which systems at a specified time.

Software running on computers and network devices should be kept up-to-date and have the latest security patches installed. Software should be kept up-to-date, and to this end:

- Organizations should have a license for software running on computers and network devices that are connected to or capable of connecting to the internet (by the software vendor or supplier of the software) to ensure security patches for known vulnerabilities are made available.
- Organizations should install updates to software (including operating system software and firmware) running on computers and network devices that are connected to or capable of connecting to the internet in a timely manner (e.g., within 30 days of release or automatically when they become available from vendors).
- Organizations should remove out-of-date software (i.e., software that is no longer supported) from computer and network devices that are connected to or capable of connecting to the Internet.
- Organizations should install all security patches for software running on computers and network devices that are connected to or capable of connecting to the Internet in a timely manner (e.g., within 14 days of release or automatically when they become available from vendors).

A.4 Vulnerability management

Vulnerability management is the practice and procedure of identifying, classifying, remediating, and mitigating vulnerabilities. To this end:

- Organizations should establish a vulnerability management plan, including identifying information assets for personnel in charge of monitoring cycle and target systems, and the methodology for the vulnerability management.
- Organizations should conduct vulnerability monitoring against information systems and services that an organization manage.
- The vulnerability monitoring results should be reported to the personnel who are in charge of security in an organization.
- The competent personnel in an organization should conduct vulnerability monitoring.
- Vulnerability monitoring for critical information asset such as web servers and information systems processing PII should be carried out at least two times per year.
- Timely remedy should be taken and remedy result should be reported to the personnel who is in charge of information security.

A.5 Information security incidents management

This security measure ensures information security events and vulnerabilities associated with the organization's information and information system assets are communicated in a manner to allow appropriate corrective actions to be taken.

Managing incidents effectively involves detective and corrective security measures designed to minimize adverse impacts, gather forensic evidence (where applicable) and learn the lessons in terms of the implementation of more effective preventive measures. To this end:

- Organizations should operate information systems for detecting incidents and maintain the event records.
- Organizations should establish management framework and document roles and responsibilities for and process and procedures of the incident management, and maintain point of contacts for the incident management in an organization.
- Organizations should conduct continuous, consistent monitoring to prevent sensitive data leakage incident and systems being hacked.
- Organization should have appropriate incident corrective actions in place according to the nature of incidents.
- Organization should conduct training and testing to verify the effectiveness of incident response systems at least one time every year and provide the report to the personnel in charge of information security on any necessary actions and remedies for mitigating the occurrence of incidents.

A.6 System development security

Secure development is a requirement to build up a secure service, architecture, software and system. To this end:

- Organizations should identify security requirements, such as compliance requirements (i.e., encryption requirement) and apply them to any information system development efforts.
- Organizations should ensure that software developers complete training and education programme, for example on secure coding technology, or use monitoring tool to check if secure coding techniques are applied.
- Organizations should conduct vulnerability monitoring for the software that has been developed and have remedy actions in place for identified vulnerabilities, if necessary, prior to deploying it in a real operating environment.
- Organizations should separate the operation server from the server for development and testing data should be used when testing the server.

A.7 Authentication for information systems and applications

Procedures should be established to ensure strong authentication for information systems and applications. To this end:

- User authentication management should use secure password in terms of strength and length when users and/or administrator access information systems and applications.
- Organizations should have the security policy and procedures in place, concerning identification and authentication to information systems and applications.
- Organizations should check if authentication practice meets requirements according to security policy and guidance.
- Organizations should grant access privilege to information systems and applications only to the administrator according to their authorization procedure.
- Organizations should employ strong authentication method, for example multi-factor authentication such as combined use of the one-time password and public-key certificate when administrator's privilege are used to access information system and applications.

A.8 Data leakage prevention

Procedures should be established to ensure prevention of data leakage in an organization. To this end:

- Organizations should encrypt sensitive information in transit and at rest according to organizational policy.
- Organizations should have data leakage prevention system in place to prevent unauthorized disclosure of data through the use of portable media and removable media.
- Organizations should have security system in place to detect and prevent unauthorized leakage of sensitive data by insiders.
- Organizations should analyse log information recorded by the information security gateway and database to detect and prevent data leakage in advance.

A.9 Operations security

Secure operations of information processing facilities should be ensured. To this end:

- Organizations should implement malware protection measures: anti-virus program installation, patching of vulnerable system, and blocking remote use and access to internal information systems.
- Organizations should establish the procedure for assigning administrator for information systems and managing policy update, ruleset change, and events monitoring of information systems according to type and nature of information systems.
- Organizations should produce event logging recordings and keep (at least 6 months) and review regularly them.
- Organizations should establish and implement procedures for managing information systems and services operations (i.e., management for configuration change, acquisition, performance monitoring and recovery procedure from failure event).

Organizations should ensure security of teleworking.

A.10 Backup and disaster recovery

Procedures for backup and disaster recovery should be established to protect loss of data. To this end:

- Organizations should establish policy for backup and recovery, define requirements of backup of information, software and systems to ensure integrity and availability of information assets, and conduct backup procedure periodically according to organization's backup policy.
- Organizations should provide appropriate level of physical and environmental protection of critical backup information i.e., a secure place to prevent physically unauthorized access and environmental threats.
- Organizations should maintain real-time backup system and store the backup information in a remote location, at a sufficient distance to escape any damage from a disaster at the main site.
- Organizations should conduct disaster recovery training regularly (at least one time per year) using backup information.

A.11 Desktop PC and mobile device protection

Desktop PC should be protected by appropriate security measures. When using mobile devices, organizations should take special care to ensure that business information is not compromised data. To this end:

- Organizations should define and disseminate security guidance of desktop PCs to support user's self-assessment.

- Organizations should periodically monitor the effectiveness of security measures against the desktop PC for business (i.e., anti-virus program installation and update configuration, security patch for operating systems and removing shared directory).
- Organizations should establish and operate centralized management system to apply security measures in a centrally controlled manner against PCs in a business environment.
- Organizations should establish and implement security practices for use of mobile device (notebook, smart device, smart phones, and smart pad) in business.

Appendix I

Organizational implementation guidance

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

This appendix provides additional organizational implementation guidance that an organization can consider.

I.1 Information security policies

A set of operational policies should be defined, approved by management, published and communicated to employees and relevant external parties. In this regard:

- Organizations should document operational policies including management commitment to operational policies, compliance to relevant laws/regulations.
- Organizations should publish operational policies, approved by management, which are easily accessible by all employees.
- Organizations should review the operational policies periodically on a regular basis to take into account updates of laws/regulations.
- Organizations should put disciplinary measures in place to address employees breaching the operational policies.

The organization's approach to managing information security and its implementation should be reviewed independently at planned intervals or when significant changes occur.

- The individual in charge of information security in top management should review implementation of security measures at least once per year to ensure that all activities relevant to information security are properly maintained.
- Organizations should establish the review of implementation including review team, timeline for review, scope of implementation, and items to be reviewed.
- The review results should be reported to management including the chief executive officer (CEO) and communicated to relevant employees for corrective actions.
- The review should be conducted by an independent and competent team.

I.2 Organization of information security

- Organizations should identify and set up the following tasks:
  - roles and responsibilities;
  - relevant laws and regulations;
  - security objectives and assets to be protected;
  - resource (budget, human) plan.
- An organization should appoint an individual in charge of information security in top management to ensure that assets and technologies are adequately protected.
- The individual in charge of information security in top management security measures should be competent and have the appropriate education, training, and experience to perform information security.
- The information security organization should periodically report information security activities to the individual in charge of information security in top management .

Annual information security plan should be established.

- Organizations should establish the annual information security controls to address risks in an annual information security plan.

- Organizations should document an annual information security plan including scope to be protected, owner of controls, control objectives, and implementation timeline.
- Organizations should obtain approval of the information security plan from the individual responsible for implementing security measures.
- Implementation of the information security plan should be reviewed by the individual responsible for implementing security measures.

The organization should have budget to implement the controls.

- Organizations should establish and document the information security budget plan, obtain approval of this budget plan from the top management.
- Organizations should assign and invest at least a certain ratio of budget of information security to that of information communication technology (ICT).
- Organizations should evaluate and audit the implementation of the budget plan periodically.

The organization should provide dedicated resources needed for the establishment, implementation, maintenance and continual improvement of the information security.

- Organizations should assign information security staff who are in charge of operation of information security and document their roles and responsibilities.
- Organizations should engage information security staff with a number of years of experience, a certain degree of education, and certifications relevant to information security.
- Information security staff should take training courses for at least the number of hours per year specified in the information policy.
- Organizations should have dedicated information security staff.

The organization should perform internal and external communications regarding the information security as follows:

- Organizations should periodically provide the CEO with the necessary information relevant to information security (for example, newsletter, best practices, implementation guidance etc.).
- Organizations should inform external parties of any updates of technologies and regulations at least once per year.
- Organizations should conduct periodic internal briefings with information security staff.
- Organizations should have a periodic internal meeting with the participation of the CEO, the individual responsible for implementing security measures, and relevant employees to determine the information security policy.

I.3 Human resources security

Organizations should conduct human resources security during the whole life cycle of employment: prior to employment, during employment and termination of employment. To facilitate the human resources security process:

- Organizations should obtain from the employee, prior to employment, information security related agreement including confidential and non-disclosure, legal responsibilities and rights, disciplinary actions in case of a breach of the information security policies.
- Organizations should obtain separate information security pledge agreement including confidential and non-disclosure, legal responsibilities and rights, disciplinary actions when breaching the information security policies from employee on termination of employment.
- Organizations should withdraw as soon as possible (at least within five days) access right to the information system, and restrict operation rooms to staff that terminates or changes employment.

All employees and contractors should receive appropriate awareness education and training along the following guidelines:

- Organizations should establish the annual education and training plan and conduct them at planned intervals.
- Organizations should conduct education and training for all staff and contractors.
- Organizations should conduct education and training of the staff of the organization and contractors dedicated to specific roles.
- Organizations should submit a report related to the education and training to management including the individual responsible for implementing security measures with the feedback result from trainees, participation rates and corrective actions.
- Organizations can encourage participation in education and training.
- Organization should establish and provide information security awareness program to the staff that has access right to the critical information system and PII processing system requesting employees to comply with the information security policies of an organization.

I.4 Asset management

Assets should be identified and an inventory of these assets should be systematically maintained and to this end:

- Organizations should identify, document and keep up-to-date an inventory of assets.
- Organizations should classify information in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification.
- Organizations should maintain a log to record the change or modification of assets.
- Organizations should check on a regular basis consistency of assets (for example asset owner, Internet protocol (IP) address, physical deployment location, administrator) against the inventory of assets.

I.5 Physical and environment security

Organizations should prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities. In order to guarantee physical and environment security:

- Organizations should provide secure areas to guard either sensitive or critical information and information processing facilities.
- Organizations should apply the necessary physical protection facilities (for example, the fire extinguisher) to protect against natural disasters, malicious attack or accidents.
- Organizations should apply (for example, the emergence power supplier and uninterruptable power supply) to protect from power failures and other disruptions caused by failures in supporting utilities.
- Organizations should operate supporting utilities (for example, air conditioning, sewage and ventilation) for stable operation of information processing system.

Organizations should ensure that only authorized personnel be allowed access to the secure area that contains both sensitive or critical information and information processing facilities. In order to ensure this:

- Organizations should operate physical entry control to secure areas to ensure that only authorized personnel is allowed access and record the data and time of entry and departure of visitor.
- Organizations should perform physical entry control for visitors to secure areas: the identity of visitors should be registered and authenticated by an appropriate means, the internal

personnel should accompany visitors, and physically separated visitor's reception room should be provided outside secure areas.

- Organizations should record and monitor all entries and departures of visitors to secure areas and all activities of visitors in the secure area by some monitoring facilities.
- Organizations should register incoming materials (for example, notebook computers, computing facilities, removable media, smart devices in accordance with asset management policies on entry to the site and inspected incoming materials for evidence of tampering en route.

Organizations should ensure physical security for offices and rooms. To this end:

- Organizations should put in place measures, e.g., paper shredders, to destroy sensitive and confidential documents and provide a cabinet to store sensitive documents.
- Organizations should establish the office security policy for entry control and secure document management and review implementation of this policy on a monthly basis.
- Organizations should apply an entry control to the secure document storage and secure office and rooms to ensure that only authorized personnel is allowed access to them.
- Organizations should apply a physical access control to the office machines (for example, facsimile, copy machine and scanner) to ensure that only authorized personnel is allowed access.

I.6 Supplier relationship

Organizations should conduct supplier relationships' security measures as follows:

- Organizations should obtain information security pledge agreement from the employee of contractors, who has access right to the critical information system and PII processing system.
- Organizations should establish information security terms in an agreement and contracts for inclusion: the purpose and scope of each supplier, obligation of each contractual party to implement an agreed set of controls, relevant regulations for sub-contracting, right to audit the supplier processes and controls related to the agreement, supplier's obligation to periodically deliver an independent report on the effectiveness of controls, legal and regulatory requirements.
- Organizations should evaluate the implementation of information security controls when contractors terminates the supplier relationship: safe return of assets provided, complete destruction of sensitive information, and non-disclosure of information acquired during being outsourced.
- Organizations should establish and implement information security policy for supplier relationships including identifying management owner, procedure and process for managing information security policy for supplier relationships.
- Organizations should identify and put in place information security requirements and perform regular evaluation to audit the compliance of the supplier processes and controls with the agreement or contract.

Further implementation guidance is provided in [b-ITU-T X.1051].

Appendix II

Level of security assurance

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

This appendix provides typical examples of level of assurance related to the security.

II.1 Level of assurance for entity authentication [b-ITU-T X.1254]

This entity authentication assurance framework in [b-ITU-T X.1254] defines four levels of assurance (LoA) for entity authentication.

II.2 Level of security assurance

This appendix presents the example of five levels of security assurance (LoA) in an organization as shown in Table II.1.

Table II.1 – Level of security assurance [b-SECU]

Level	Description
1-limited (B)	Organizational security practices are not formalized, and risk is not managed.
2-partial (BB)	Organizational security practices are not formalized, and risk is managed in an ad hoc and sometimes reactive manner.
3-medium (A)	Risk management practices are approved by management but may not be established as organizational-wide policy.
4-repeatable (AA)	The organization's security practices are formally approved and expressed as policy. Organizational security practices are regularly updated based on the application of risk management processes to changes in business/mission requirements and a changing threat and technology landscape.
5-adaptible (AAA)	The organization adapts its security practices based on lessons learned and predictive indicators derived from previous and current cybersecurity activities.

Appendix III

Guidance on assigning specific level of security assurance from the final index

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

III.1 Methodology for level of security assurance

This appendix suggests how to calculate the level of security assurance. The following steps apply:

- Select all indicators (that are of interest to an organization) in the technical implementation guidance (in clause 7, Annex A, Appendix I).
- Determine sub-indices from indicators, depending on their nature.
- Determine the weight for indicators and sub-indices.
- Calculate the value of weighted indicators and sub-indices.
- Calculate the final value by summing up the weighted indicators.
- Assign the specific level of security assurance according to final values (see Table III.1 for example).

This appendix provides an example about level of security assurance from the final index values.

Table III.1 – Level of security assurance [b-SECU]

Level of security assurance	Final assurance value
1-limited (B)	B_{min}(for example, 0.23) >= and > B_{max}(for example, 0.4)
2-partial (BB)	BB_{min}(for example, 0.4) >= and > BB_{min}(for example, 0.6)
3-medium (A)	A_{min}(for example, 0.6) >= and > A_{min}(for example, 0.8)
4-repeatable (AA)	AA_{min}(for example, 0.8) >= and > AA_{min}(for example, 0.9)
5-adaptible (AAA)	>= $AAAA_{min}$(for example, 0.9)

The parameters in Table III.1 should be determined according to security policies in an organization.

Appendix IV

SGSN specific implementation guideline

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

This appendix provides implementation guidance for SGSN (Serving GPRS Support Node) based on security dimension described in [ITU-T X.805] security dimension.

IV.1 Overview

General packet radio service (GPRS) is based on IP. The serving GPRS support node (SGSN) is a main component of the GPRS network, which deals with all packet switched data within the network. Table IV.1 provides an [ITU-T X.805] security architecture.

Table IV.1 – Security architecture

	Infrastructure layer	**Services layer**	**Application layer**
End user plane	Module 3	Module 6	Module 9
Control plane	Module 2	Module 5	Module 8
Management plane	Module 1	Module 4	Module 7

The infrastructure layer refers to components that are individual network elements (i.e., SGSN) as well as the communication links between them. The management plane is concerned with operations, administration, maintenance and provisioning (OAM&P) activities such as provisioning a user or network elements.

IV.2 Access control dimension for module 1

The access control dimension protects against unauthorized access of network elements and ensures that only authorized personnel or devices are allowed access network elements. The following measures should be ensured:

- Management access user restriction: SGSN is provided with role-based access control (RBAC) which provides different access levels to guarantee that individuals can only perform the operations that they are authorized for.
- Management IP access restriction: Access control lists (ACLs) are deployed on the SGSN to limit the IP addresses or networks to ensure that only authorized personnel or devices are allowed access to network node elements, stored information, information flows, services and applications.
- Password/secret stored locally in SGSN are in encrypted form and protected using strong algorithms (e.g., NIST approved algorithms).
- Password lockout – SGSN detects repeated invalid attempts to sign into an account with incorrect passwords, i.e., by performing brute-force attack (for example, password guessing or dictionary based attacks, etc.).

IV.3 Availability dimension for module 1

The availability security dimension ensures that there is no denial of authorized access to SGSN's stored information, information flows, services and applications due to network interruption. The following should be ensured:

- Vulnerabilities of protocol are removed for management protocols of SGSN, i.e., file transfer protocol (FTP), Telnet, hypertext transport protocol (HTTP), and simple network management protocol (SNMP).

- SGSN is able to handle all the malformed and anomalous traffic.
- SGSN does not hang in a busy loop, causing a permanent denial-of-service situation.
- SGSN software is provided with anti-source IP spoofing protection mechanisms like unicast Reverse path forwarding (RPF) and IP source guard (IPSG).

IV.4 Non repudiation dimension for module 1

The non-repudiation dimension provides a record identifying each individual or device that accessed the SGSN and the record is to be used as a proof of access to the end-user data. The following should be ensured:

- Audit data event generation: SGSN generates logs for the specified auditable event(s).
- Audit data protection: Access and deletion of audit information is restricted to a certain subset of users.

IV.5 Authentication dimension for module 1

Authentication is the provision of proof that the claimed identity of an entity is true. Entities include not only human users but also devices, services and applications. Entities are authenticated before performing any action on SGSN. The following should be ensured:

- Management user authentication: Remote access to the SGSN for configuration and maintenance purposes is granted only to authenticated users.

IV.6 Data integrity dimension for module

Data integrity is the property that data have not been altered in an unauthorized manner. Data integrity also ensures that information is protected against unauthorized modification. The following should be ensured:

- Software integrity check feature for operating system (OS)/application image of SGSN is checked during the installation process.
- SGSN supports the possibility of preventing illegal software installation by verifying its integrity (e.g., hashing for integrity check).

IV.7 Privacy and data confidentiality dimension for module 1

Privacy considers the protection of the association of the identity of users and the activities performed by them. Data confidentiality considers the protection against unauthorized access to information asset. Encryption, access control lists, and file permissions are methods for data confidentiality. The following should be ensured:

- Login credentials for the remote access are not captured by unauthorized user using application layer encryption protocols, such as hypertext transport protocol secure (HTTPS), SSHv2, or lower tunnelling protocol such as Internet protocol security (IPsec) virtual private network (VPN), transport layer security (TLS) VPN, etc.
- The cryptographic algorithm used should not be affected by known attacks or vulnerabilities.

IV.8 Communication security dimension for module 1

The communication security dimension ensures that information flows only between authorized end points. The following should be ensured:

- IPSec tunnel employing AES128, AES192, and AES256 encryption algorithms between SGSN and GGSN is provided.
- Secure data transmission is provided through the established IPSec tunnel between SGSN and GGSN.

Bibliography

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

[b-ITU-T X.813] Recommendation ITU-T X.813 (1996), *Information technology – Open Systems Interconnection – Security frameworks for open systens: Non-repudiation framework*.

[b-ITU-T X.814] Recommendation ITU-T X.814 (1995), *Information technology – Open Systems Interconnection – Security frameworks for open systens: Confidentiality framework.*

[b-ITU-T X.1051] Recommendation ITU-T X.1051 (2016), *Information technology – Security techniques – Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations.*

[b-ITU-T X.1158] Recommendation ITU-T X.1158 (2014), *Multi-factor authentication mechanisms using a mobile device.*

[b-ITU-T X.1254] Recommendation ITU-T X.1254 (2012), *Entity authentication assurance framework.*

[b-ISO/IEC 27000] ISO/IEC 27000:2014, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.

[b-ISO/IEC 27033-1] ISO/IEC 27033-1:2015, *Information technology – Security techniques – Network security – Part 1: Overview and concepts*.

[b-ISO/IEC 27039] ISO/IEC 27039:2015, *Information technology – Security techniques – Selection, deployment and operations of intrusion detection and prevention systems (IDPS)*.

[b-ISO/IEC 29100] ISO/IEC 29100:2011, *Information technology – Security techniques – Privacy framework.*

[b-NIST SP 800-53] NIST Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations.*

[b-SECU] Secustar, *Criteria for information security readiness assessment*, Korea, October 2014.
(http://www.kfict.or.kr/board/index.html?board_id=business2&action=view&page=2&seq=13150)

[b-Wi-Fi] Wi-Fi Alliance
(https://www.wi-fi.org/ko)

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	Environment and ICTs, climate change, e-waste, energy efficiency; 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	Terminals and subjective and objective assessment methods
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, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2017