INTERNATIONAL STANDARD

ISO/IEC 27033-1

First edition
2009-12-15

Information technology — Security techniques — Network security —

Part 1: Overview and concepts

Technologies de l'information — Techniques de sécurité — Sécurité de réseau —

Partie 1: Vue d'ensemble et concepts

Reference number
ISO/IEC 27033-1:2009(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 27033-1 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This first edition of ISO/IEC 27033-1 cancels and replaces ISO/IEC 18028-1:2006.

ISO/IEC 27033 consists of the following parts, under the general title *Information technology — Security techniques — IT network security*:

— *Part 1: Guidelines for network security*

The following parts are under preparation:

— *Part 2: Guidelines for the design and implementation of network security*

— *Part 3: Reference networking scenarios — Risks, design techniques and control issues*

Risks, design techniques and control issues for

— securing communications between networks using security gateways,

— securing virtual private networks,

— IP convergence, and

— wireless networks

will form the subject of future parts.

Introduction

In today's world, the majority of both commercial and government organizations have their information systems connected by networks (see Figure 1), with the network connections being one or more of the following:

— within the organization,

— between different organizations,

— between the organization and the general public.

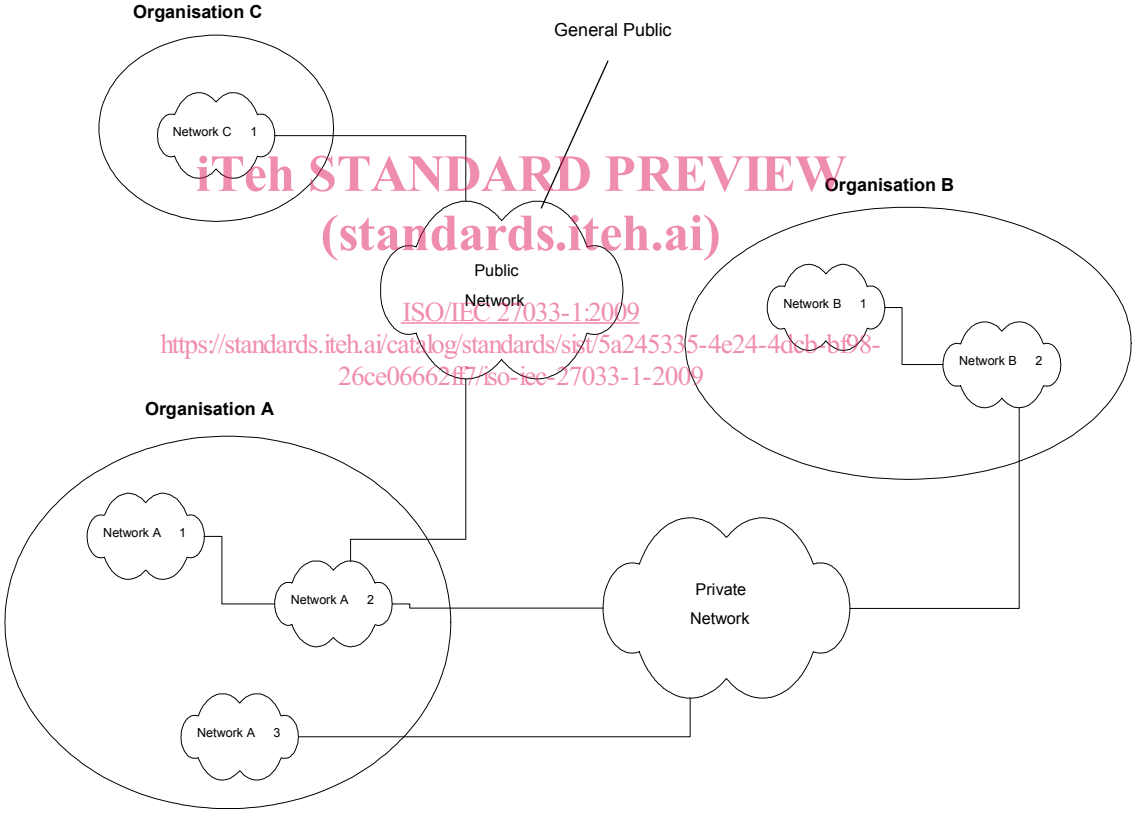

Figure 1 — Broad types of network connection

Further, with the rapid developments in publicly available network technology (in particular with the Internet) offering significant business opportunities, organizations are increasingly conducting electronic business on a global scale and providing online public services. The opportunities include the provision of lower cost data communications, using the Internet simply as a global connection medium, through to more sophisticated services provided by Internet service providers (ISPs). This can mean the use of relatively low cost local attachment points at each end of a circuit to full scale online electronic trading and service delivery systems, using web-based applications and services. Additionally, the new technology (including the integration of data,

voice and video) increases the opportunities for remote working (also known as “teleworking” or “telecommuting”) that enable personnel to operate away from their home work base for significant periods of time. They are able to keep in contact through the use of remote facilities to access organization and community networks and related business support information and services.

However, whilst this environment does facilitate significant business benefits, there are new security risks to be managed. With organizations relying heavily on the use of information and associated networks to conduct their business, the loss of confidentiality, integrity, and availability of information and services could have significant adverse impacts on business operations. Thus, there is a major requirement to properly protect networks and their related information systems and information. In other words: *implementing and maintaining adequate network security is absolutely critical to the success of any organization’s business operations.*

In this context, the telecommunications and information technology industries are seeking cost-effective comprehensive security solutions, aimed at protecting networks against malicious attacks and inadvertent incorrect actions, and meeting the business requirements for confidentiality, integrity, and availability of information and services. Securing a network is also essential for maintaining the accuracy of billing or usage information as appropriate. Security capabilities in products are crucial to overall network security (including applications and services). However, as more products are combined to provide total solutions, the interoperability, or the lack thereof, will define the success of the solution. Security must not only be a thread of concern for each product or service, but must be developed in a manner that promotes the interweaving of security capabilities in the overall security solution.

The purpose of ISO/IEC 27033 is to provide detailed guidance on the security aspects of the management, operation and use of information system networks, and their inter-connections. Those individuals within an organization that are responsible for information security in general, and network security in particular, should be able to adapt the material in this International Standard to meet their specific requirements. Its main objectives are as follows.

— ISO/IEC 27033-1, *Overview and concepts,* to define and describe the concepts associated with, and provide management guidance on, network security. This includes the provision of an overview of network security and related definitions, and guidance on how to identify and analyze network security risks and then define network security requirements. It also introduces how to achieve good quality technical security architectures, and the risk, design and control aspects associated with typical network scenarios and network “technology” areas (which are dealt with in detail in subsequent parts of ISO/IEC 27033).

— ISO/IEC 27033-2, *Guidelines for the design and implementation of network security,* to define how organizations should achieve quality network technical security architectures, designs and implementations that will ensure network security appropriate to their business environments, using a consistent approach to the planning, design and implementation of network security, as relevant, aided by the use of models/frameworks (in this context, a model/framework is used to outline a representation or description showing the structure and high level workings of a type of technical security architecture/design), and is relevant to all personnel who are involved in the planning, design and implementation of the architectural aspects of network security (for example network architects and designers, network managers, and network security officers).

— ISO/IEC 27033-3, *Risks, design techniques and control issues for reference network scenarios*, to define the specific risks, design techniques and control issues associated with typical network scenarios. It is relevant to all personnel who are involved in the planning, design and implementation of the architectural aspects of network security (for example network architects and designers, network managers, and network security officers).

It is proposed that future parts of ISO/IEC 27033 will address the following topics.

— ISO/IEC 27033-4, *Risks, design techniques and control issues for securing communications between networks using security gateways*, to define the specific risks, design techniques and control issues for securing information flows between networks using security gateways. It will be relevant to all personnel who are involved in the detailed planning, design and implementation of security gateways (for example network architects and designers, network managers, and network security officers).

— SO/IEC 27033-5, *Risks, design techniques and control issues for securing virtual private networks,* to define the specific risks, design techniques and control issues for securing connections that are established using virtual private networks (VPNs). It will be relevant to all personnel who are involved in the detailed planning, design and implementation of VPN security (for example network architects and designers, network managers, and network security officers).

— ISO/IEC 27033-6, *IP convergence*, to define the specific risks, design techniques and control issues for securing IP convergence networks, i.e. those with the convergence of data, voice and video. It will be relevant to all personnel who are involved in the detailed planning, design and implementation of security for IP convergence networks (for example network architects and designers, network managers, and network security officers).

— ISO/IEC 27033-7, *Wireless*, to define the specific risks, design techniques and control issues for securing wireless and radio networks. It will be relevant to all personnel who are involved in the detailed planning, design and implementation of security for wireless and radio networks (for example network architects and designers, network managers, and network security officers).

It is emphasized that ISOI/IEC 27033 provides further detailed implementation guidance on the network security controls that are described at a basic standardized level in ISO/IEC 27002.

If there are other parts in the future, these will be relevant to all personnel who are involved in the detailed planning, design and implementation of the network aspects covered by those parts (for example network architects and designers, network managers, and network security officers).

It should be noted that this International Standard is not a reference or normative document for regulatory and legislative security requirements. Although it emphasizes the importance of these influences, it cannot state them specifically, since they are dependent on the country, the type of business, etc.

Unless otherwise stated, throughout this part of ISO/IEC 27033 the guidance referenced is applicable to current and/or planned networks, but will only be referenced as “networks” or “the network”.

Information technology — Security techniques — Network security —

Part 1: Overview and concepts

1 Scope

This part of ISO/IEC 27033 provides an overview of network security and related definitions. It defines and describes the concepts associated with, and provides management guidance on, network security. (Network security applies to the security of devices, security of management activities related to the devices, applications/services, and end-users, in addition to security of the information being transferred across the communication links.)

It is relevant to anyone involved in owning, operating or using a network. This includes senior managers and other non-technical managers or users, in addition to managers and administrators who have specific responsibilities for information security and/or network security, network operation, or who are responsible for an organization's overall security program and security policy development. It is also relevant to anyone involved in the planning, design and implementation of the architectural aspects of network security.

This part of ISO/IEC 27033 also

— provides guidance on how to identify and analyse network security risks and the definition of network security requirements based on that analysis,

— provides an overview of the controls that support network technical security architectures and related technical controls, as well as those non-technical controls and technical controls that are applicable not just to networks,

— introduces how to achieve good quality network technical security architectures, and the risk, design and control aspects associated with typical network scenarios and network "technology" areas (which are dealt with in detail in subsequent parts of ISO/IEC 27033), and

— briefly addresses the issues associated with implementing and operating network security controls, and the on-going monitoring and reviewing of their implementation.

Overall, it provides an overview of the ISO/IEC 27033 series and a "road map" to all other parts.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 7498 (all parts), *Information technology — Open Systems Interconnection — Basic Reference Model*

ISO/IEC 27000:2009, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 27001:2005, *Information technology — Security techniques — Information security management systems — Requirements*

ISO/IEC 27002:2005, *Information technology — Security techniques — Code of practice for information security management*

ISO/IEC 27005:2008, *Information technology — Security techniques — Information security risk management*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 7498, ISO/IEC 27000, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005 and the following apply.

NOTE The following terms and definitions will also apply to future parts of ISO/IEC 27033.

3.1
alert
"instant" indication that an information system and network may be under attack, or in danger because of accident, failure or human error

3.2
architecture
fundamental organization of a system embodied in its components, their relationships to each other, and to the environment, and the principles guiding its design and evolution

[ISO/IEC 15288:2008, definition 4.5]

3.3
attacker
person deliberately exploiting vulnerabilities in technical and non-technical security controls in order to steal or compromise information systems and networks, or to compromise availability to legitimate users of information system and network resources

3.4
audit logging
recording of data on information security events for the purpose of review and analysis, and ongoing monitoring

3.5
audit tools
automated tools to aid the analysis of the contents of audit logs

3.6
certification authority
CA
authority trusted by one or more users to create and assign public-key certificates

NOTE 1 Optionally, the certification authority can create the users' keys.

NOTE 2 The role of the certification authority (CA) in this process is to guarantee that the individual granted the unique certificate is, in fact, who he or she claims to be. Usually, this means that the CA has an arrangement with an institution which provides it with information to confirm an individual's claimed identity. CAs are a critical component in information security and electronic commerce because they guarantee that the two parties exchanging information are really who they claim to be.

3.7
corporate information security policy
document that describes management direction and support for information security in accordance with business requirements and relevant laws and regulations

NOTE The document describes the high level information security requirements that have to be followed throughout the organization.

3.8
demilitarized zone
DMZ
perimeter network (also known as a screened sub-net) inserted as a “neutral zone” between networks

3.9
denial of service
DoS
prevention of authorized access to a system resource or the delaying of system operations and functions, with resultant loss of availability to authorized users

3.10
extranet
extension of an organization's Intranet, especially over the public network infrastructure, enabling resource sharing between the organization and other organizations and individuals that it deals with by providing limited access to its Intranet

NOTE For example, an organization's customers can be provided access to some part of its Intranet, creating an extranet, but the customers cannot be considered “trusted” from a security standpoint.

3.11
filtering
process of accepting or rejecting data flows through a network, according to specified criteria

3.12
firewall
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

3.13
hub
network device that functions at layer 1 of the OSI reference model

NOTE There is no real intelligence in network hubs; they only provide physical attachment points for networked systems or resources.

3.14
the Internet
global system of inter-connected networks in the public domain

3.15
internet
collection of interconnected networks called an internetwork or just *an* internet

3.16
intranet
private computer network that uses Internet protocols and network connectivity to securely share part of an organization's information or operations with its employees

3.17
intrusion
unauthorized access to a network or a network-connected system, i.e. deliberate or accidental unauthorized access to an information system, to include malicious activity against an information system, or unauthorized use of resources within an information system

3.18
intrusion detection
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 so as to include how and when it occurred

NOTE See ISO/IEC 18043.

3.19
intrusion detection system
IDS
technical system that is used to identify that an intrusion has been attempted, is occurring, or has occurred and possibly respond to intrusions in information systems and networks

NOTE See ISO/IEC 18043.

3.20
intrusion prevention
formal process of actively responding to prevent intrusions

3.21
intrusion prevention system
IPS
variant on intrusion detection systems that are specifically designed to provide an active response capability

NOTE See ISO/IEC 18043.

3.22
malware
malicious software designed specifically to damage or disrupt a system, attacking confidentiality, integrity and/or availability

NOTE Viruses and Trojan horses are examples of malware.

3.23
multi protocol label switching
MPLS
technique, developed for use in inter-network routing, whereby labels are assigned to individual data paths or flows, and used to switch connections, underneath and in addition to normal routing protocol mechanisms

NOTE Label switching can be used as one method of creating tunnels.

3.24
network administration
day-to-day operation and management of network processes, and assets using networks

3.25
network analyzer
device or software used to observe and analyze information flowing in networks

NOTE Prior to the information flow analysis, information should be gathered in a specific way such as by using a network sniffer.

3.26
network element
information system that is connected to a network

3.27
network management
process of planning, designing, implementing, operating, monitoring and maintaining a network

3.28
network monitoring
process of continuously observing and reviewing data recorded on network activity and operations, including audit logs and alerts, and related analysis

3.29
network security policy
set of statements, rules and practices that explain an organization's approach to the use of its network resources, and specify how its network infrastructure and services should be protected

3.30
network sniffer
device or software used to capture information flowing in networks

3.31
port
endpoint to a connection

NOTE In the context of the Internet protocol a port is a logical channel endpoint of a TCP or UDP connection. Application protocols which are based on TCP or UDP have typically assigned default port numbers, e.g. port 80 for HTTP.

3.32
remote access
process of accessing network resources from another network, or from a terminal device which is not permanently connected, physically or logically, to the network it is accessing

3.33
remote user
user at a site other than the one at which the network resources being used are located

3.34
router
network device that is used to establish and control the flow of data between different networks by selecting paths or routes based upon routing protocol mechanisms and algorithms

NOTE 1 The networks can themselves be based on different protocols.

NOTE 2 The routing information is kept in a routing table.

3.35
security domain
set of assets and resources subject to a common security policy

3.36
security gateway
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

3.37
spam
unsolicited e-mails, which can carry malicious contents and/or scam messages.

3.38
spoofing
impersonating a legitimate resource or user

3.39
switch
device which provides connectivity between networked devices by means of internal switching mechanisms, with the switching technology typically implemented at layer 2 or layer 3 of the OSI reference model

NOTE Switches are distinct from other local area network interconnection devices (e.g. a hub) as the technology used in switches sets up connections on a point to point basis.

3.40
tunnel
data path between networked devices which is established across an existing network infrastructure

NOTE Tunnels can be established using techniques such as protocol encapsulation, label switching, or virtual circuits.

3.41
virtual local area network
independent network created from a logical point of view within a physical network

4 Abbreviated terms

NOTE The following abbreviated terms are used in all parts of ISO/IEC 27033.

AAA	authentication, authorization and accounting
ACL	access control list
ADSL	asymmetric digital subscriber line
AES	advanced encryption standard
ATM	asynchronous transfer mode
BPL	broadband power line
CA	certification authority
CDPD	cellular digital packet data
CDMA	code division multiple access

CLID	calling line identifier
CLNP	connectionless network protocol
CoS	class of service
CRM	customer relationship management
DEL	direct exchange line
DES	data encryption standard
DMZ	demilitarized zone
DNS	domain name service
DPNSS	digital private network signaling system
DoS	denial of service
DSL	digital subscriber line
EDGE	enhanced data-rates for GSM evolution
EDI	electronic data interchange
EGPRS	enhanced general packet radio service
EIS	enterprise information system
FiOS	fiber optic service
FTP	file transfer protocol
FTTH	fiber to the home
GPRS	general packet radio service
GSM	global system for mobile communications
HIDS	host based intrusion detection system
HTTP	hypertext transfer protocol
IDS	intrusion detection system
IG	Implementation Guidance
IP	Internet protocol
IPS	intrusion prevention system
ISP	Internet service provider
IT	information technology
LAN	local area network
MPLS	multi-protocol label switching