INTERNATIONAL STANDARD

ISO/IEC 18028-2

First edition
2006-02-01

Information technology — Security techniques — IT network security —

Part 2: Network security architecture

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

Partie 2: Architecture de sécurité de réseau

Reference number
ISO/IEC 18028-2:2006(E)

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 18028-2 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee 27, *IT Security techniques*, in collaboration with ITU-T. This part of ISO/IEC 18028 is technically aligned with ITU Rec. X.805 but is not published as identical text.

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 IT networks, and their inter-connections. Those individuals within an organization that are responsible for IT security in general, and IT network security in particular, should be able to adapt the material in ISO/IEC 18028 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 analyse 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 (VPN).

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 (IS) and/or network security, network operation, or who are responsible for an organization's overall security programme 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 IT network managers, administrators, engineers, and IT 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 IT network managers, administrators, engineers and IT 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 IT network managers, administrators, engineers, and IT 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 IT network managers, administrators, engineers, and IT network security officers).

Information technology — Security techniques — IT network security —

Part 2:
Network security architecture

1 Scope

This part of ISO/IEC 18028 defines a network security architecture for providing end-to-end network security. The architecture can be applied to various kinds of networks where end-to-end security is a concern and independently of the network's underlying technology. The objective of this part of ISO/IEC 18028 is to serve as a foundation for developing the detailed recommendations for the end-to-end network security.

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 7498-2:1989, *Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture*

CCITT Recommendation X.800 (1991), *Security architecture for Open Systems — Interconnection for CCITT applications*

3 Terms and definitions

For the purposes of this document, the following terms defined in ISO 7498-2:1989 | CCIT Rec. X.800 apply.

3.1
access control
prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner

3.2
data origin authentication
corroboration that the source of data received is as claimed

3.3
peer-entity authentication
corroboration that a peer entity in an association is the one claimed

3.4
availability
property of being accessible and useable upon demand by an authorized entity

3.5
confidentiality
property that information is not made available or disclosed to unauthorized individuals, entities, or processes

3.6
data integrity
property that data has not been altered or destroyed in an unauthorized manner

3.7
non-repudiation with proof of origin
security service in which the recipient of data is provided with proof of the origin of data

NOTE 1 This will protect against any attempt by the sender to falsely deny sending the data or its contents.

NOTE 2 Adapted from ISO 7498-2 | CCIT Rec. X.800.

3.8
non-repudiation with proof of delivery
security service in which the sender of data is provided with proof of delivery of data

NOTE 1 This will protect against any subsequent attempt by the recipient to falsely deny receiving the data or its contents.

NOTE 2 Adapted from ISO 7498-2 | CCIT Rec. X.800.

3.9
privacy
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

4 Abbreviations

ASP	Application Service Provider
ATM	Asynchronous Transfer Mode
DHCP	Dynamic Host Configuration Protocol
DS-3	Digital Signal level 3
IPsec	IP Security protocol
MD5	Message Digest Version 5
OAM&P	Operations Administration Maintenance and Provisioning
OSI	Open Systems Interconnection
PSTN	Public Switched Telephone Network
PVC	Permanent Virtual Circuit
SHA-1	Secure Hash Algorithm
SIP	Session Initiation Protocol
SMTP	Simple Mail Transfer Protocol
SONET	Synchronous Optical Network

SS7	Signalling System #7
SSL	Secure Socket Layer (encryption and authentication protocol)
TLS	Transport Layer Security (encryption and authentication protocol)
VLAN	Virtual Local Area Network

5 Reference Architecture for network security

The Reference Architecture was created to address the global security challenges of Service Providers, enterprises, and consumers and is applicable to wireless, optical and wire-line voice, data and converged networks. In context of this document the word “reference” in conjuncture with the word “architecture” is used to convey that the specification presents an example of high-level security architecture that could serve as a base for designing more detailed security solutions for various networks. This Reference Architecture addresses security concerns for the management, control, and use of network infrastructure, services, and applications. The Reference Architecture provides a comprehensive, top-down, end-to-end perspective of network security and can be applied to network elements, services, and applications in order to predict, detect, and correct security vulnerabilities.

The Reference Architecture logically divides a complex set of end-to-end network security-related features into separate architectural components. This separation allows for a systematic approach to end-to-end security that can be used for planning of new security solutions as well as for assessing the security of the existing networks.

The Reference Architecture addresses the network security needs covering following essential questions:

1. What kind of information needs to be protected?
2. What are the security risks, and what kind of protection is needed to manage these risks?
3. What are the distinct types of network activities that need to be protected?
4. What are the distinct types of network equipment and facility groupings that need to be protected?

A risk assessment should be conducted to prioritize the protection requirements and help to determine the appropriate security measures for security architecture.

These questions are addressed by three architectural components – Security Dimensions, Security Planes and Security Layers.

The principles described by the multifaceted Reference Architecture can be applied to a wide variety of networks independent of the network's technology or location in the protocol stack.

The following sections describe in detail the architectural elements and their functions with respect to the major security threats.

6 Security Dimensions

Typically within a risk management process, appropriate security measures are identified to manage or mitigate assessed risks. The security dimensions introduce a grouping of security measures that are used to implement particular aspects of network security. The concept of security dimensions is not limited to networks, but is also usable in the context of application or end-user information. In addition, the Security Dimensions apply to Service Providers or enterprises offering security services to their customers. The Security Dimensions are: (1) Access Control, (2) Authentication, (3) Non-repudiation, (4) Data Confidentiality, (5) Communication Flow Security, (6) Data Integrity, (7) Availability, and (8) Privacy.

Properly designed and implemented Security Dimensions support security policy that is defined for a particular network and facilitate the rules set by the security management.

6.1 Access Control Security Dimension

The Access Control Security Dimension provides authorization for the use of the network resources. Access Control ensures that only authorized personnel or devices are allowed access to network elements, stored information, information flows, services and applications. For example, Role-Based Access Control (RBAC) provides different access levels to guarantee that individuals and devices can only gain access to and perform operations on network elements, stored information, and information flows for which they are authorized.

6.2 Authentication Security Dimension

The Authentication Security Dimension serves to confirm the identities or other authorizing attributes of communicating entities. Authentication ensures the validity of the claimed identities when used by authorization or Access Control of the entities participating in communication (e.g. person, device, service or application) and provides assurance that an entity is not attempting a masquerade or unauthorized replay of a previous communication. Authentication methods that employ techniques based on user identification and password pair, two-factor authentication (e.g. token), biometrics are among widely used methods.

6.3 Non-repudiation Security Dimension

The Non-repudiation Security Dimension provides technical 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). It helps to ensure the availability of evidence that can be presented to a third party as technical proof that some kind of event or action has taken place. Note, however, that non-repudiation provided by technical means does not lead to a necessary conclusion of law. Cryptographic methods are often used for providing non-repudiation.

6.4 Data Confidentiality Security Dimension

The Data Confidentiality Security Dimension protects data from unauthorized disclosure. Encryption is a method often used to ensure data confidentiality. Access control lists, and file permissions are methods that help to keep data confidential.

6.5 Communication Flow Security Dimension

The Communication Flow Security Dimension ensures that information flows only between the authorized end points (the information is not diverted or intercepted as it flows between these end points). Security mechanisms of Communication Flow Security Dimension do not protect against modification/corruption; this is a function of Data Integrity. MPLS tunnels, VLANs, and VPNs are examples of technologies that can provide communication flow security.

6.6 Data Integrity Security Dimension

The Data Integrity Security Dimension ensures the correctness or accuracy (i.e., data are only processed by authorized processes or actions of authorized people or devices) of data. The data is protected against unauthorized modification, deletion, creation, and replication and provides an indication of these unauthorized activities. Hashed Message Authentication Code methods (e.g. MD5, SHA-1) often used for ensuring data integrity.

6.7 Availability Security Dimension

The Availability Security Dimension 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. Disaster recovery solutions are included in this category.

6.8 Privacy Security Dimension

The Privacy Security Dimension provides for the protection of any information (identity of a party to communications or any data – including packet headers – pertaining to any activity carried by this party) that might be derived from the observation of network activities. Examples of this information include web-sites that a user has visited, a user's geographic location, and the IP addresses and DNS names of devices in a Service Provider network. Network Address Translation (NAT) and application proxies are examples of the techniques that can be used for privacy protection. Depending on the respective national privacy and data protection legislations and regulations, this Privacy Security Dimension should also provide the appropriate protection structure and controls for collection, processing and dissemination of personal information.

7 Security Layers

In order to provide an end-to-end security solution, the Security Dimensions described in the previous section must be applied to a hierarchy of network equipment and facility groupings, which are referred to as Security Layers. This Reference Architecture defines three Security Layers – the Infrastructure Security Layer, the Services Security Layer, and the Applications Security Layer, which build on one another to provide network-based solutions.

The Security Layers are a series of enablers for secure network solutions: the Infrastructure Security Layer enables the Services Security Layer and the Services Security Layer enables the Applications Security Layer. The Reference Architecture addresses the fact that each layer has different security vulnerabilities and offers the flexibility of countering the potential threats in a way most suited for a particular security layer. The decision of whether the higher levels must assume that lower level security has functioned as intended or whether they should contain processes to detect failures is left to implementations.

It should be noted that Security Layers (as defined above) have different than the OSI layers meaning.

The Security Layers identify where security must be addressed in products and solutions by providing a sequential perspective of network security. For example, first security vulnerabilities are addressed for the Infrastructure Security Layer, then for the Services Security Layer, and finally security vulnerabilities are addressed for the Applications Security Layer. Security Dimensions identify areas that need to be addressed in each Security Layer. Figure 1 depicts how the mechanisms within each Security Dimension are applied to Security Layers in order to diminish vulnerabilities that exist at each layer and thus mitigate security attacks.

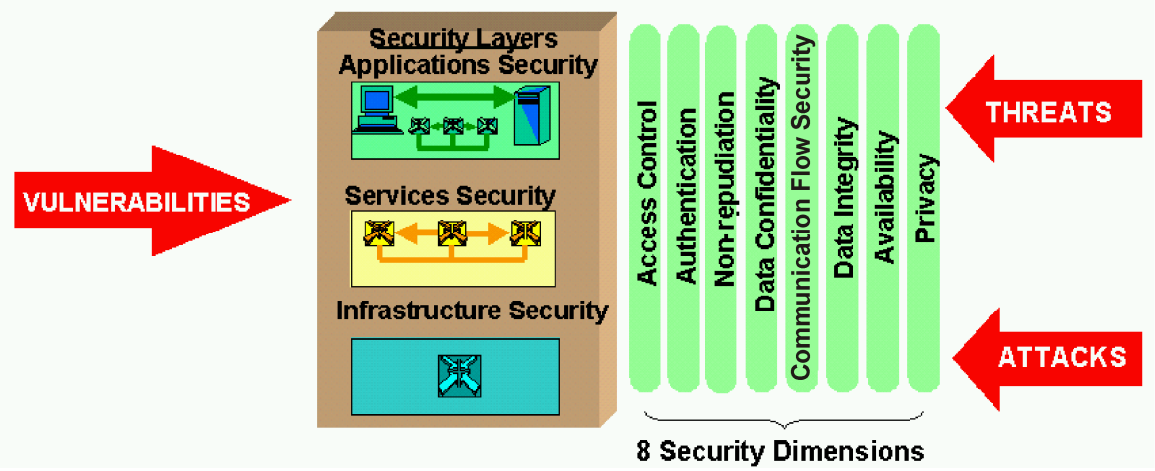

Figure 1 — Applying Security Dimensions to Security Layers