

## Loeng 2 Sissejuhatus, mõisted, definiitsioonid, probleemid,

Erika Matsak, PhD

---

---

---

---

---

---

---

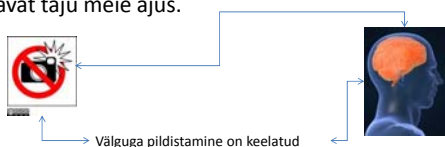
---

### Teadmised, andmed, informatsioon

Semiootikud:

Antud teooria raames teadmiste all vaadeldakse kolmikuid, mis koosnevad

- kujutisest (näiteks pilt, ikoon jne),
- selle tähendusest (näiteks tekstina),
- vastavat taju meie ajus.




---

---

---

---

---

---

---

---

### Teadmised, andmed, informatsioon

- P. Lorents (NATO Cooperative Cyber Defence Centre of Excellence): *“Teadmiseks nimetame iga niisugust järjestatud paari, mille esimese elemendi tähenduseks on teine element, teise elemendi tähenduseks on esimene element”.*



**Definiitsioon** (vt Lorents 2008). X on andmed, kui on mingis teadmises tähiseks või tähenduseks.

**Definiitsioon** (vt Lorents, Ottis, Rikk 2009). M on informatsioon, kui M on kas teadmine või andmed.

---

---

---

---

---

---

---

---

## Turvaprobleemide näited

- Firmal on mitu kontorit, mis paiknevad üksteisest kaugel. Konfidentsiaalse info edastamisel interneti kaudu peab olema kindel, et mitte keegi ei saa infot ei näha ega muuta.
- Võrgu administraator juhib serveri tööd olles väljastpoolt kontorit. Vastane napsab juhtkäsu, muudab seda ja saadab serverisse
- Kasutaja saab liigipääsu arvutisse mitteseaduslikult, või omades üht liigipääsu ühetele õigustega, saab liigipääsu veel mujale või suuremate õigustega.
- Firma avab interneti poe, mis võtab vastu makseid elektroonselt. Müüa peab olema kindel, et kaup, mille ta annab üle on ka tegelikult makstud. Ostja aga peab olema kindel, et saab selle kauba kätte ja seejuures mitte keegi ei saaks teada tema krediitkaardi andmeid.
- Firma avab internetis oma saidi. Mingil momendil asendatakse saidi sisu teise sisuga või tekib selline päringute koormus, et server ei tule sellega toime ning jookseb kinni.

---

---

---

---

---

---

---

---

---

---

## Mõned terminid

- **Andmete käideldavus** (availability) on teabe õigeaegne ning mugav kättesaadavus ning kasutatavus selleks volitatud isikutele ning subjektidele
- (Lorents 2010) **Info käideldavus** seisneb olukorras, mille raames peab saama vastava teadmise või eelmainitud teadmise moodustamist võimaldava tähise või tähenduse (ehk *andmete*) kasutamine ettenähtud viisil
- **Andmete terviklus** (integrity) on andmete pärinemine autentsest allikast ning veendumine, et need pole hiljem muutunud ja/või neid pole hiljem volitatamatult muudetud
- (Lorents 2010) **Info terviklus** seisneb olukorras, mille raames on vastaval teadmisel või eelmainitud teadmise moodustamist võimaldaval tähisel või tähendusel (ehk *andmetel*) või nendevahelisel seosel olemas kõik ettenähtud komponendid ning ettenähtud ülesehitus
- **Andmete konfidentsiaalsus** (confidentiality) ehk salastus on andmete kättesaadavus ainult selleks volitatud isikutele (ning kättesaamatus kõikidele ülejäänutele)
- (Lorents 2010) **Info konfidentsiaalsus** seisneb ühe süsteemi (edaspidi salastaja) loodud olukorras, mille sihiks on muuta teiste süsteemide jaoks võimatuks vastava teadmise (ehk *salastatud teadmise*) omandamine või muuta teiste süsteemide jaoks võimatuks eelmainitud teadmise moodustamist võimaldava tähise või tähenduse (ehk *salastatud andmete*) või nendevahelise seose omandamine

---

---

---

---

---

---

---

---

---

---

## Küberründed ning informatsiooni konfidentsiaalsus, terviklus ja käideldavus

- (Lorents, Ottis 2010) **Konfidentsiaalsuse vastu suunatud küberrünne** on säärane küberrünne, mille soovitud tagajärjeks on salastatuse kadu ehk olukord, kus mingi süsteem (nt konkureeriv firma) võib omandada teadmise, mida ei soovi selle teadmise salastaja
- (Lorents, Ottis 2010) **Tervikluse vastu suunatud küberrünne** on säärane küberrünne, mille soovitud tagajärjeks on teadmise või selles sisalduvate asjade (nt tähiste, tähenduste, nendevahelise seose vms) ettenähtud struktuuri (ehk kindlaksmääratud ülesehituse) rikkumine (näiteks "kustutakse" sihtmärgi koordinaatides mõned arvud, "lõigatakse" ettekandest välja teatavad tekstiosad)
- (Lorents, Ottis 2010) **Käideldavuse vastu suunatud küberrünne** on säärane küberrünne, mille soovitud tagajärjeks on teadmise või selles sisalduvate asjade (nt tähiste, tähenduste, nendevahelise seose vms) ettenähtud kasutamise võimatuks muutmine (näiteks sel teel, et "ummistatakse" infoedastuskanalid)

---

---

---

---

---

---

---

---

---

---

## Mõned terminid

- Nõrkused – süsteemi nõrgad kohad, turvaaukud, vms, mida kasutatakse rünneteks
- Risk – võimaliku kahju suuruse ning selle kahju tekke tõenäosuse korrutis (nt kui teostatakse konkreetne rünne konkreetsete turvaaukude kaudu). Iga organisatsioon peab enda jaoks selgitama välja "lubatavad" riskid.
- Turvameetmed – direktiivid, seadused, praktilised lahendused, mis reguleerivad kuidas väärtusi kasutatakse, kaitstakse, jagatakse infosüsteemide vahel; kriteeriumite kogum turvateenuste osutamiseks.
- Turvapoliitika on organisatsiooni infoturbetaevuse alusdokument.
- Rünne – iga tegevus, mille sihiks on kahjustada infosüsteemi turvalisust

---

---

---

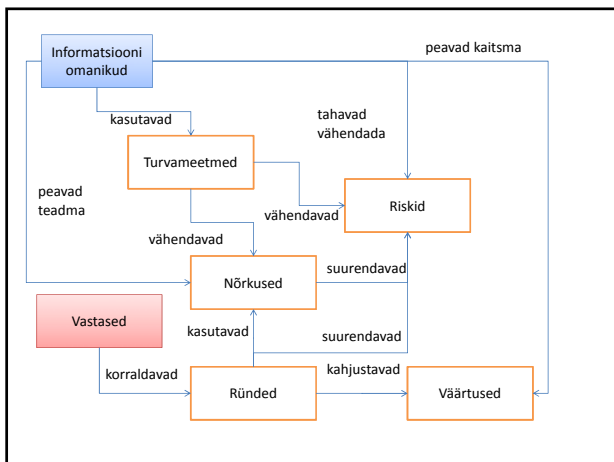
---

---

---

---

---




---

---

---

---

---

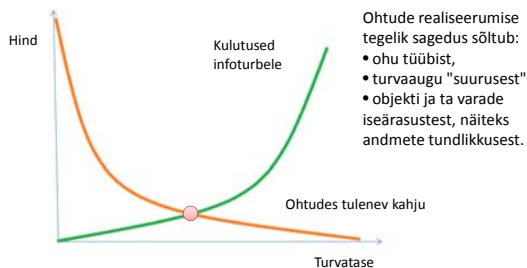
---

---

---

## Turvarisk

varade väärtus x ohtude realiseerumise tõenäosus




---

---

---

---

---

---

---

---



## EAL (Evaluation Assurance Level)

- EAL1: funktsionaalselt testitud
- EAL2: struktuurselt testitud
- EAL3: metoodiliselt testitud ja verifitseeritud
- EAL4: metoodiliselt disainitud, testitud ja üle vaadatud
- EAL5: poolformaalselt disainitud ja testitud
- EAL6: poolformaalselt verifitseeritud disain ja testitud
- EAL7: formaalselt verifitseeritud disain ja testitud

[http://en.wikipedia.org/wiki/Evaluation\\_Assurance\\_Level](http://en.wikipedia.org/wiki/Evaluation_Assurance_Level)

---

---

---

---

---

---

---

---

## EAL (Evaluation Assurance Level)

- Näide  
EAL1 on kasutatav seal, kus on nõutav teatud kindlus, et IT süsteem toimib korrektselt (nii nagu ette nähtud), samas ei näi ohud turvalisusele eriti tõsised olevat

---

---

---

---

---

---

---

---

## Infosüsteemide turvameetmete süsteemi kehtestamine

- Vabariigi Valitsuse 12. augusti 2004. a määrus nr 273

<http://riigiteataja.ee/ert/act.jsp?id=791875>

- (1) Määrusega kehtestatakse riigi ja kohaliku omavalitsuse andmekogude pidamisel kasutatavate infosüsteemide ning nendega seotud infovarade turvameetmete süsteem.
- (2) Turvameetmete süsteem koosneb turvanõuete spetsifitseerimise korrast ning andmete organisatsiooniliste, füüsiliste ja infotehniliste turvameetmete kirjeldustest.
- (3) Määrust ei kohaldata riigisaladust töötlevate infosüsteemide turbeks.

---

---

---

---

---

---

---

---

## Näide — konfidentsiaalsus

- S3 — Andmete avalikustamine on ohtlik riigi, asutuse või inimese julgeolekule (võib põhjustada kontrollimatuid muutusi riigile või asutusele tähtsates süsteemides. Riigi korral on kahjud võrreldavad eelarvega, ettevõtte korral aastakäibega). Juurdepääsupiirangutega teave.

---

---

---

---

---

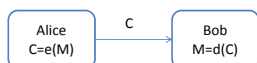
---

---

---

## Krüptosüsteemi baas-stsenaarium

- Alice ja Bob tahavad suhelda salaja.
- Alice saadab teade Bobile  
Formaalselt on Alice teade avatekst (plaintext)  $M$ . See krüpteeritakse funktsiooniga  $e()$ . Tulemuseks on krüptogramm  $C=e(M)$ .  
Bob võtab krüptogrammi vastu ning dekrüpteerib selle kasutades funktsiooni  $d()$ . Sellisel juhul  $d(C)=d(e(M))=M$ .




---

---

---

---

---

---

---

---

## Saladused

- Määratlus (P. Lorents, 2006). *H jaoks on saladuseks selline teadmine, mida H ei tohi omada. Saladust eristab mitteteadmise asjaolu, et "ei tohi omada", mis pole sugugi samaväärne asjaoluga "ei oma".*
- **Näide:** Inimese palk kui saladus. Kui on kirjutatud inimese nimi, siis ei tohi kõrval olla kirjutatud palga numbrit.
- **Salastatud andmed:** Meenutame, et andmeteks on teadmise "pooled" (kus esimene on tähise, teine aga tähenduse jaoks). Andmete salastamiseks tuleb vähemalt üks "pooltest" ära varjata. Seega tähis saadaksegi kätte, siis tähendust ei tohiks kätte saada. Ning vastupidi, kui on tähendus on kätte saadud, siis tähis peaks jääma kättesaamatuks.
- **Näide:** krüptogramm – tähis, mille tähendus ei tohi sattuda sattuda võõra kätte.

---

---

---

---

---

---

---

---

### Konfidentsiaalsuse tagamine krüpteerimise abil

- SSL/TLS
- SSH
- IPSec
- PGP
- jne

**Šifreerimine (erijuhul krüpteerimine)** on niisugune kodeerimine, mille korral kodeeritavad tekstid, kõnede või piltide salvestused jms jäävad teise (mittelubatud) isiku jaoks saladusse.

---

---

---

---

---

---

---

---

---

---

### Konfidentsiaalsuse tagamine krüpteerimise abil

- Transpordikihi turbeprotokoll *TLS (Transport Layer Security)* lubab autentimist ning andmete turvalist ülekandmist läbi interneti kasutades krüpteerimist.
- *SSL (Secure Sockets Layer)* sisaldab kolm etappi:
  - Osapoolte vaheline dialoog, mille eesmärgiks on šifreerimise algoritmi valik
  - Vastastikune võtmete vahetus, näiteks autentimine sertifikaatide abil
  - Andmete ülekandmine kasutades krüpteerimis-algoritme

---

---

---

---

---

---

---

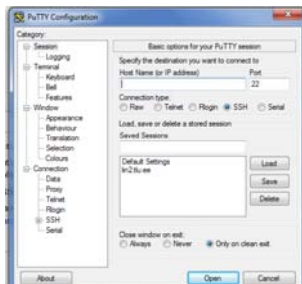
---

---

---

### Konfidentsiaalsuse tagamine krüpteerimise abil

- Turvakest SSH (Secure Shell)**
- SSH kasutab avaliku võtme krüpteerimist, et autentida võrguarvuti ja vajadusel ka kasutaja. SSH-d kasutatakse enamasti võrguarvutisse sisselogimiseks ja seal tegutsemiseks.
  - Standardne TCP port 22 on määratud SSH serveritega ühendumiseks




---

---

---

---

---

---

---

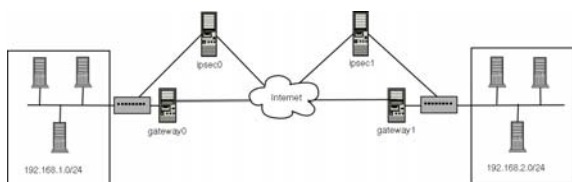
---

---

---

### Konfidentsiaalsuse tagamine krüpteerimise abil

- IPsec (IP Security) – protokollide komplekt, mis on seotud šifreerimisega, autentimisega ning IP pakettide turvalise edastamisega. IPsec “kapseldab” IP paketid turvalistesse pakettidesse.




---

---

---

---

---

---

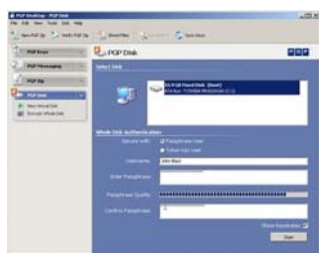
---

---

### Konfidentsiaalsuse tagamine krüpteerimise abil

- PGP (*Pretty Good Privacy*) – arvuti programm, mis võimaldab failide ja muu digiinfo šifreerimist ja digiallkirjastamist.

<http://www.pgp.com/>




---

---

---

---

---

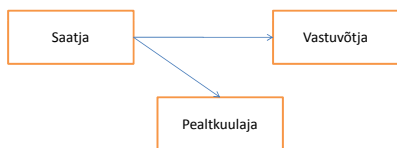
---

---

---

### Rünnete klassifikatsioon

- I. **Passiivne.** Rünne, kus vastane kuulab pealt, aga ei saa andmeid muuta, kustutada või lisada midagi omapoolset.



Andmete korjamine, analüüs

---

---

---

---

---

---

---

---

## Rünnete klassifikatsioon

II **Aktiivne rünne**- rünne, kus vastane saab edastavat informatsiooni muuta (sh täiendada)

1. teenuse tõkestamine ehk **DoS rünnak (Denial of Service)**- tekitatakse tõrge normaalses funktsioneerimises. Tõrge võib olla nii tarkvara kui riistvara tasemel ( nt. elektromagnetilised rünnakud ).

Näited:

- **BGP rünnak (Border Gateway Protocol):**  
Mustade aukude tekitamine (*blackholing*)  
Ümbersuunamine (*redirection*)  
Alamversiooni tekitamine (*subversion*)  
Võrguliikluse mittestabiilsus (*instability*)
- **PDoS (Permanent Denial-of-Service):** ruuteri või mõne muu võrguseadme vastu suunatud rünnakud. Mõjutavad seadme tarkvara või teeavad tarkvara uuendusi (firmware flashing)




---

---

---

---

---

---

---

---

---

---

## Näide: Denial of Service

- Ülekoormus
- Ressursside ammendamine
  - Kettaruum
  - Mälu, protsessitabel
  - Protsessoriaeg (näiteks tehakse "tühja" krüpteerimist)
  - Võrguriba (ujutatakse pakettidega üle)
- Vead süsteemi ja protokollide disainis ja realiseerimises

Meelis Roos, Tartu Ülikool,  
<http://math.ut.ee/~mroos/turve/vork.pdf>

---

---

---

---

---

---

---

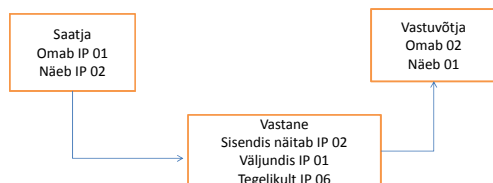
---

---

---

## Rünnete klassifikatsioon

2. Vahemehe rünnak (Man in the middle): muudab kas saadetud info või info pakettide järjekorda. Saatja ja vastuvõtja seadmetele valetatakse oma tõelist identiteeti ning nad ei tea, et "räägivad" läbi kolmanda isiku.




---

---

---

---

---

---

---

---

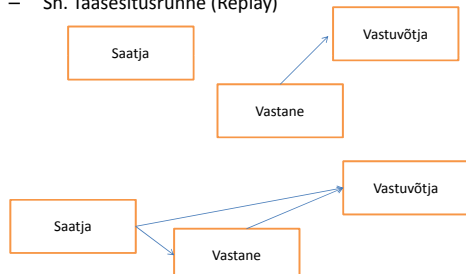
---

---

## Rünnete klassifikatsioon

3. Võltsimine, falsifitseerimine – vastane näitab end teise isikuna (autentimisjada kasutamine teeskluks)

– Sh. Taasesitusrünne (Replay)




---

---

---

---

---

---

---

---

## Näited: Kuidas võltsida...

- IP aadressi vahetus
- MAC aadressi vahetus
- IP aadressi võltsimine (*IP spoofing*)
- MAC aadressi võltsimine
- ARP võltsimine
- DNS kirjade võltsimine, valed pöördteisendused
- Source ruuting
- Marsruutimisinfo võltsimine
- Ühenduste kaaperdamine (*hijacking*)

Meelis Roos, Tartu Ülikool,  
<http://math.ut.ee/~mroos/turve/vork.pdf>

---

---

---

---

---

---

---

---

## IT-relvad ja küberrelvad

- (Lorents, Ottis 2010) **Infotehnoloogiliseks relvaks** nimetame sellist IT-lahendustele rajatud süsteemi, mis on loodud just selleks, et lõhkuda teiste süsteemide ülesehitust või muuta võimatuks nende (ettenähtud viisil) toimimine

**Näide.** "Targad piloodita lahingulennukid", mis suudavad iseseisvalt, vajadusel marsruuti valides ja korrigeerides hävitatava sihtmärgini jõuda, on IT-relvad. 11. septembril New Yorgi kaksiktorne tabanud ja väga palju protsessoreid ja tarkvara kasutavad "Boengid" pole IT-relvad

- (Lorents, Ottis 2010) **Küberrelvaks** nimetame sellist IT-süsteemi, mis on loodud just selleks, et lõhkuda teiste **IT-süsteemide** ülesehitust või muuta võimatuks nende (ettenähtud viisil) toimimine

**Näide.** Arvutiviirused on küberrelvad. Nn fondi- või foonivärvijad pole relvad, kuigi nende abil võib kirjutatu mittedähtavaks muuta (nt punane kiri punasel taustal)

---

---

---

---

---

---

---

---

## Küberintsidendid ja küberründed

- (Lorents, Ottis 2010) **Küberintsident** on sündmus (*event*), mis põhjustab või võimalik, et põhjustab mittelubataavaid muutusi IT-süsteemi ülesehituses või toimimises ettenähtud viisil  
**Näited.** Välglööök, viirusest nakatumine.
- (Lorents, Ottis 2010) **Küberrünne** on küberrelva või küberrelvana kasutatava süsteemi ettekavatsetud kasutamine küberintsidendi esilekutsumiseks või selleks, et lõhkuda teiste IT-süsteemide ülesehitust või muuta võimatuks nende (ettenähtud viisil) toimimine

---

---

---

---

---

---

---

---

---

---

## Turvateenused

- **Turvateenused** takistavad ohtude realiseerumist ja/või aitavad vähendada ohtude realiseerumisel saadavat kahju.
- Konfidentsiaalsuse tagamine
- Käideldavuse tagamine
- Autentimine – kinnitus sellele, et info on saadud seaduslikest allikatest ning saaja on just see isik kellena ta end esitab.
- Terviklus – kinnitus sellele, et info ei ole säilitamisel või edastamisel muudetud.

---

---

---

---

---

---

---

---

---

---

## Turvateenused

- Salgamise vääramine – Saaja ning vastuvõtja ei saa keelduda info edastamisest. Kui info on saadetud, siis vastuvõtja saab võimaluse kindlaks teha (tõestuse) kas info on saadetud ja kas saatja oli legaalne. Samuti, kui info on vastuvõetud, siis saatja saab võimaluse kindlaks teha (tõestuse), et see on võetud vastu ning legaalse vastuvõtjaga.
- Pääsu reguleerimine (*access control*) – võimalus piirata ja kontrollida juurdepääsu süsteemidesse kommunikatsiooni liinide kaudu
- Juurdepääsevus – rünnete tagajärjeks võib olla süsteemi või teenuse juurdepääsu häire. Antud teenus vähendab teenuse tõkestamise DoS-ründeid

---

---

---

---

---

---

---

---

---

---

## Turvamehhanismid

- Sümmeetriline šifreerimine – algoritmid kasutavad ühte ja sama võtit nii šifreerimiseks kui ka dešifreerimiseks, või siis dešifreerimise võtit on võimalik saada šifreerimise võtmest.
- Asümmeetriline šifreerimine – algoritmides kasutatakse kaht erinevat võtit šifreerimiseks ja dešifreerimiseks, kusjuures teades üht ei ole ise-enesest veel võimalik saada teist.
- Räsifunktsioonid (Hash functions) – funktsioonid, mille sisendiks on suvalise pikkusega sõnum ning väljundiks on **kindla** pikkusega krüptograafiline lühend.
- Taastemehhanismid – varundamine, infosüsteemi kriitiliste sõlmede dubleerimine, operatsioonide päeviku pidamine

---

---

---

---

---

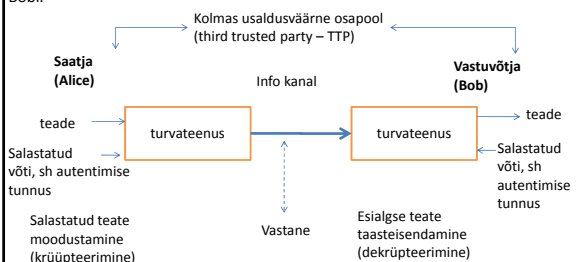
---

---

---

## Mudel

Alice' peab olema veendunud, et teine osapool on Bob, sest pahalane võib mängida Bobi.



Oletame, et Alice vajab krüpteerimisvõtit, aga pole kunagi Bobiga kohtunud. Kolmas osapool (TTP) on see pool, mis "teab" Bob-i ja on volitatud teadma tema krüpteerimisvõtit. Alice saab usaldada sellist võtit, kui ta usaldab kolmandat osapoolt.

---

---

---

---

---

---

---

---

## Mudelist tulenevad eesmärgid

- Töötada välja krüpteerimise/dekrüpteerimise algoritm, mis võimaldaks info turvalist edastamist. Algoritm peab olema selline, et vastane ei saaks dekrüpteerida sõnumit, kui ta ei tea salastatud võtit.
- Moodustada salajased krüpteerimisvõtmed
- Töötada välja protokoll, mis võimaldab salavõtmete edastamist nõnda, et see ei sattuks vastasele.

---

---

---

---

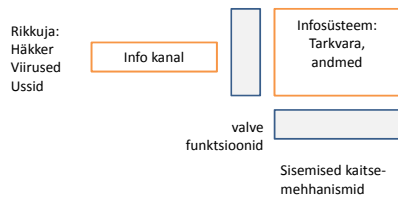
---

---

---

---

## Infosüsteemi turvamudel



- rünne eesmärgiga saada või muuta süsteemis paiknevad andmed
- rünne teenuste vastu, et häirida turvateenuste tööd

### Turvateenused:

*Valvefunktsioonid:* Antud mehhanismid sisaldavad näiteks autentimist, tulemüüre.  
*Sisemised kaitse-mehhanismid:* sise-monitooring, mis kontrollib, et kes on ühenduses ja mis on tema tegevus.

---

---

---

---

---

---

---

---

---

---

## Infosüsteemi turva-alused

- Infosüsteemi turvalisus peab vastama organisatsiooni rollidele ja eesmärkidele
- Infoturbe osutamiseks on vaja terviklikku lähenemisviisi
- Infoturbe peaks olema lahutamatu osa organisatsiooni haldamise korraldamises
- Infoturbe peab olema majanduslikult põhjendatud
- Vastutus süsteemi turvalisuse eest peab olema selgelt määratletud
- Infosüsteemi ohutust tuleks perioodiliselt uuesti hinnata
- Suure tähtsusega infosüsteemide turvalisuse juures on olulised ka sotsiaalsed tegurid, samuti haldus-, organisatsiooniline- ja füüsiline turvalisus

---

---

---

---

---

---

---

---

---

---