

STN	Informačné technológie Bezpečnostné metódy Sieťová bezpečnosť Časť 6: Zabezpečenie bezdrôtového IP sieťového prístupu	STN ISO/IEC 27033-6 97 4103
------------	--	---

Information technology
Security techniques
Network security
Part 6: Securing wireless IP network access

Technologies de l'information
Techniques de sécurité
Sécurité de réseau
Partie 6: Sécurisation de l'accès réseau IP sans fil

Informationstechnologie
Sicherheitstechniken
Netzwerksicherheit
Teil 6: Sicherung von drahtlosen IP-Netzwerkzugängen

Táto norma obsahuje anglickú verziu ISO/IEC 27033-6: 2016.

This standard includes the English version of ISO/IEC 27033-6: 2016.

132823

Úrad pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky, 2021

Slovenská technická norma a technická normalizačná informácia je chránená zákonom č. 60/2018 Z. z. o technickej normalizácii.

Anotácia

Táto časť ISO/IEC 27033 popisuje hrozby, bezpečnostné požiadavky, bezpečnostné opatrenia a techniky návrhu spojené s bezdrôtovými sieťami. Poskytuje návod na výber, implementáciu a monitorovanie technických opatrení potrebných na zabezpečenie bezpečnej komunikácie pomocou bezdrôtových sietí. Informácie v tejto časti ISO/IEC 27033 sú určené na použitie pri preskúmaní alebo výbere možností technickej bezpečnostnej architektúry/návrhu, ktoré zahŕňajú použitie bezdrôtovej siete v súlade s ISO/IEC 27033-2.

Celkovo ISO/IEC 27033-6 významne pomôže pri komplexnom vymedzení a implementácii zabezpečenia pre bezdrôtové sieťové prostredie akejkoľvek organizácie. Je zameraná na používateľov a realizátorov, ktorí sú zodpovední za implementáciu a údržbu technických opatrení potrebných na vytvorenie bezpečných bezdrôtových sietí.

Národný predhovor

Normatívne referenčné dokumenty

Nasledujúce dokumenty, celé alebo ich časti, sú v tomto dokumente normatívnymi odkazmi a sú nevyhnutné pri jeho používaní. Pri datovaných odkazoch sa použije len citované vydanie. Pri nedatovaných odkazoch sa použije najnovšie vydanie citovaného dokumentu (vrátane všetkých zmien).

POZNÁMKA 1. – Ak bola medzinárodná publikácia zmenená spoločnými modifikáciami, čo je indikované označením (mod), použije sa príslušná EN/HD.

POZNÁMKA 2. – Aktuálne informácie o platných a zrušených STN možno získať na webovej stránke www.unms.sk

ISO/IEC 27000 zavedená v STN EN ISO/IEC 27000 Informačné technológie. Bezpečnostné metódy. Systémy riadenia informačnej bezpečnosti. Prehľad a slovník (ISO/IEC 27000) (36 9789)

ISO/IEC 27033-1 dosiaľ nezavedená

ISO/IEC 27033-2 zavedená v STN ISO/IEC 27033-2 Informačné technológie. Bezpečnostné metódy. Sieťová bezpečnosť. Časť 2: Návod pre návrh a implementáciu sieťovej bezpečnosti (97 4103)

Vypracovanie normy

Spracovateľ: Úrad pre normalizáciu, metrológiu a skúšobníctvo SR, Bratislava

Technická komisia: TK 37 Informačné technológie

Contents

Page

Foreword	v
Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Abbreviated terms	3
5 Structure	5
6 Overview	5
7 Security threats	8
7.1 General	8
7.2 Unauthorized access	8
7.3 Packet sniffing	8
7.4 Rogue wireless access point	9
7.5 Denial of service attack	9
7.6 Bluejacking	10
7.7 Bluesnarfing	10
7.8 Adhoc networks	10
7.9 Other threats	10
8 Security requirements	10
8.1 General	10
8.2 Confidentiality	11
8.3 Integrity	11
8.4 Availability	11
8.5 Authentication	11
8.6 Authorization	12
8.7 Accountability (Non-repudiation)	12
9 Security controls	12
9.1 General	12
9.2 Encryption control and implementation	13
9.3 Integrity evaluation	14
9.4 Authentication	14
9.5 Access control	15
9.5.1 General	15
9.5.2 Permission control	16
9.5.3 Network-based control	16
9.6 Denial of service attack resilience	16
9.7 DMZ segregation via firewall protection	16
9.8 Vulnerability management through secure configurations and hardening of devices	16
9.9 Continuous monitoring of wireless networks	17
10 Security design techniques and considerations	17
10.1 General	17
10.2 Wi-Fi	18
10.2.1 General	18
10.2.2 User authentication	18
10.2.3 Confidentiality and integrity	19
10.2.4 Wireless Wi-Fi technologies	19
10.2.5 Other Wi-Fi Configurations	19
10.2.6 Access control — User equipment	19
10.2.7 Access control — Infrastructure access point	20
10.2.8 Availability	21

ISO/IEC 27033-6:2016(E)

10.2.9	Accountability	21
10.3	Mobile communication security design	21
10.4	Bluetooth.....	22
10.5	Other wireless technologies.....	23
Annex A (informative) Technical description of threats and countermeasures		24
Bibliography		26

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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: [Foreword - Supplementary information](#)

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *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 networking scenarios — Threats, design techniques and control issues*
- *Part 4: Securing communications between networks using security gateways*
- *Part 5: Securing communications across networks using virtual private networks (VPNs)*
- *Part 6: Securing wireless IP network access*

ISO/IEC 27033-6:2016(E)

Introduction

In today's world, the majority of both commercial and government organizations have their information systems connected by networks with the network connections being one or more of the following:

- within the organization;
- between different organizations;
- between the organization and the general public.

Further, with the rapid developments in publicly available network technology (in particular with the Internet) offering significant business opportunities, organizations are increasingly conducting electronic business on a global scale and providing online public services. The opportunities include the provision of lower cost data communications, using the Internet simply as a global connection medium, through to more sophisticated services provided by Internet service providers (ISPs). This can mean the use of relatively low cost local attachment points at each end of a circuit to full scale online electronic trading and service delivery systems, using web-based applications and services. Additionally, the new technology (including the integration of data, voice and video) increases the opportunities for remote working (also known as “teleworking” or “telecommuting”) that enable personnel to operate away from their homework base for significant periods of time. They are able to keep in contact through the use of remote facilities to access organization and community networks and related business support information and services.

However, while this environment does facilitate significant business benefits, there are new security risks to be managed. With organizations relying heavily on the use of information and associated networks to conduct their business, the loss of confidentiality, integrity, and availability of information and services could have significant adverse impacts on business operations. Thus, there is a major requirement to properly protect networks and their related information systems and information. In other words, *implementing and maintaining adequate network security is absolutely critical to the success of any organization's business operations.*

In this context, the telecommunications and information technology industries are seeking cost-effective comprehensive security solutions, aimed at protecting networks against malicious attacks and inadvertent incorrect actions, and meeting the business requirements for confidentiality, integrity, and availability 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 should not only be a thread of concern for each product or service, but should be developed in a manner that promotes the interweaving of security capabilities in the overall security solution.

The purpose of ISO/IEC 27033 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 document to meet their specific requirements. Its main objectives are as follows.

- ISO/IEC 27033-1 aims to define and describe the concepts associated with, and provide management guidance on, network security. This includes the provision of an overview of network security and related definitions, and guidance on how to identify and analyze network security risks and then define network security requirements. It also introduces how to achieve good quality technical security architectures, and the risk, design and control aspects associated with typical network scenarios and network – technology areas (which are dealt with in detail in subsequent parts of ISO/IEC 27033).
- ISO/IEC 27033-2 aims to define how organizations should achieve quality network technical security architectures, designs and implementations that will ensure network security appropriate to their

business environments, using a consistent approach to the planning, design and implementation of network security, as relevant, aided by the use of models/frameworks (in this context, a model/framework is used to outline a representation or description showing the structure and high level workings of a type of technical security architecture/design), and is relevant to all personnel who are involved in the planning, design and implementation of the architectural aspects of network security (for example, network architects and designers, network managers, and network security officers).

- ISO/IEC 27033-3 aims to define the specific risks, design techniques and control issues associated with typical network scenarios. It is relevant to all personnel who are involved in the planning, design and implementation of the architectural aspects of network security (for example, network architects and designers, network managers, and network security officers).
- ISO/IEC 27033-4 aims to define the specific risks, design techniques and control issues for securing information flows between networks using security gateways. It is relevant to all personnel who are involved in the detailed planning, design and implementation of security gateways (for example, network architects and designers, network managers, and network security officers).
- ISO/IEC 27033-5 aims to define the specific risks, design techniques and control issues for securing connections that are established using virtual private networks (VPNs). It is relevant to all personnel who are involved in the detailed planning, design and implementation of VPN security (for example, network architects and designers, network managers, and network security officers).
- ISO/IEC 27033-6 aims to define the specific risks, design techniques and control issues for securing IP wireless networks. It is relevant to all personnel who are involved in the detailed planning, design and implementation of security for wireless networks (for example, network architects and designers, network managers, and network security officers).

It is emphasized that ISO/IEC 27033 provides further detailed implementation guidance on the network security controls that are described at a basic standardized level in ISO/IEC 27002.

It should be noted that this part of ISO/IEC 27033 is not a reference or normative document for regulatory and legislative security requirements. Although it emphasizes the importance of these influences, it cannot state them specifically, since they are dependent on the country, the type of business, etc.

Unless otherwise stated, throughout this part of ISO/IEC 27033, the guidance referenced is applicable to current and/or planned networks, but will only be referenced as “networks” or “the network”.

Information technology — Security techniques — Network security —

Part 6: Securing wireless IP network access

1 Scope

This part of ISO/IEC 27033 describes the threats, security requirements, security control and design techniques associated with wireless networks. It provides guidelines for the selection, implementation and monitoring of the technical controls necessary to provide secure communications using wireless networks. The information in this part of ISO/IEC 27033 is intended to be used when reviewing or selecting technical security architecture/design options that involve the use of wireless network in accordance with ISO/IEC 27033-2.

Overall, ISO/IEC 27033-6 will aid considerably the comprehensive definition and implementation of security for any organization's wireless network environment. It is aimed at users and implementers who are responsible for the implementation and maintenance of the technical controls necessary to provide secure wireless networks.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. 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*

ISO/IEC 27033-2, *Information technology — Security techniques — Network security — Part 2: Guidelines for the design and implementation of network security*

koniec náhľadu – text ďalej pokračuje v platenej verzii STN