Andmeturve

Meelis Roos
mroos@ut.ee

kevad 2018

Kava (1)

- Turvaeesmärgid, ohud, riskianalüüs, turvapoliitika, turbestrateegiad, turvatasemed, turvastandardid
- Mitmekasutajasüsteemide turve, DAC & MAC, usaldatavad süsteemid
- Autentimismeetodid, paroolid, NIS(+), Kerberos, NT domeenid, LDAP kataloogid, Active Directory, *single signon*
- PKI (avaliku võtme infrastruktuuride) idee, rakendamine autentimisel ja signeerimisel, hierarhiad

Kava (2)

- Ohud võrgus, tulemüürid, krüpto rakendamine
- Rünnakute avastamine: *IDS*, logimine; taasteplaanid; turvaprobleemide PR
- Viirused, ussid, trooja hobused, tagauksed, . . .
- Privaatsus ja anonüümsus Internetis
- Pöördkodeerimine, seadused, kopeerimiskaitsed, . . .

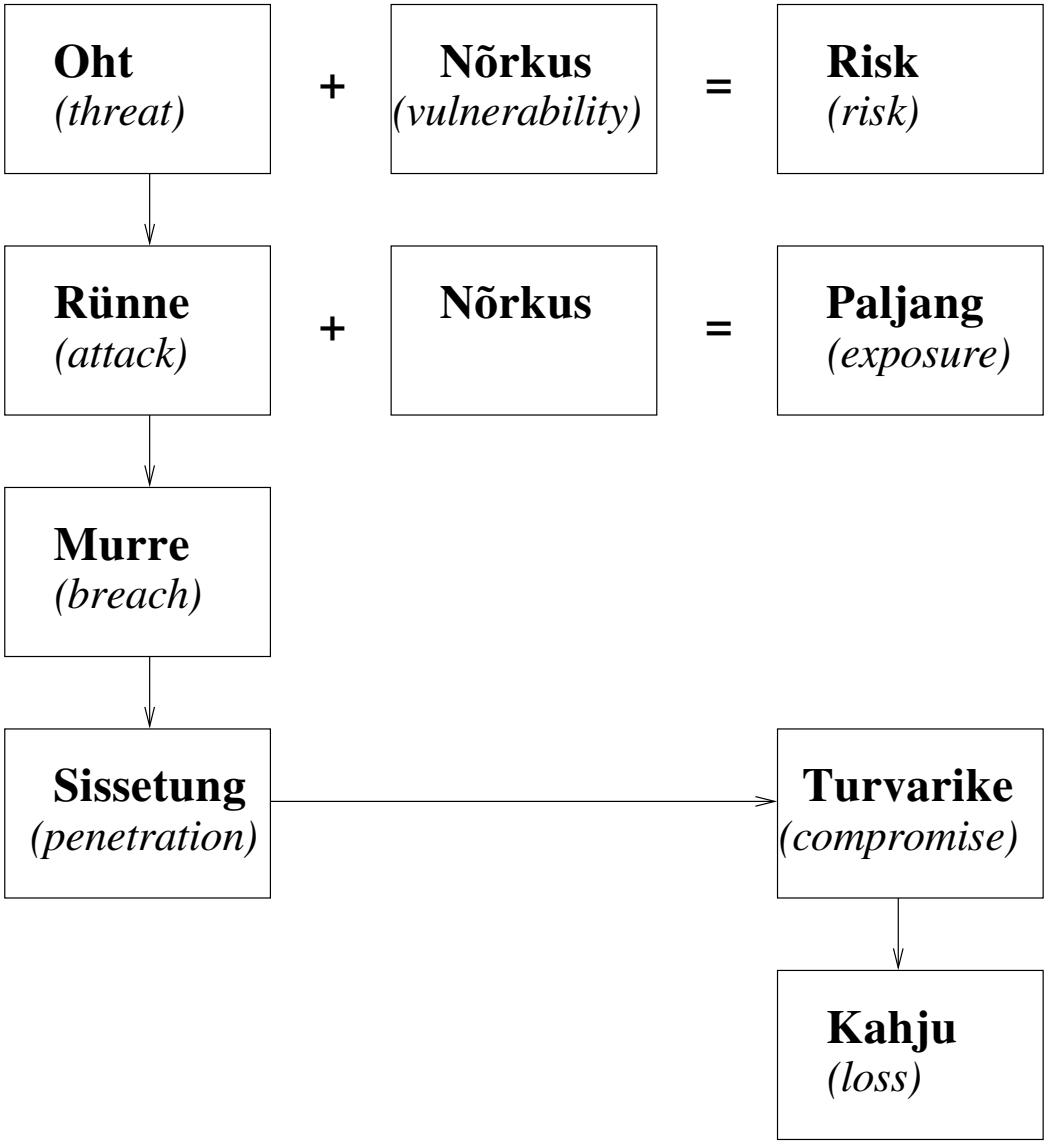
Kirjandus

- Infosüsteemide turve 1: turvarisk. Vello Hanson, Märt Laur, Monika Oit, Kristjan Alliksoo. Cybernetica AS, Tallinn 2009
- Infosüsteemide turve 2: turbetehnoloogia. Vello Hanson, Ahto Buldas, Tarvi Martens, Helger Lipmaa, Arne Ansper, Viljar Tulit. Küberneetika AS, Tallinn 1998
- Security Engineering. Ross Anderson, Wiley 2001
- Practical UNIX & Internet Security. Simson Garfinkel, Gene Spafford. Second edition. O'Reilly 1996 (tasuta, aga vanavõitu)
- Firewalls and Internet Security: Repelling the Wily Hacker. William R. Cheswick and Steven M. Bellovin. Addison-Wesley, 1994 (tasuta), 2011; http://www.wilyhacker.com/
- Secrets and Lies: Digital Security in a Networked World. Bruce Schneier. John Wiley & Sons 2000

Turvaeesmärgid

- Käideldavus (*availability*) — varad peavad olema kasutatavad
- Terviklus (*integrity*) — varasid tohivad modifitseerida ainult volitatud asjaosalised
- Konfidentsiaalsus (*confidentiality*) — varad on kättesaadavad ainult volitatud asjaosalistele

Turvalisuse rikkumise tasemed



Ohud

- Ohtude liigid:
  - halvang
  - infopüük
  - modifitseering
  - võltsing
- Ohustatud objektid:
  - andmed
  - tarkvara
  - riistvara
  - side
- Stiihilised ohud (keskkond, tehnilised rikked, inimohud) vs ründeohud
- Sisemised või välised ohud

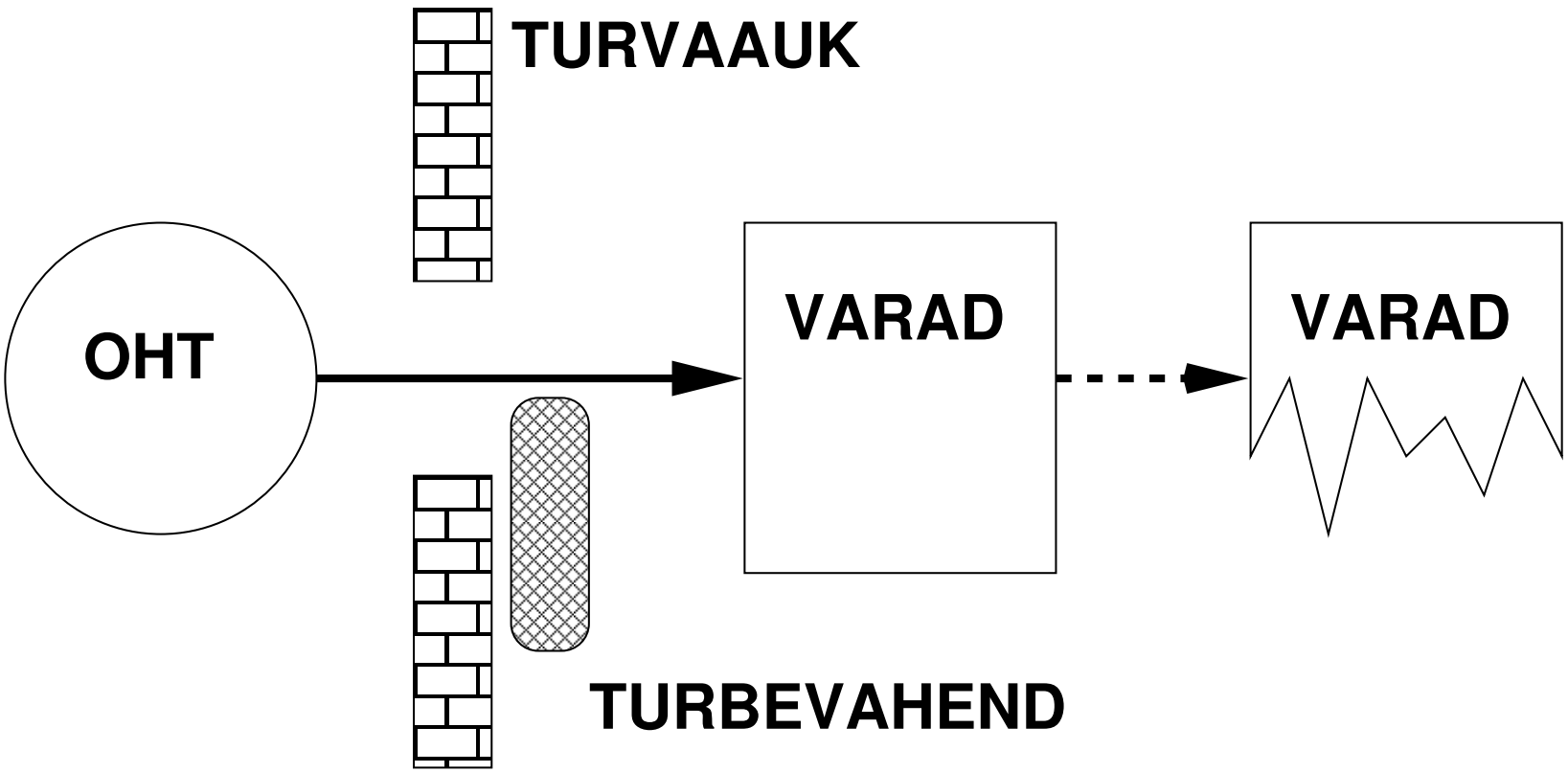
Ohud: leia näited

	andmed	tarkvara	riistvara	side
halvang	?	?	?	?
infopüük	?	?	?	?
modifitseering	?	?	?	?
võltsing	?	?	?	?

Ründajad

- Volitatud kasutajad — suurim oht
- Majandus- ja sõjalise luure agendid: vähe teada, tihti profid, peidavad jälgi. Enamasti otsivad mingit konkreetset infot.
- Häkkerid
  - Niisama huvilised — uurivad süsteemide turvalisust oma lõbuks. Reeglina ei tee kurja, vahel teavitavad omanikku leitud turvaprobleemidest. Leiavad uusi turvaauke.
  - Skriptijuntsud (*script kiddies*) — Murravad süsteemi sisse, teevad pahategusid (näotustamine (*defacement*), andmete kustutamine). Enamasti kasutavad teiste tehtud ründeprogramme, tihti neist ise aru saamata.
  - Organiseeritud kuritegevus — see on terve tööstusharu
- Muud (arvutivargused, . . .)

Riskianalüüs



Riskianalüüs

- Potentsiaalsete ohtude tõenäosused on erinevad
- Erinevate ohtude poolt tekitatav kahju on erinev
- Riskianalüüs — hindame reaalseid ohte ning kulutusi ning püüame leida aktsepteeritava riski, kus turbekulud on ligikaudu võrdsed tõenäoliste kahjudega

Ohtude edetabel 2014

- Pahavara (ussid, trooja hobused, nuhkvara)
- Veebipõhised ründed kliendi pihta
- Ründed veebirakendustele
- Zombivõrgud (*botnets*)
- Teenustõkestusründed
- Spämm
- Õngitsemine (*phishing*)
- Eksploidipakid
- Andmelekked
- Füüsiline kahjustamine, vargused
- Siseründed
- Identiteedivargused
- Spionaaž
- Lunavara (*ransomware*)

Turbestrateegiad 1

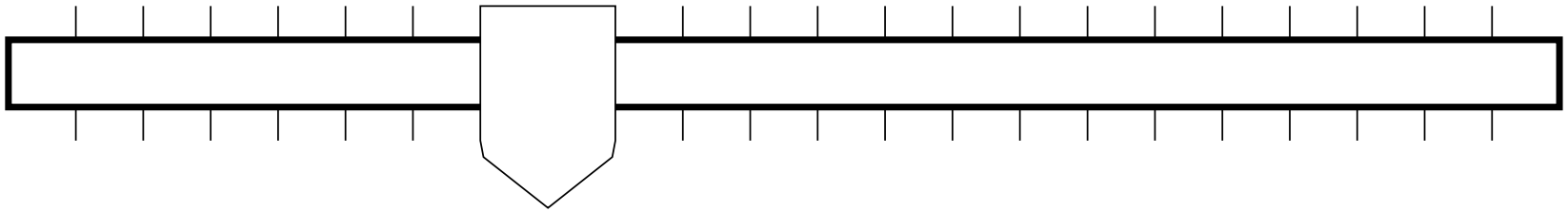
- Vähim vajalik privileeg — igale objektile ja subjektile antakse minimaalne tööks vajalik õiguste komplekt
- Kaitse sügavuti — kasutatakse mitut järjestikku asuvat kaitsemehhanismi
- Läbilaske punkt — kogu pääs toimub ühest, hästi kontrolli all olevast punktist
- Nõrgim lüli — kett on nii tugev kui tugev on tema nõrgim lüli
- Tõrkekindel süsteem — turvasüsteemi tõrke korral pääs pigem keelatakse kui lubatakse

Turbestrateegiad 2

- Üldine osavõtt — turvameetmed ei toimi, kui kasutajad neist mööda hiilivad
- Kaitse mitmekesisus — mitte loota ühte sorti ja ühest allikast pärit vahenditele, kasutada heterogeenseid kaitsesüsteeme
- Lihtsus — keerukus on turvalisuse vaenlane
- Turvalisus läbi varjamise — ründajat üritatakse hägustamisega segadusse ajada

Mõned suured prohmakad uskumises

- Marcus Ranum:
  - *Default permit*
  - *Enumerating badness*
  - *Penetrate and patch*
  - *Hacking is cool*
  - *Action is better than inaction*
  - *Educating users solves problem*
  - *We are not a target*
  - *Everyone would be secure if they all just ran Z*
  - *We don't need a firewall, we have good host security*
  - *We don't need host security, we have a good firewall*
  - *Let's go production with it now and we can secure it later*



- Reaalses elus on vaja teha kompromiss turvalisuse ja kasutatavuse vahel