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

Thus, the order in which the scenarios are listed in this part of ISO/IEC 27033 is as follows:

- Internet access services for employees (clause 7);
- Business to business services (clause 8);
- Business to customer services (clause 9);
- Enhanced collaboration services (clause 10);
- Network segmentation (clause 11);
- Networking support for home and small business offices (clause 12);
- Mobile communication (clause 13);
- Networking support for travelling users (clause 14);
- Outsourced services (clause 15).

6 Overview

The guidance presented in this part of ISO/IEC 27033 for each of the identified reference network scenarios is based on the following approach.

- Review the background information and scope of the scenario.
- Describe the threats relevant to the scenario.
- Perform risk analysis on discovered vulnerabilities.
- Analyse the business impact of addressing the vulnerabilities.
- Determine the implementation recommendations for securing the network.

In order to address the security of any network, an approach that is systematic and provides an end-to-end evaluation is desirable. The complexity of such an analysis is a function of the nature and size of the network in scope. However, a consistent methodology is important to managing security, especially due to the evolving nature of technology.

The first consideration in a security assessment is the determination of assets that require protection. These can be largely categorized into infrastructure, services or application assets. However, an enterprise can chose to define their own categories, but the distinction is important because the exposure to threats and attacks is unique to each asset category or type. For instance, if a router is categorized an infrastructure asset, and Voice over IP as an end-user service, then a Denial of Service (DoS) attack requires a different consideration in each case . Specifically, the router requires protection against a flood of bogus packets on the router's physical port that can prevent or impede the transmission of legitimate traffic. Similarly, the VoIP service requires protection of the subscriber’s account/service information from deletion or corruption such that a legitimate user is not prevented from accessing the service.

Network security also entails protection of the various activities supported on the network, such as management activities; control/signaling messages; and end-user data (resident and in-transit). For example, a management GUI can be subject to disclosure as a result of unauthorized access (easy to guess administrator ID and password). The management traffic itself is subject to corruption due to forged OA&M commands with spoofed IP addresses of the operations systems, or disclosure by sniffing, or interruption due to a packet flood attack.

The approach of identifying assets and activities enables a modular and systematic consideration of threats. Each reference network scenario is examined against a known set of threats to ascertain which threats are applicable. Annex B provides a list of known industry threats. Although the list should not be viewed as exhaustive, it provides a starting point for any analysis. Once the threat profile for the network is derived, the vulnerabilities are analyzed to determine how the threats may be realized in the context of the specific asset under consideration. Such an analysis will help determine what mitigations are missing and what countermeasures need to be deployed to achieve the protection objectives. A countermeasure will reduce the likelihood of the threat being successful and/or reduces its impact. Risk analysis that analyzes the risk represented by discovered vulnerabilities. Business impact analysis consists of arriving at a business decision regarding how to address each vulnerability: remediate, accept risk, or transfer risk.

Designing countermeasures and implementing controls for protecting vulnerabilities against threats is part of any security assessment methodology. In accordance with the ISO/IEC 27000 series standard, the selection and implementation of relevant controls is critical to asset/information protection. The standard requires the preservation of confidentiality, integrity and availability of information, and specifically states that in addition, other properties such as authenticity, non-repudiation and reliability can also be involved.

The following is a set of security properties that is used in this part of ISO/IEC 27033 to develop mitigations and countermeasures in an objective manner. The rationalization for the need for each security property (in addition to confidentiality, integrity and availability) is described below.

- Confidentiality is concerned with protecting data from unauthorized disclosure.
- Integrity is concerned with maintaining the correctness or accuracy of data and protecting against unauthorized modification, deletion, creation, and replication.
- Availability is concerned with ensuring that there is no denial of authorized access to network elements, stored information, information flows, services, and applications.
- Access Control provides, through the use of authentication and authorization, control to enforce access to network devices and services, and ensures that only authorized personnel or devices are allowed access to network elements, stored information, information flows, services and applications. For example, in an IPTV deployment, one of the known security recommendations, disabling the debugging interface on subscriber set top boxes, is derived from a consideration of the access control property. A review of confidentiality, integrity or availability will not result in some other recommendations.
- Authentication is concerned with confirming or substantiating the claimed identity of a user or communicating parties when used by access control for authorization, and provides assurance that an entity is not attempting a masquerade or unauthorized replay of a previous communication. For instance, an individual may gain access to a network management system, but will need to be authenticated in order to update subscriber service records. Thus the ability to perform network management activities cannot be assured by simply addressing confidentiality, integrity, availability, or access control.

NOTE In Role-Based Access Control, authorization takes place by virtue of the user being assigned to a role. Access control then verifies the user has the role prior to granting access. Similarly, access control lists grant access to anything that satisfies the policy, so if you satisfy the policy requirements you are authorized access. The authentication and authorization functions are null in this case.

- Communication or Transport Security is concerned with ensuring that information only flows between authorized end-points without being diverted or intercepted.
- Non-repudiation in concerned with maintaining an audit trail, so that the origin of data or the cause of an event or action cannot be denied. Identifying the authorized person that performed an unauthorized action on protected data has nothing to do with the data's confidentiality, integrity, availability.
- Opacity is concerned with protecting information that might be derived from the observation of network activities. Opacity recognizes the need to protect actions in addition to information. Protecting information is addressed by confidentiality. Protecting the conversation in a phone call between Person A and Person B protects their confidentiality. Protecting the fact that Person A and Person B had a phone call ensures opacity.

In all the scenarios described in this part of ISO/IEC 27033, the above-stated security properties are reviewed as part of the security design technique and control phase. Table 2 below shows examples of network security mechanisms that can be implemented for security properties that are selected for mitigating the potential risk.

Table 2 — Example Network Security Techniques

Security Considerations	Security Mechanisms / Techniques
Access Control	Physical badge system, Access Control Lists (ACL), Separation of duties
Authentication	Simple log-in/password, Digital certificates, Digital Signatures, TLSv1.2, SSO, CHAP
Availability	Redundancy & back-up, Firewalls, IDS/IPS (for blocking DoS), Business continuity, Managed network & services with SLAs
Communication Security	IPsec / L2TP, Private Lines, Separate networks
Confidentiality	Encryption (3DES, AES), Access control lists, File permissions
Integrity	IPsec HMACs (e.g. SHA-256), Cyclic redundancy checks, Anti-Virus Software
Non-repudiation	Logs, Role based access control, Digital signatures
Opacity	Encryption of IP headers(for example: VPN with IPSec tunnel mode), NAT (for IPv4)

In this part of ISO/IEC 27033, the above considerations are inherent in the design and implementation discussed in the context of each reference network scenarios. Typically, an organization will select the relevant ISO/IEC 27002 controls to meet their business objectives, and the guidelines in this part of ISO/IEC 27033 are intended to provide the network level considerations required for the implementation of the chosen controls.

7 Internet access services for employees

7.1 Background

Organizations that need to provide Internet access services for their employees should consider this scenario so as to ensure access for clearly identified and authorized purposes, not general open access. Organizations need to be concerned about managing that access to avoid loss of network bandwidth and responsiveness as well as exposure to legal liability when employees have uncontrolled access to Internet services.

Controlling employee access to the Internet is a growing concern given the number of emerging Internet case laws. Thus an organization is responsible for establishing, monitoring and enforcing an unambiguous Internet Use Policy by evaluating the following scenarios, and providing relevant claims in the policy:

- Internet access is allowed for business reasons;
- if Internet access is also allowed in (limited) form for private purposes, which services are allowed to be used;
- if enhanced collaboration services are allowed;
- if employees are allowed to participate in chat channels, forums etc.

Even though often a written policy acts as a significant deterrent to unacceptable Internet usage, the organization is still subject to substantial information security risks. In the clauses below, the security threats and advice on security design techniques and controls to mitigate those risks are described for internal, and internal plus external, usage.

7.2 Security threats

Security threats related to Internet access services for employees are:

- Virus attacks and introduction of malware:
  - employees using the Internet are also a prime target for malware which may lead to, loss or corruption of information and loss of control of IT infrastructure, and a huge risk to an organization's network security;
  - user downloaded files or programs may contain malicious code. Given the ubiquity of applications such as instant messaging, peer-to-peer file sharing, and IP telephony, employees can inadvertently download and install a malicious application that can evade network defences using such techniques as port agility (jumping around among open ports) and encryption. In addition, peer-to-peer applications can be exploited to serve as covert channels for botnets;
  - vulnerabilities in web browsers or other web applications may be exploited by malware, and result in virus infections and installation of trojans. Once infected, availability can be severely impacted due to virus propagation activities leading to network overload. Trojans can enable unauthorized external access leading to confidentiality violations.
- Information leakage:
  - applications that allow upload of information to web-based servers, may lead to uncontrolled transfer of data from inside an organization to the Internet. If encrypted sessions are used (e.g. TLS) then even logging of such activity may not be possible. Similar security risks are introduced when unauthenticated portable code is executed on systems inside an organization.
- Unauthorized usage and access:
  - loss of control of infrastructure, systems and applications can result in fraud, denial of service, and abuse of facilities.
- Liability due to regulatory non-compliance:
  - legal liability due to non-compliance with legislation or regulatory obligations;
  - non-conformance with an organization's use policy can lead to regulatory non-compliance.
- Reducing network availability due to inadequate bandwidth or stability problems:
  - excessive use of high bandwidth services such as streaming media or peer to peer file sharing may lead to network overload.

7.3 Security design techniques and controls

Security design techniques and controls related to employee internet access services are discussed in Table 3.

For a given security risk, each security property is reviewed for applicability in reducing the risk, and then a corresponding technical implementation example is presented in the second column. For example, integrity, access control, and authentication are applicable for protecting against malicious code.

Table 3 — Security Controls for Employee Internet Access Scenario

Applicable Security Properties for Identified Threats	Implementation Design and Technologies
Virus attacks and Introduction of Malware	
• Integrity • Access Control • Authentication	• Only provide the business relevant internet services towards the employee. Use of blacklists for authorized services, so as to not allow chat channels or web mail services, or peer-to-peer networking protocols. • Use of antivirus software on the gateways to the Internet for scanning all traffic from and to the Internet. Scanning should include all network protocols authorized for use. Ensure that anti-virus updates are automatically installed or the user is alerted to the fact that updates are available. • Use of antivirus software on all client systems, especially those used for internet access by employees. • Scan files and all stored information for viruses and Trojans and other forms of malware. • Data/file integrity verification using algorithms such as hash/checksums, certificates. • Blocking pop-ups and web advertisements. • Routing of traffic used for Internet access services through a small number of controlled security gateways. • Active content authentication.
Information Leakage	
• Communication security • Integrity • Access Control	• Implementing Filters for mobile code on the gateways to the Internet. • Accept mobile code only from uncritical, white listed sites. • Accept only digital signed mobile code signed from approved Certification Authorities or from approved vendors, enable the respective configuration options on the client side, e.g. by actively manage and implement a white list of allowed code signing Certification Authorities.
Unauthorized Access and Usage	
• Access Control • Non-Repudiation	• Only provide the business relevant internet services towards the employee. Use of blacklists for unauthorized services, e.g. chat channels or web mail services. Implementation of filters for non authorized protocols, e.g. peer-to-peer networking protocols. • Restrict the use of services which easily enable the transfer of big amounts of data. • Ensure that proper logging and monitoring is in place for all services which allow the possibility to transfer data towards the Internet. • Clearly define authorized and unauthorized usage of internet access in a dedicated policy (see sample template in Annex A). • Ensure user awareness through adequate education and training. • Only provide the business relevant internet services towards the employee. Use of blacklists for unauthorized services, e.g. chat channels or web mail services. Implementation of filters for non authorized protocols, e.g. peer-to-peer networking protocols.
Liability due to Regulatory Non-Compliance	
• Non-Repudiation	• Usage logs, time stamps. • User awareness and training.