

INFOTEHNOLOOGIA
Turbemeetodid
Infotehnoloogiavõrkude turve
Osa 2: Võrguturbe arhitektuur
(ISO/IEC 18028-2:2006)

Information technology
Security techniques
IT network security
Part 2: Network security architecture
(ISO/IEC 18028-2:2006)

EESTI STANDARDI EESSÕNA

Käesolev Eesti standard on 2006. aastal ilmunud rahvusvahelise standardi ISO/IEC 18028-2 "Information technology – Security techniques – IT network security – Part 2: Network security architecture" tõlge eesti keelde.

Standard EVS-ISO/IEC 18028-2 on koostatud Majandus- ja Kommunikatsiooniministeeriumi tellimusel. Standardi tõlkis Cybernetica AS ja tõlke kiitis heaks EVS/TK 4 "Infotehnoloogia".

Rahvusvahelise standardi ISO/IEC 18028-2:2006 tekst on avaldatud Eesti standardina EVS-ISO/IEC 18028-2:2007, mis on kinnitatud Eesti Standardikeskuse 07.12.2007 käskkirjaga nr 200 ning jõustub selle kohta EVS Teataja 2008. aasta jaanuarikuu numbris teate avaldamisega.

This standard is the Estonian [et] version of the International standard ISO/IEC 18028-2:2006 "Information technology – Security techniques – IT network security – Part 2: Network security architecture". It has the same status as the official version.

In case of interpretation disputes the English text applies.

Standardite reprodutseerimis- ja levitamiseõigus kuulub Eesti Standardikeskusele

SISUKORD

EESSÕNA.....	4
SISSEJUHATUS	5
1 KÄSITLUSALA	7
2 NORMATIIVVIITED	7
3 TERMINID JA MÄÄRATLUSED	7
4 LÜHENDID	8
5 VÕRGUTURBE ETALONARHITEKTUUR.....	9
6 TURBEMÕÕTMED.....	10
6.1 Pääsu reguleerimise turbemõõde	10
6.2 Autentimise turbemõõde.....	10
6.3 Salgamise vääramise turbemõõde.....	10
6.4 Andmete konfidentsiaalsuse turbemõõde	11
6.5 Sidevoo turbemõõde	11
6.6 Andmetervikluse turbemõõde.....	11
6.7 Käideldavuse turbemõõde.....	11
6.8 Privaatsuse turbemõõde	11
7 TURBEKIHID	12
7.1 Infrastruktuuri turbekiht.....	12
7.2 Teenuste turbekiht.....	13
7.3 Rakenduste turbekiht	13
8 TURBETASANDID	13
8.1 Halduse turbetasand	14
8.2 Juhtimise turbetasand.....	14
8.3 Lõppkasutaja turbetasand.....	15
10 EESMÄRGID, MIS SAAVUTATAKSE TURBEMÕÕTMEID TURBEKIHTIDELE RAKENDADES	16
10.1 Infrastruktuuri turbekiht.....	18
10.2 Teenuste turbekiht.....	21
10.3 Rakenduste turbekiht	24
Kasutatud kirjandus	28

EESSÕNA

ISO (Rahvusvaheline Standardiorganisatsioon) ja IEC (Rahvusvaheline Elektrotehnikakomisjon) moodustavad ülemaailmse standardimise spetsialiseeritud süsteemi. ISO või IEC rahvuslikud liikmeskogud osalevad rahvusvaheliste standardite väljatöötamises tehniliste komiteede kaudu, mis on nendes organisatsioonides rajatud käsitlema tehnilise tegevuse eri valdkondi. ISO ja IEC tehnilised komiteed teevad koostööd mõlemale huvi pakkuvatel aladel. Selles töös osalevad käsikäes ISO ja IECga ka muud rahvusvahelised riiklikud ja mitteriiklikud organisatsioonid. Infotehnoloogia alal on ISO ja IEC loonud ühise tehnilise komitee ISO/IEC JTC 1.

Rahvusvahelised standardid kavandatakse vastavalt ISO/IEC direktiivide 2. osas esitatud reeglitele.

Ühise tehnilise komitee peamine ülesanne on koostada rahvusvahelisi standardeid. Ühises tehnilises komitees vastuvõetud rahvusvahelised standardikavandid saadetakse rahvuslikele kogudele hääletamiseks. Avaldamine rahvusvahelise standardina nõuab heakskiitu vähemalt 75 protsendilt hääletanud rahvuslikelt kogudelt.

Tuleb pöörata tähelepanu võimalusele, et mõned selle rahvusvahelise standardi elemendid võivad olla patendiõiguse objektiks. ISO ega IEC ei ole kohustatud mingeid või kõiki selliseid patendiõigusi välja selgitama.

Rahvusvahelise standardi ISO/IEC 18028-2 koostas ISO/IEC ühendatud tehniline komitee JTC 1 "Infotehnoloogia" alamkomitee SC 27, "Infoturbemeetodid" koostöös ITU sektoriga ITU-T. Käesolev ISO/IEC 18028 osa on tehniliselt kooskõlastatud dokumendiga ITU Rec. X.805, kuid ei ole sellega identne tekst.

ISO/IEC 18028, üldpealkirjaga "Infotehnoloogia. Turbemeetodid. Infotehnoloogia-võrkude turve", koosneb järgmistest osadest.

- Osa 1: Võrguturbe haldus
- Osa 2: Võrguturbe arhitektuur
- Osa 3: Võrkudevahelise side turve turvalüüside abil
- Osa 4: Kaugpöörduse turve
- Osa 5: Võrkudevahelise side turve virtuaalsete privaatvõrkude abil

SISSEJUHATUS

Side ja infotehnoloogia valdkonnad otsivad kõikehõlmavaid ökonoomseid turbelahendusi. Turvaline võrk peaks olema kaitstud rünnete eest, olgu need pahatahtlikud või ettekavatsematud, ning peaks vastama tööalastele nõuetele, mis puudutavad teabe ja teenuste konfidentsiaalsust, terviklust, käideldavust, salgamise vääramist, jälitatavust, autentsust ja stabiilsust. Võrgu turve on oluline ka arveldus- või kasutamisteabe õigsuse seisukohalt. Kogu võrgu (sealhulgas rakenduste ja teenuste) üldise turvalisuse saavutamiseks on olulised toodete turbevõimed. Kuna terviklahenduste saamiseks ühendatakse üha suurem arv tooteid, otsustab lahenduse õnnestumise nende koostalitlusvõime või selle puudumine. Turbele tuleb mitte ainult pöörata tähelepanu iga toote ja teenuse puhul, vaid teda tuleb arendada nii, et edendataks turbevõimete põimumist täieulatuslikus turbelahenduses tervikuna. Seetõttu on ISO/IEC 18028 eesmärk anda detailseid juhiseid infosüsteemide võrkude ja nende vaheliste ühenduste halduse, käigushoiu ja kasutamise turbeaspektide kohta. Need, kes organisatsioonis vastutavad üldise infoturbe eest ja eriti võrguturbe eest, peaksid suutma sobitada selles standardis olevat materjali oma konkreetsete vajadustega. Standardi peaeesmärgid on järgmised.

- ISO/IEC 18028-1: määratleda ja kirjeldada võrguturbega seotud mõisted ja anda juhiseid võrguturbe halduse kohta, sealhulgas selle kohta, kuidas piiritleda ja analüüsida sidega seotud tegureid, mida tuleb arvestada võrguturbe nõuete väljaselgitamiseks, ning tutvustada võimalikke turbealasid ja spetsiifilisi tehnilisi alasid (mida käsitlevad ISO/IEC 18028 järgmised osad);
- ISO/IEC 18028-2: määratleda standardne turbearhitektuur, mis kirjeldab üht kooskõlalist raamstruktuuri võrguturbe plaanimise, projekteerimise ja teostamise abistamiseks;
- ISO/IEC 18028-3: määratleda meetodid võrkudevaheliste infovoogude kaitsmiseks turvalüüside abil;
- ISO/IEC 18028-4: määratleda kaugpöörduse turbe meetodid;
- ISO/IEC 18028-5: määratleda meetodid võrkude vahel loodavate ühenduste kaitsmiseks virtuaalsete privaativõrkude (VPNide) abil.

ISO/IEC 18028-1 puudutab kõiki, kes on seotud võrgu omamise, käituse või kasutamisega. See hõlmab juhte ja haldureid, kellel on spetsiifilised kohustused infoturbe ja/või võrguturbe ja võrkude käituse alal või kes vastutavad organisatsiooni üldise turbekava ja turvapoliitika väljatöötamise eest, lisaks neile ka kõrgemaid juhte ja muid mittetehnilisi juhte või kasutajaid.

ISO/IEC 18028-2 puudutab kõiki neid töötajaid, kes osalevad võrguturbe arhitektuuri-aspektide plaanimises, projekteerimises ja teostamises (näiteks võrguhaldureid, administraatoreid, insenere ja võrguturbe ametnikke).

ISO/IEC 18028-3 puudutab kõiki neid töötajaid, kes osalevad turvalüüside detailses plaanimises, projekteerimises ja teostamises (näiteks võrguhaldureid, administraatoreid, insenere ja võrguturbe ametnikke).

ISO/IEC 18028-4 puudutab kõiki neid töötajaid, kes osalevad kaugpöörduse turbe detailses plaanimises, projekteerimises ja teostamises (näiteks võrguhaldureid, administraatoreid, insenere ja võrguturbe ametnikke).

ISO/IEC 18028-5 puudutab kõiki neid töötajaid, kes osalevad VPNi turbe detailses plaanimises, projekteerimises ja teostamises (näiteks võrguhaldureid, administraatoreid, insenere ja võrguturbe ametnikke).

INFOTEHNOLOOGIA

Turbemeetodid. Infotehnoloogiavõrkude turve

Osa 2: Võrguturbe arhitektuur

Information technology

Security techniques. IT network security

Part 2: Network security architecture

1 KÄSITLUSALA

ISO/IEC 18028 see osa määratleb võrguturbe arhitektuuri, millega tagada võrgu turvalisus otspunktist otspunktini. Seda arhitektuuri saab rakendada mitmesugust tüüpi võrkudes, kus probleemiks on turvalisus otspunktist otspunktini, ja sõltumatult võrgu aluseks olevast tehnoloogiast. ISO/IEC 18028 selle osa eesmärk on olla aluseks üksikasjalike soovitude väljatöötamisel otspunktide vahelise turbe kohta.

2 NORMATIIVVIITED

Alljärgnevas viidatud dokumendid on käesoleva dokumendi rakendamiseks möödapääsmatud. Dateeritud viidete puhul kehtib ainult siin viidatud redaktsioon. Dateerimata viidete puhul kehtib viidatud dokumendi uusim redaktsioon (koos võimalike muudatustega).

ISO 7498-2:1989 Infotöötlussüsteemid. Avatud süsteemide ühendamine. Etalonmudel. Osa 2: Turbearhitektuur

CCITT soovitus X.800 (1991) Avatud süsteemide turbe arhitektuur. CCITT rakenduste ühendamine.

3 TERMINID JA MÄÄRATLUSED

Käesoleva dokumendi otstarbeks kehtivad järgmised terminid, mis on määratletud dokumentides ISO 7498-2:1989 | CCIT Rec. X.800.

3.1

pääsu reguleerimine

ressursi lubamatu kasutamise vältimine, sealhulgas ressursi lubamatul viisil kasutamise vältimine

3.2

andmete allika autentimine

kinnituse saamine sellele, et vastuvõetud andmed pärinevad väidetavast allikast