INFOTEHNOLOOGIA
Turbemeetodid
Infotehnoloogiavõrkude turve
Osa 1: Võrguturbe haldus

Information technology
Security techniques
IT network security
Part 1: Network security management

EESTI STANDARDIKESKUS
ESTONIAN CENTRE FOR STANDARDISATION

EESTI STANDARDI EESSÕNA

Käesolev Eesti standard EVS-ISO/IEC 18028-1:2007 "Infotehnoloogia. Turbemeetodid. Infotehnoloogiavõrkude turve. Osa 1: Võrguturbe haldus" sisaldab rahvusvahelise standardi ISO/IEC 18028-1:2006 "Information technology — Security techniques — IT network security — Part 1: Network security management" identset ingliskeelset teksti.

Standardi avaldamise korraldas Eesti Standardikeskus.

Standard EVS-ISO/IEC 18028-1:2007 on kinnitatud Eesti Standardikeskuse 07.12.2007 käskkirjaga ja jõustub sellekohase teate avaldamisel EVS Teataja 2008. aasta jaanuarikuu numbris.

Standard on kättesaadav Eesti Standardikeskusest.

NATIONAL FOREWORD

This Estonian Standard EVS-ISO/IEC 18028-1:2007 consists of the identical English text of the International Standard ISO/IEC 18028-1:2006 "Information technology — Security techniques — IT network security — Part 1: Network security management".

Estonian standard is published by the Estonian Centre for Standardisation.

This standard is ratified with the order of Estonian Centre for Standardisation dated 07.12.2007 and is endorsed with the notification published in the official bulletin of the Estonian national standardisation organisation.

The standard is available from Estonian Centre for Standardisation.

Käsitlusala

ISO/IEC 18028-1 annab suuniseid võrkude ja side kohta, hõlmates infosüsteemide võrkude endi ühendamise turvaaspekte ja kaugkasutajate võrkudesse ühendamise turvaaspekte. Ta on suunatud neile, kes vastutavad üldise infoturbe halduse ja eriti võrguturbe halduse eest. Need suunised aitavad piiritleda ja analüüsida sidega seotud tegureid, mida tuleks arvestada võrguturbe nõuete väljaselgitamiseks, tutvustab seda, kuidas tuvastada sidevõrguühendustega seotud turvalisuse seisukohalt sobivad turbealad, ning annab ülevaate võimalikest turbealadest, hõlmates neid tehnilise projekteerimise ja teostamise teemasid, mida detailselt käsitletakse ISO/IEC 18028 järgmistes osades.

ICS 35.040 Märgistikud ja informatsiooni kodeerimine

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 should not be held responsible for identifying any or all such patent rights.

ISO/IEC 18028-1 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 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 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 standard 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 analyze 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 (VPNs).

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

Information technology — Security techniques — IT network security —

Part 1: Network security management

1 Scope

ISO/IEC 18028-1 provides direction with respect to networks and communications, including on the security aspects of connecting information system networks themselves, and of connecting remote users to networks. It is aimed at those responsible for the management of information security in general, and network security in particular. This direction supports the identification and analysis of the communications related factors that should be taken into account to establish network security requirements, provides an introduction on how to identify appropriate control areas with respect to security associated with connections to communications networks, and provides an overview of the possible control areas including those technical design and implementation topics dealt with in detail in ISO/IEC 18028-2 to ISO/IEC 18028-5.

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 18028-2:2005, *Information technology — Security techniques — IT network security — Part 2: Network security architecture*

ISO/IEC 18028-3:2005, *Information technology — Security techniques — IT network security — Part 3: Securing communications between networks using security gateways*

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

ISO/IEC 18028-5:2006, *Information technology — Security techniques — IT network security — Part 5: Securing communications across networks using virtual private networks*

ISO/IEC 13335-1:2004, *Information technology — Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management*

ISO/IEC 17799:2005, *Information technology — Security techniques — Code of practice for information security management*

ISO/IEC 18044:2004, *Information technology — Security techniques — Information security incident management*

ISO/IEC 18043:2006, *Information technology — Security techniques — Selection, deployment and operations of intrusion detection systems*