INTERNATIONAL STANDARD

ISO/IEC 18028-1

First edition
2006-07-01

Information technology — Security techniques — IT network security —

Part 1: Network security management

Technologies de l'information — Techniques de sécurité — Sécurité de réseaux TI —

Partie 1: Gestion de sécurité de réseau

Reference number
ISO/IEC 18028-1:2006(E)

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but should not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

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

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 should not be held responsible for identifying any or all such patent rights.

ISO/IEC 18028-1 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

ISO/IEC 18028 consists of the following parts, under the general title *Information technology — Security techniques — IT network security*:

- *Part 1: Network security management*
- *Part 2: Network security architecture*
- *Part 3: Securing communications between networks using security gateways*
- *Part 4: Securing remote access*
- *Part 5: Securing communications across networks using virtual private networks*

Introduction

The telecommunications and information technology industries are seeking cost-effective comprehensive security solutions. A secure network should be protected against malicious and inadvertent attacks, and should meet the business requirements for confidentiality, integrity, availability, non-repudiation, accountability, authenticity and reliability 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 end-to-end security solution. Thus, the purpose of ISO/IEC 18028 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 standard to meet their specific requirements. Its main objectives are as follows:

— in ISO/IEC 18028-1, to define and describe the concepts associated with, and provide management guidance on, network security – including on how to identify and analyze the communications related factors to be taken into account to establish network security requirements, with an introduction to the possible control areas and the specific technical areas (dealt with in subsequent parts of ISO/IEC 18028);

— in ISO/IEC 18028-2, to define a standard security architecture, which describes a consistent framework to support the planning, design and implementation of network security;

— in ISO/IEC 18028-3, to define techniques for securing information flows between networks using security gateways;

— in ISO/IEC 18028-4, to define techniques for securing remote access;

— in ISO/IEC 18028-5, to define techniques for securing inter-network connections that are established using virtual private networks (VPNs).

ISO/IEC 18028-1 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.

ISO/IEC 18028-2 is relevant to all personnel who are involved in the planning, design and implementation of the architectural aspects of network security (for example network managers, administrators, engineers, and network security officers).

ISO/IEC 18028-3 is relevant to all personnel who are involved in the detailed planning, design and implementation of security gateways (for example network managers, administrators, engineers and network security officers).

ISO/IEC 18028-4 is relevant to all personnel who are involved in the detailed planning, design and implementation of remote access security (for example network managers, administrators, engineers, and network security officers).

ISO/IEC 18028-5 is relevant to all personnel who are involved in the detailed planning, design and implementation of VPN security (for example network managers, administrators, engineers, and network security officers).

Information technology — Security techniques — IT network security —

Part 1:
Network security management

1 Scope

ISO/IEC 18028-1 provides direction with respect to networks and communications, including on the security aspects of connecting information system networks themselves, and of connecting remote users to networks. It is aimed at those responsible for the management of information security in general, and network security in particular. This direction supports the identification and analysis of the communications related factors that should be taken into account to establish network security requirements, provides an introduction on how to identify appropriate control areas with respect to security associated with connections to communications networks, and provides an overview of the possible control areas including those technical design and implementation topics dealt with in detail in ISO/IEC 18028-2 to ISO/IEC 18028-5.

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 18028-2:2005, *Information technology — Security techniques — IT network security — Part 2: Network security architecture*

ISO/IEC 18028-3:2005, *Information technology — Security techniques — IT network security — Part 3: Securing communications between networks using security gateways*

ISO/IEC 18028-4:2005, *Information technology — Security techniques — IT network security — Part 4: Securing remote access*

ISO/IEC 18028-5:2006, *Information technology — Security techniques — IT network security — Part 5: Securing communications across networks using virtual private networks*

ISO/IEC 13335-1:2004, *Information technology — Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management*

ISO/IEC 17799:2005, *Information technology — Security techniques — Code of practice for information security management*

ISO/IEC 18044:2004, *Information technology — Security techniques — Information security incident management*

ISO/IEC 18043:2006, *Information technology — Security techniques — Selection, deployment and operations of intrusion detection systems*

3 Terms and definitions

3.1 Terms defined in other International Standards

For the purposes of this document, the terms and definitions given in ISO/IEC 7498 (all parts) and the following terms defined in ISO/IEC 17799 and ISO/IEC 13335-1 apply: accountability, asset, authenticity, availability, baseline controls, confidentiality, data integrity, impact, integrity, security policy, non-repudiation, reliability, risk, risk analysis, risk assessment, risk management, control, threat and vulnerability.

3.2 Terms defined in this part of ISO/IEC 18028

For the purposes of this document, the following terms and definitions apply.

3.2.1
alert
'instant' indication that an information system and network may be under attack, or in danger because of accident, failure or people error

3.2.2
attacker
any 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

3.2.3
audit
formal inquiry, formal examination, or verification of facts against expectations, for compliance and conformity

3.2.4
audit logging
gathering of data on information security events for the purpose of review and analysis, and ongoing monitoring

3.2.5
audit tools
automated tools to aid the analysis of the contents of audit logs

3.2.6
business continuity management
process to ensure that recovery of operations will be assured should any unexpected or unwanted incident occur that is capable of negatively impacting the continuity of essential business functions and supporting elements

NOTE The process should also ensure that recovery is achieved in the required priorities and timescales, and subsequently all business functions and supporting elements will be recovered back to normal. The key elements of this process need to ensure that the necessary plans and facilities are put in place, and tested, and that they encompass information, business processes, information systems and services, voice and data communications, people and physical facilities.

3.2.7
Comp128-1
proprietary algorithm that was initially used by default in SIM cards

3.2.8
demilitarized zone
DMZ
perimeter network (also known as a screened sub-net) inserted as a "neutral zone" between networks

NOTE It forms a security buffer zone.

3.2.9
denial of service
DoS
prevention of authorized access to a system resource or the delaying of system operations and functions

3.2.10
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

3.2.11
filtering
process of accepting or rejecting data flows through a network, according to specified criteria

3.2.12
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 to another, and vice versa, traverses and only authorized traffic, as defined by the local security policy, is allowed to pass

3.2.13
hub
network device that functions at layer 1 of the OSI reference model (ISO/IEC 7498-1)

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

3.2.14
information security event
identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of controls, or a previously unknown situation that may be security relevant

NOTE See ISO/IEC 18044.

3.2.15
information security incident
that indicated by a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security

NOTE See ISO/IEC 18044.

3.2.16
information security incident management
formal process of responding to and dealing with information security events and incidents

NOTE See ISO/IEC 18044.

3.2.17
internet
global system of inter-connected networks in the public domain

3.2.18
intranet
private network established internally in an organization

3.2.19
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

3.2.20
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 to include how and when it occurred

NOTE See ISO/IEC 18043.

3.2.21
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.

3.2.22
intrusion prevention system
IPS
variant on intrusion detection systems that are specifically designed to provide an active response capability

NOTE See ISO/IEC 18043.

3.2.23
jitter
one form of line distortion caused when a transmitted signal deviates from its reference

3.2.24
malware
malicious software, such as a virus or a trojan horse, designed specifically to damage or disrupt a system

3.2.25
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.

3.2.26
network administration
day-to-day operation and management of network processes and users

3.2.27
network analyzer
device used to capture and decode information flowing in networks

3.2.28
network element
information system that is connected to a network

NOTE The detailed description of security element is given in ISO/IEC 18028-2.

3.2.29
network management
process of planning, designing, implementing, operating, monitoring and maintaining a network

3.2.30
network monitoring
process of continuously observing and reviewing data recorded on network activity and operations, including audit logs and alerts, and related analysis

3.2.31
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

3.2.32
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 the HTTP protocol.

3.2.33
privacy
right of every individual that his/her private and family life, home and correspondence are treated in confidence

NOTE There should be no interference by an authority with the exercise of this right except where it is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, the protection of health or morals, or for the protection of the rights and freedoms of others.

3.2.34
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

3.2.35
remote user
user at a site other than the one at which the network resources being used are located

3.2.36
router
network device that is used to establish and control the flow of data between different networks, which themselves can be based on different network protocols, by selecting paths or routes based upon routing protocol mechanisms and algorithms. The routing information is kept in a routing table

3.2.37
security dimension
set of security controls designed to address a particular aspect of network security

NOTE The detailed description of security dimensions is given in ISO/IEC 18028-2.

3.2.38
security domain
set of assets and resources subject to a common security policy

3.2.39
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

NOTE The detailed description of security gateway is given in ISO/IEC 18028-3.

3.2.40
security layers
that which represents a hierarchy of network equipment and facility groupings protected by security dimensions

NOTE The detailed description of security layer is given in ISO/IEC 18028-2.

3.2.41
security plane
that which represents a certain type of network activity protected by security dimensions

NOTE The detailed description of security plane is given in ISO/IEC 18028-2.

3.2.42
spamming
sending of bulk unsolicited messages which on receipt cause adverse effects on the availability of information system resources

3.2.43
spoofing
impersonating a legitimate resource or user

3.2.44
switch
device which provides connectivity between networked devices by means of internal switching mechanisms

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. This ensures the network traffic is only seen by the addressed network devices and enables several connections to exist simultaneously. Switching technology can typically be implemented at layer 2 or layer 3 of the OSI reference model (ISO/IEC 7498-1).

3.2.45
tunnel
data path between networked devices which is established across an existing network infrastructure by using techniques such as protocol encapsulation, label switching, or virtual circuits

3.2.46
virtual private network
restricted-use logical computer network that is constructed from the system resources of a physical network, e.g. by using encryption and/or by tunneling links of the virtual network across the real network

4 Abbreviated terms

NOTE The following abbreviated terms are used in all parts of ISO/IEC 18028.

3G	Third Generation mobile telephone system
AAA	Authentication, Authorization and Accounting
ACL	Access Control List
ADSL	Asymmetric Digital Subscriber Line
AES	Advanced Encryption Standard
ATM	Asynchronous Transfer Mode
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
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
FTP	File Transfer Protocol
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
IP	Internet Protocol
ISP	Internet Service Provider
IT	Information Technology
LAN	Local Area Network
MPLS	Multi-Protocol Label Switching

MRP	Manufacturing Resource Planning
NAT	Network Address Translation
NIDS	Network Intrusion Detection System
NTP	Network Time Protocol
OOB	‘Out of Band’
PC	Personal Computer
PDA	Personal Data Assistant
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RAID	Redundant Array of Inexpensive Disks
RAS	Remote Access Service
RTP	Real Time Protocol
SDSL	Symmetric Digital Subscriber Line
SecOPs	Security Operating Procedures
SIM	Subscriber Identity Module
SNMP	Simple Network Management Protocol
SSH	Secure Shell
TCP	Transmission Control Protocol
TDMA	Time Division Multiple Access
Telnet	Terminal emulation program to work on-line on a remote computer
TETRA	TErrestial Trunked RAdio
TKIP	Temporal Key Integrity Protocol
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications System
UPS	Uninterruptible Power Supply
USB	Universal Serial Bus
VHF	Very High Frequency
VoIP	Voice over IP
VPN	Virtual Private Network
WAN	Wide Area Network
WAP	Wireless Application Protocol
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WORM	Write Once Read Many

5 Structure

The approach taken in ISO/IEC 18028-1 is to:

- first summarize the overall process for the identification and analysis of the communications related factors that should be taken into account to establish network security requirements, and
- then provide an indication of the potential control areas with respect to security associated with connections to and between communications networks. In doing this indicators are provided to where relevant content of ISO/IEC 13335 and ISO/IEC 17799 may be used, and technical design and implementation topics are introduced with references to where they are dealt with in detail in ISO/IEC 18028-2 to ISO/IEC 18028-5.

Three simple criteria are described to aid persons responsible for information security to identify potential control areas. These criteria identify the:

- different types of network connections,
- different networking characteristics and related trust relationships, and
- potential types of security risk associated with network connections (and the use of services provided via those connections).

The results of combining these criteria are then utilized to indicate potential control areas. Subsequently, summary descriptions are provided of the potential control areas, with indications to sources of more detail.

The areas dealt with are:

- Network Security Architecture, including coverage of:
  - local area networking,
  - wide area networking,
  - wireless networks,
  - radio networks,
  - broadband networking,
  - security gateways (see also ISO/IEC 18028-3),
  - remote access services (see also ISO/IEC 18028-4),
  - virtual private networks (see also ISO/IEC 18028-5),
  - IP convergence (data, voice and video),
  - enabling access to services provided by networks external (to the organization),
  - web hosting architectures,

  (See also ISO/IEC 18028-2 for more detail of Network Security Architecture.)
- Secure Service Management Framework,
- Network Security Management,