INTERNATIONAL STANDARD

ISO/IEC 18028-3

First edition
2005-12-15

Information technology — Security techniques — IT network security —

Part 3: Securing communications between networks using security gateways

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

Partie 3: Communications de sécurité entre réseaux utilisant des portails de sécurité

Reference number
ISO/IEC 18028-3:2005(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 18028-3 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 2: Network security architecture*

— *Part 3*: *Securing communications between networks using security gateways*

— *Part 4: Securing remote access*

The following parts are under preparation:

— *Part 1: Network security management*

— *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 3:
Securing communications between networks using security gateways

1 Scope

This part of ISO/IEC 18028 provides an overview of different techniques of security gateways, of components and of different types of security gateway architectures. It also provides guidelines for selection and configuration of security gateways.

Although Personal Firewalls make use of similar techniques, they are outside the scope of this part of ISO/IEC 18028 because they do not serve as security gateways.

The intended audiences for this part of ISO/IEC 18028 are technical and managerial personnel, e.g. IT managers, system administrators, network administrators and IT security personnel. It provides guidance in helping the user choose the right type of architecture for a security gateway which best meets their security requirements.

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

3 Terms and definitions

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

3.1
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
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