INFOTEHNOLOOGIA
Turbemeetodid
Infotehnoloogiavõrkude turve
Osa 4: Kaugpöörduse turve

Information technology
Security techniques
IT network security
Part 4: Securing remote access

EESTI STANDARDIKESKUS
ESTONIAN CENTRE FOR STANDARDISATION

EESTI STANDARDI EESSÕNA

Käesolev Eesti standard EVS-ISO/IEC 18028-4:2007 "Infotehnoloogia. Turbemeetodid. Infotehnoloogiavõrkude turve. Osa 4: Kaugpöörduse turve" sisaldab rahvusvahelise standardi ISO/IEC 18028-4:2005 "Information technology — Security techniques — IT network security — Part 4: Securing remote access" identset ingliskeelset teksti.

Standardi avaldamise korraldas Eesti Standardikeskus.

Standard EVS-ISO/IEC 18028-4:2007 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 18028-4:2007 consists of the identical English text of the International Standard ISO/IEC 18028-4:2005 "Information technology — Security techniques — IT network security — Part 4: Securing remote access".

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 see osa annab juhiseid kaugpöörduse turvalise kasutamise kohta; kaugpöördus on meetod arvuti kaugühendamiseks avalike võrkude abil teise arvuti või võrguga ja ta mõjutab infotehnoloogia turvalisust. Ta tutvustab seejuures mitmesuguseid kaugpöörduse tüüpe, hõlmates ka kasutatavaid protokolle, käsitleb kaugpöördusega seotud autentimisküsimusi ning aitab kaugpöördust turvaliselt korraldada. Ta on mõeldud abistama võrguadministraatoreid ja tehnilist personali, kes plaanivad sedalaadi ühenduse kasutamist või kellel see on juba kasutusel, kuid kes vajavad nõu selle kohta, kuidas seda turvaliselt korraldada ja turvaliselt käitada.

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

ISO/IEC 18028-4 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*

Network security management and securing communications between networks using Virtual Private Networks will form the subjects of the future Parts 1 and 5, respectively.

Introduction

In Information Technology there is an ever increasing need to use networks within organizations and between organizations. Requirements have to be met to use networks securely.

The area of remote access to a network requires specific measures when IT security should be in place. This part of ISO/IEC 18028 provides guidance for accessing networks remotely – either for using email, file transfer or simply working remotely.

Information technology — Security techniques — IT network security —

Part 4:
Securing remote access

1 Scope

This part of ISO/IEC 18028 provides guidance for securely using remote access – a method to remotely connect a computer either to another computer or to a network using public networks and its implication for IT security. In this it introduces the different types of remote access including the protocols in use, discusses the authentication issues related to remote access and provides support when setting up remote access securely. It is intended to help network administrators and technicians who plan to make use of this kind of connection or who already have it in use and need advice on how to set it up securely and operate it securely.

2 Terms, definitions and abbreviated terms

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

2.1
Access Point
AP
the system providing access from a wireless network to a terrestrial network

2.2
Advanced Encryption Standard
AES
a symmetric encryption mechanism providing variable key length and allowing an efficient implementation specified as Federal Information Processing Standard (FIPS) 197

2.3
authentication
the provision of assurance of the claimed identity of an entity. In case of user authentication, users are identified either by knowledge (e.g., password), by possession (e.g., token) or by a personal characteristic (biometrics). Strong authentication is either based on strong mechanisms (e.g., biometrics) or makes use of at least two of these factors (so-called multi-factor authentication).

2.4
call-back
a mechanism to place a call to a pre-defined or proposed location (and address) after receiving valid ID parameters

2.5
Challenge-Handshake Authentication Protocol
CHAP
a three-way authentication protocol defined in RFC 1994