INTERNATIONAL STANDARD

ISO/IEC 27033-3

First edition
2010-12-15

Information technology — Security techniques — Network security —

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

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

Partie 3: Scénarios de réseautage de référence — Menaces, techniques conceptuelles et questions de contrôle

Reference number
ISO/IEC 27033-3:2010(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 shall 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

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 27033-3 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

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

— *Part 1: Overview and concepts*

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

— *Part 3: Reference network scenarios — Threats, design techniques and control issues*

The following parts are under preparation:

— *Part 4: Securing communications between networks using security gateways — Threats, design techniques and control issues*

— *Part 5: Securing virtual private networks — Threats, design techniques and control issues*

There may be future parts to cover topics such as local area networks, wide area networks, wireless and radio networks, broadband networks, voice networks, Internet Protocol (IP) convergence (data, voice, video) networks, web host architectures, Internet email architectures (including outgoing online access to the Internet, and incoming access from the Internet), and routed access to third party organizations.

Information technology — Security techniques — Network security —

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

1 Scope

This part of ISO/IEC 27033 describes the threats, design techniques and control issues associated with reference network scenarios. For each scenario, it provides detailed guidance on the security threats and the security design techniques and controls required to mitigate the associated risks. Where relevant, it includes references to ISO/IEC 27033-4 to ISO/IEC 27033-6 to avoid duplicating the content of those documents.

The information in this part of ISO/IEC 27033 is for use when reviewing technical security architecture/design options and when selecting and documenting the preferred technical security architecture/design and related security controls, in accordance with ISO/IEC 27033-2. The particular information selected (together with information selected from ISO/IEC 27033-4 to ISO/IEC 27033-6) will depend on the characteristics of the network environment under review, i.e. the particular network scenario(s) and ‘technology’ topic(s) concerned.

Overall, this part of ISO/IEC 27033 will aid considerably the comprehensive definition and implementation of security for any organization's network environment.

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 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 27033-1, *Information technology — Security techniques — Network security — Part 1: Overview and concepts*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000, ISO/IEC 27033-1 and the following apply.

3.1
malware
malicious software
category of software that is designed with a malicious intent, containing features or capabilities that could potentially cause harm directly or indirectly to the user and/or the user's computer system

NOTE See ISO/IEC 27032.

3.2
opacity
protection of information that might be derived by observing network activities, such as deriving addresses of end-points in a voice-over-Internet-Protocol call

NOTE Opacity recognizes the need to protect actions in addition to information.

3.3
outsourcing
acquisition of services by an acquirer to perform activities required to support the acquirer's business functions

3.4
social engineering
act of manipulating people into performing actions or divulging confidential information

4 Abbreviated terms

AAA	Authentication, Authorization and Accounting
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service
DNSSEC	DNS SECurity extensions
DoS	Denial of Service
FTP	File Transfer Protocol
IDS	Intrusion Detection System
IP	Internet Protocol
IPsec	IP Security Protocol
OAM&P	Operations, Administration, Maintenance & Provisioning
OSI	Open Systems Interconnection
PDA	Personal Data Assistant
PSTN	Public Switched Telephone Network
QoS	Quality of Service
SIP	Session Initiation Protocol
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SSL	Secure Socket Layer (Encryption and authentication protocol)
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network

5 Structure

The structure of this part of ISO/IEC 27033 comprises:

- an overview of the approach to addressing security for each reference scenario listed in this part of ISO/IEC 27033 (clause 6);
- a clause for each reference scenario (clause 7-15), which describes
  - threats for the reference scenario,
  - a presentation of the security controls and techniques based on the approach in clause 6.

The scenarios in the document are ordered per the following framework where the objective is to evaluate a given scenario as a function of the:

- **type of user access**, whether the user is inside an enterprise, or the user is an employee who is accessing enterprise resources from outside, or the user is a consumer, vendor or business partner, and,
- **type of information resources accessed**, open, restricted or outsourced resources.

Thus, the framework helps present a consistent structure, and makes addition of new scenarios manageable, as well as justifies the need for the various scenarios presented in this part of ISO/IEC 27033.

Table 1 — Framework for Ordering Network Scenarios

		Users		
		Inside	**Employees from outside**	**Outside**
Accessed information resources	**Open**	- Internet access services for employees - Business to business services		- Business to customer services
	Restricted	- Enhanced collaboration services - Business to business services - Network segmentation - Networking support for home and small business offices	- Mobile communication - Networking support for travelling users	- Enhanced collaboration services - Business to business services - Business to customer services
	Outsourced	- Outsourced services		- Outsourced services