Arvuti turvalisus

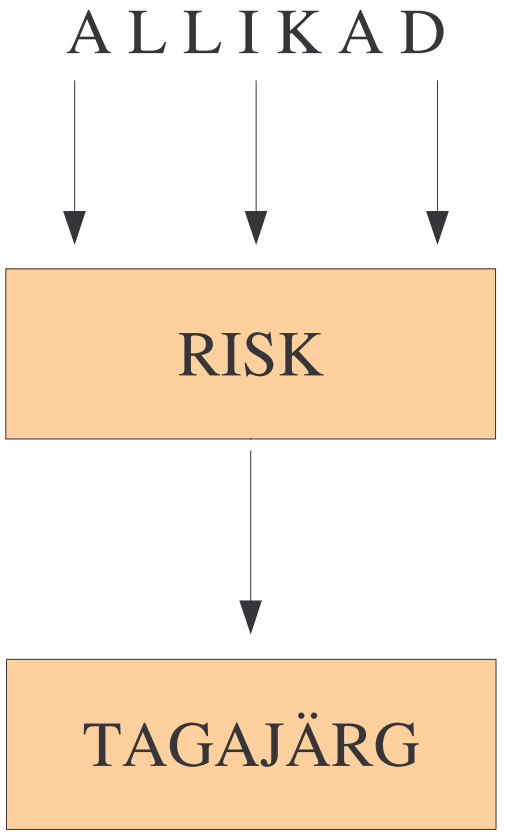
Ivari Horm
ranger@risk.ee

Sissejuhatus

- **Riskide liigitus**
- **Riskiallikad**
  - Füüsilised riskiallikad täpsemalt
  - Tarkvaralised riskiallikad täpsemalt
  - Psühholoogilised riskiallikad täpsemalt
  - Süsteemsed riskiallikad täpsemalt

Riski tekkimine

- Risk – võimalik oht
- Tekib **allika** mõjul
- Võib omada **tagajärge**



Riskid

Ivari Horm
ranger@risk.ee

Riskid

- **Tarkvaralised**
  Seotud andmetega

- **Riistvaralised**
  Seotud arvuti riistvaraga

Tarkvaralised riskid

- Andmete kadumine
- Lubamatu andmete muutmine
- Volitamata juurdepääs andmetele

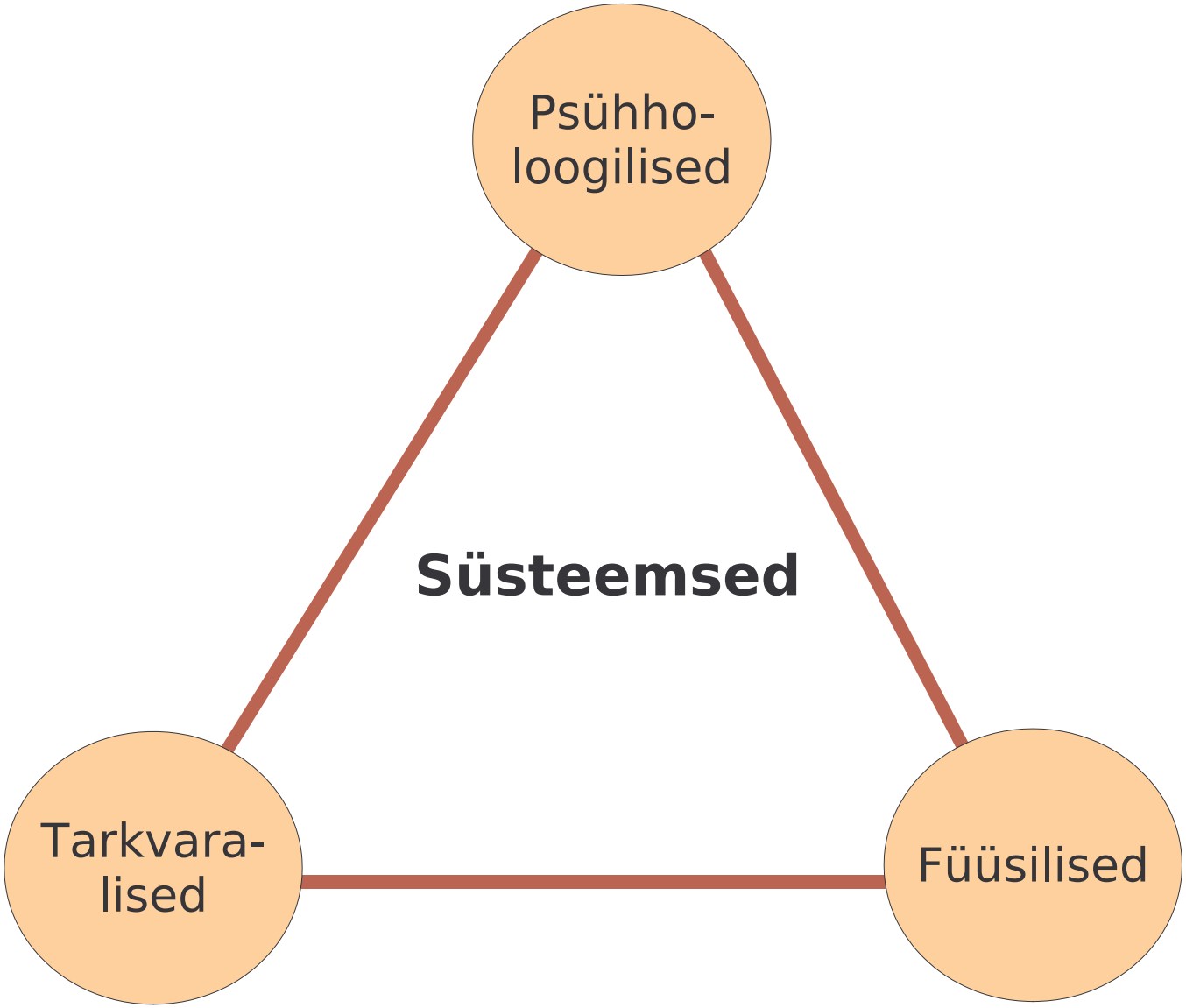
Riistvaralised riskid

- Riistvara rikkumine
- Riistvara hävimine
  Tagajärjeks võib olla ka andmete hävimine
- Ressursside omavoliline ärakasutamine

Riskiallikad

Ivari Horm
ranger@risk.ee

Riskiallikad



Füüsilised allikad

- **Arvuti asukoht**
  Määrab füüsilise turvalisuse taseme
- **Füüsiline turvalisus**
  Seotud arvuti asukohaga
- **Amortisatsioon**
  Riistvara vananemine

Tarkvaralised allikad

- Pahtahtlik tarkvara (malware)
- Vigane tarkvara
  - Vigased lõpp-produktid
  - Beetaversioonid

Psühholoogilised allikad

- **Valed ootused**
  "Arvuti on eksimatu"

- **"Operaatorivead"**
  Tarkvara vale kasutamine

Süsteemsed allikad

- **Riistvara + tarkvara**
- Riskid, mis tulenevad kasutatavast arvutisüsteemist
- Süsteemihalduri eksimused
  - Süsteemi vale (ebaturvaline) disain
  - Vead süsteemi haldamisel

Füüsilised riskiallikad

Ivari Horm
ranger@risk.ee

Füüsilised riskiallikad

- Arvuti füüsiline turvalisus ei suuda täielikult tasakaalustada asukohast tulenevat riski!
- Keset tänavat asuvat arvutit ei ole võimalik muuta sama turvaliseks kui laboriarvutit.
- Arvuti asukoht on määravaima tähtsusega

Füüsiline juurdepääs

- Kui arvutile on võimalik füüsiliselt juurde pääseda, on turvalisus sama hea kui null.

Füüsiline juurdepääs

- **Arvuti korpuse lukustamine**
  Ketassaag
- **Arvuti kinnitamine põranda külge**
  Kõvaketta väljavõtmine
- **BIOS-i parool**
  BIOS-i parooli lähtestamine emaplaadilt
- **Operatsioonisüsteemi parool**
  Mõne teise operatsioonisüsteemi kasutamine (live-CD)

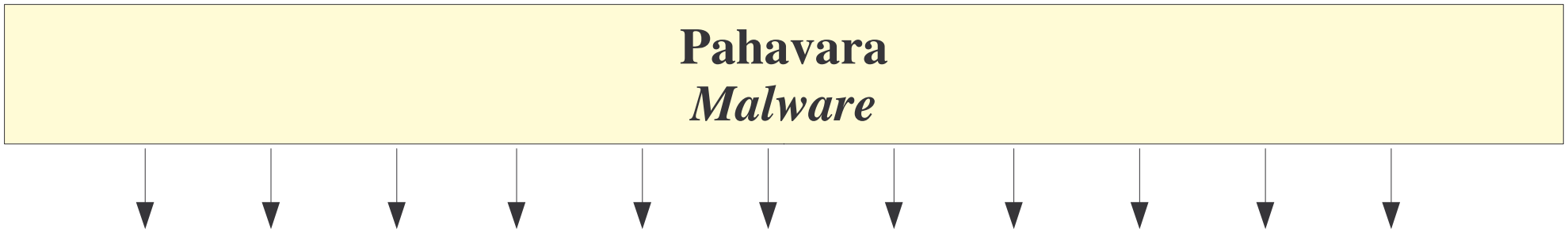
Amortisatsioon

- Kui arvuti on juba töötanud 10 aastat, siis suure tõenäosusega töötab veel 10 aastat.
- Põhiline risk peitub kuluvates osades
  Ventilaatorid, mootorid, lugemispead jne.

Tarkvaralised riskiallikad

Ivari Horm
ranger@risk.ee

Pahatahtlik tarkvara



Viirused *Viruses*	Trooja hobused *Trojan horses*	Nuhkvara *Spyware*	Ussid *Worms*
? *Rootkits*	? *Exploits*	Varasvara *Stealware*	
Tagauks *Backdoor*	? *Dropper*	? *Wabbit*	Rotivara *Ratware*

Viirused

- *Virus, viruses (*mitm. ka *virii)*
- Esimene viirus 1982. aastal
- Rich Skrenta poolt loodud “Elk Cloner”
- Levis AppleDOS 3.3 süsteemis flopide abil

Viirused

- Terminit kasutas esmakordselt Fred Cohen 1984. aastal
- Mõiste oli kasutusel varem kirjanduses ja filmides
  - “When H.A.R.L.I.E was One”, David Gerrold (1970)
  - “The Shockwave Rider”, John Brunner (1975)
  - Film “Westworld” (1973)

Viirused

- Viimasel ajal vähem levinud kui teised pahavara liigid
- Võimelised ise levima
- Levivad teiste programmide kaudu
- Võivad iseeneslikult muutuda (muteeruda)

Viirused

- **Nakatamine *(infection)***
  Viiruskoodi lisamine olemasolevale programmile

- **Viirusekandja *(host)***
  Viirusega nakatunud programm

Viirused

- Viirus suudab teist arvutit nakatada ainult ainult viirusekandja abil, mis tuleb arvutis käivitada.
- Iseeneslikult viirus võõrast arvutit nakatada ei suuda!
- Mitte segamini ajada ussidega!

Viirused

- Ei pruugi olla ohtlikud, pigem tüütud
- Siiski ka väga palju ohtlikke viirusi!
- **Pomm *(bomb)***
  Viirus, mis käivitub teatud aja pärast

Ussid

- Mõiste pärit novellist “Shockwave Rider”, John Brunner (1970)
- 1978 esimene testiuss Xeroxi Palo Alto uurimiskeskuses

Ussid

- 2. november 1988 esimene reaalne võrgus leviv uss
- Kirjutatud Cornelli ülikooli tudengi Robert Tappan Morris Jr. poolt
- Levis BSD Unixi turvaaugu kaudu

Ussid

- Võimelised ise levima
- Ei vaja paljunemiseks viirusekandjat
- Kustutavad arvutist faile või saadavad nakatatud e-kirju

Ussid

- Võivad installeerida tagauksi
- Nakatatud arvuteid kasutavad spämmerid masspostituseks
- “Head ussid”
  - Nachi (Welchia) paigaldas nakatatud masinasse Windowsi kriitilisi veaparandusi
  - PAHA: suur võrgukoormus ja masinate taaskäivitumine

Tagauks

- Annab volitamata juurdepääsu arvutile
- **Volitamata juurdepääs**
  Arvutis olevale infole pääseb ligi ilma paroolita või mingi varem kindlaks määratud parooli alusel
- Sissetungijal ei pea olema selles arvutis kasutajakontot

Tagauks

- Film “War Games” (1983)
- November 2003 GNU/Linux-i tagauks
- Ken Thompson “Reflection on Trusting Trust”
  Ühe tagaukse loomise võimaluse kirjeldus

Trusting Trust

- **Kompilaator**
  Programm, mis teisendab programmi lähtekoodi masinkoodiks, mida saab käivitada
- Masinkoodi inimene kunagi ei loe
- Inimene usaldab kompilaatorit
  - Masinkood on loodud lähtekoodist ausal teel
  - Masinkood vastab lähtekoodile

Trusting Trust

- Kompilaator on ka programm
- Programmid on masinkoodis
- Inimene ei tea, kuidas kompilaator tegelikult töötab

Trusting Trust

- Programmi teisendamisel masinkoodi lisab kompilaator sinna sisse tagaukse
- Inimene seda ei tea, sest ta ei loe kunagi masinkoodi

Trooja hobune

- *Trojan horse, trojan*
- Pahavara, mis näitab ennast tavalise tarkvarana
- Ei suuda ise levida

Trooja hobune

- Programmid, mille nimi näitab üht, sisu aga teine
  free_phonecalls.exe
- Kahekordsed faililaiendid
  interesting_document.doc.exe

Trooja hobune

- Kustutab arvutist faile
- Aitab levitada muud pahavara
- Kogub infot kasutaja tegevuse kohta ja edastab seda

Nuhkvara

- Kogub kasutaja teadmata infot tema harjumuste kohta
- Näitab reklaamiga hüpikaknaid *(popup)*
- Suunab kasutajat veebis mõnele libalehekülgele
- Paigaldab arvutisse kaugekõnede valimise tarkvara

Nuhkvara

- Esimest korda kasutati terminit 1995. aasta oktoobris Ironiseeriti Microsofti ärimudelit
- Vahepeal tähistas ka spiooni tööriistu (nt. minikaameraid)
- 1999. kasutas Zone Alarm oma Personal Firewall tarkvaras terminit praeguses tähenduses
- 2000. aastal esimene nuhkvaravastane programm OptOut

Nuhkvara

- Üldjuhul ei levi iseeneslikult
- Üldjuhul ei kahjusta arvutis olevat infot
- Üldjuhul õhutab kasutajat installeerima

Nuhkvara

- Neelab arvuti ressursse
- Halvim näide
  Kuni 50% arvuti ressurssidest nuhkvara all
- Arvuti hangub, jookseb kokku
- Internetiga ühendumine raske või võimatu

Nuhkvara

- Võivad muuta arvutivõrgu tööks vajalikke faile, et raskendada enda eemaldamist
- Eemaldamise tulemusena võib Internetiühendus kaduda

Nuhkvara levimine

- Mõne teise programmi installeerimise kaudu (failivahetusprogrammid, “vabavara” programmid)
- Brauseri (Internet Explorer) turvaaukude abil
- Veebi kaudu kasutaja tähelepanematusest (kasutajat õhutatakse klikkima mõnel lingil)

Exploit

- Ühe programmi turvaauku ärakasutav tarvkara
- Kasutatakse turvaaukude demonstreerimisel
- Pärast vea parandamist programmis enam ei tööta

Exploit

- **Remote exploit**
  Ründab üle võrgu mõnda teist arvutit
- **Local exploit**
  Töötab ainult kohaliku masina piirides
- **Zero-day (0-day) exploit**
  Sihilikult mitte avaldatud exploit, mida saab hiljem sissetungiks ära kasutada

Script kiddie

- Otsivad Internetist võimalikke exploite ning proovivad neid erinevate arvutite peal
- Ei tea midagi sellest, kuidas need täpselt töötavad
- Nende tarbeks luuakse “libaexploite”, mis kahjustavad hoopis nende endi arvutit!

Wabbit

- Iseenselikult leviv programm
- Erinevalt viirusest ei kahjusta arvutis olevaid faile
- Erinevalt ussidest ei levi võrgu kaudu
- Paljundab ennast ise kohalikus arvutis

Rootkit

- Tuleneb Unixi administraatorkasutaja *(root)* nimest
- Programmide komplekt, mis varjab sissetungija tegevused
- Kuulab pealt arvutis toimuvat (võrguliiklust, klahvivajutusi)

Rootkit

- Võimaldab sissetungijal omada Unixis juurkasutajat
- Tõeline administraator ei märka seda

Rootkit

- Eksisteerib ka mujal kui Unix-süsteemides
  Ka Windowsis on administraatori kasutajakonto!
- Mõnikord liigitatakse ka trooja hobuste alla

Dropper

- Viirusepaigaldaja
- Viirus sisaldub dropperis selliselt, et viirusetõrjeprogramm seda ei märka
- **Injector**
  Dropper, mis kopeerib viiruse ainult arvuti mällu,mitte kõvakettale

Dropper

- Võib olla mõni tuntud programm, kuhu on **peidetud** viirus
- Sellisel juhul sarnaneb trooja hobusele
  - Tuttav programm, mis teeb tegelikult hoopis midagi muud

Rotivara

- Tarkvara, mida kasutatakse masspostitusel
- Spämmeri tarkvara
- Paigaldatakse mõnesse teise arvutisse
  Võimaldab selle arvuti kaudu spämmi saata

Vigane tarkvara

Ivari Horm
ranger@risk.ee

Vigane tarkvara

- Tarkvara muutub pidevalt keerulisemaks
- Uued tarkvaralahendused on ajakriitilised

Tarkvara ajakriitilisus

- Kes on maailma suurim Interneti-raamatupood?

http://www.amazon.com

- Aga kes on selles valdkonnas teisel kohal?

Tarkvara ajakriitilisus

- Uus toode tuleb turule tuua enne kui keegi ette jõuab

Vigane tarkvara

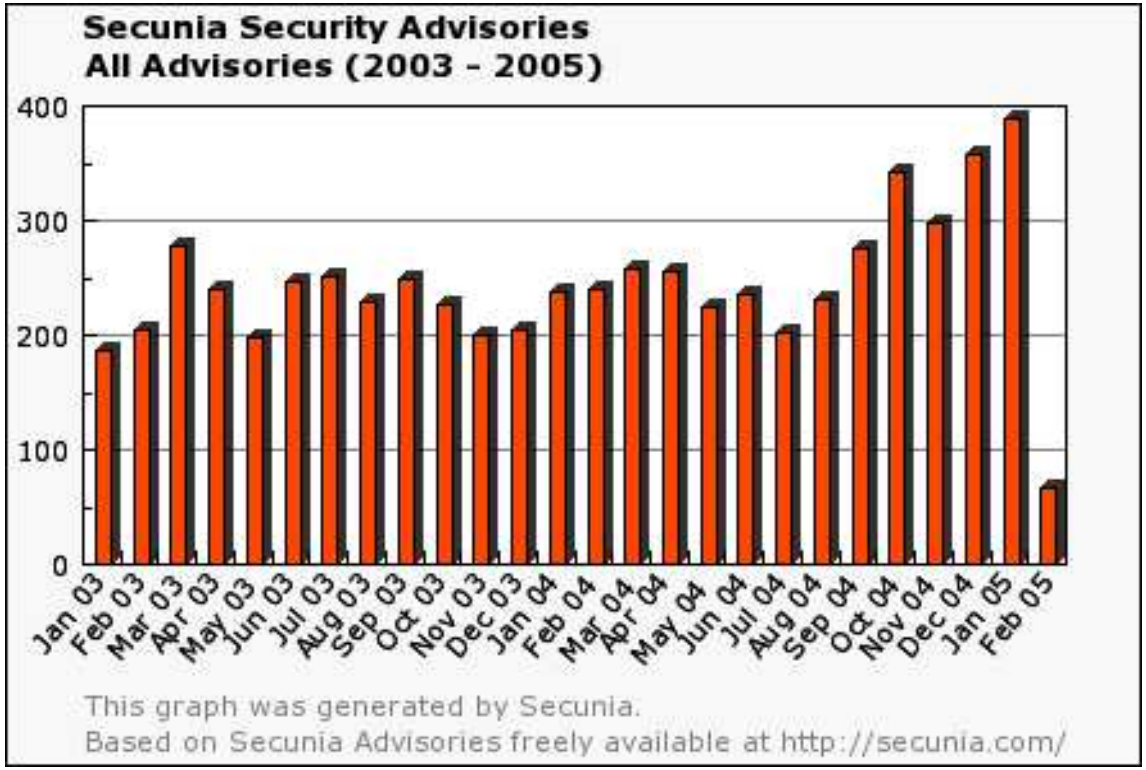
- Kõiki vigu ei suudeta parandada
- Ka uus tarkvara sisaldab vigu
- Tarkvara loojad varjavad vigu
  Põhjus: majanduslikud huvid

Vigane tarkvara

- Tarkvara loojad töötavad välja vigade parandusi
- Vigade parandused võivad uusi vigu tekitada!

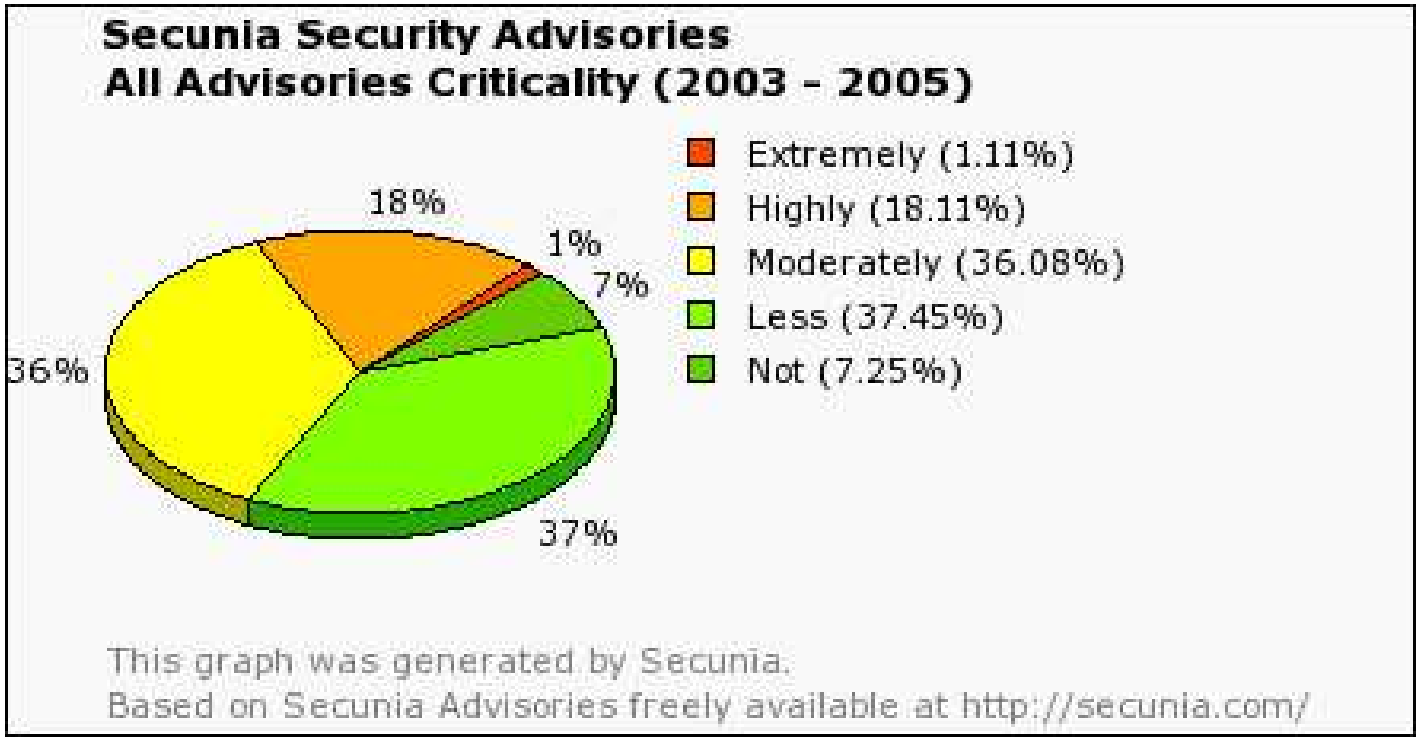
Tarkvaravigade statistika

- Avastatud vigade koguarv ajavahemikus 2003-2005



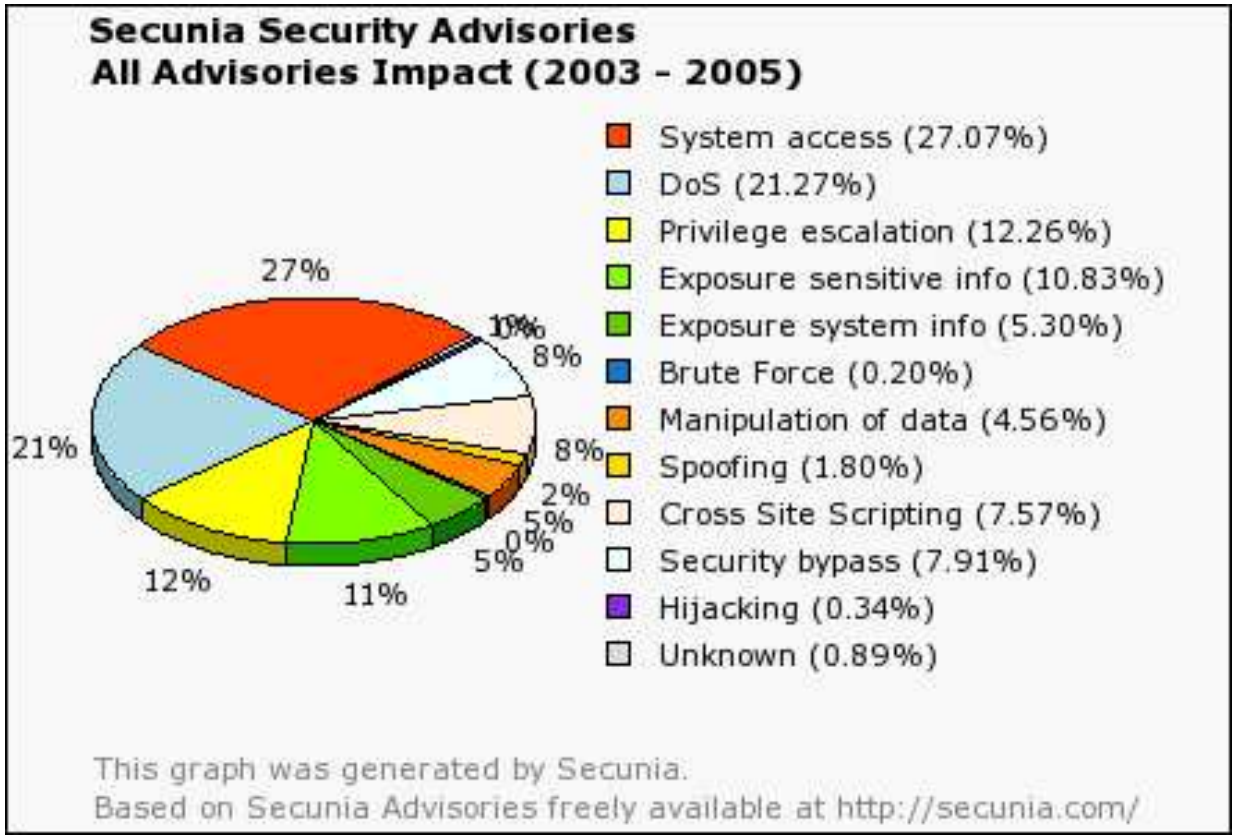
Tarkvaravigade statistika

- Tarkvaravigade jagunemine tõsiduse järgi



Tarkvaravigade statistika

- Tarkvaravigade mõju arvutisüsteemile ja andmetele



Vigane tarkvara

- Vigane tarkvara ei ole pahavara

Psühholoogilised riskiallikad

Ivari Horm
ranger@risk.ee

Valed ootused

- Programmidele ja arvutile pannakse liiga suuri lootusi
- Usaldatakse masinat
- Usaldatakse programme

Valed ootused

- Ettevaatamatu kustutamine (taastamine võimatu)
- Andmeid ei salvestata (voolukatkestus)
- Andmeid muudetakse ettevaatamatult

Valed ootused

- Automaatset töötavat programmi ei testita
- Loodetakse, et töötab kohe õigesti

```
cd C:\TEMP

del *.*
```

Programmide vale kasutamine

- Ei arvestata kõikide võimalike olukordadega
- Programmid käituvad erinevalt

```
cd C:\TEMP

del *.*
```

Programmide vale kasutamine

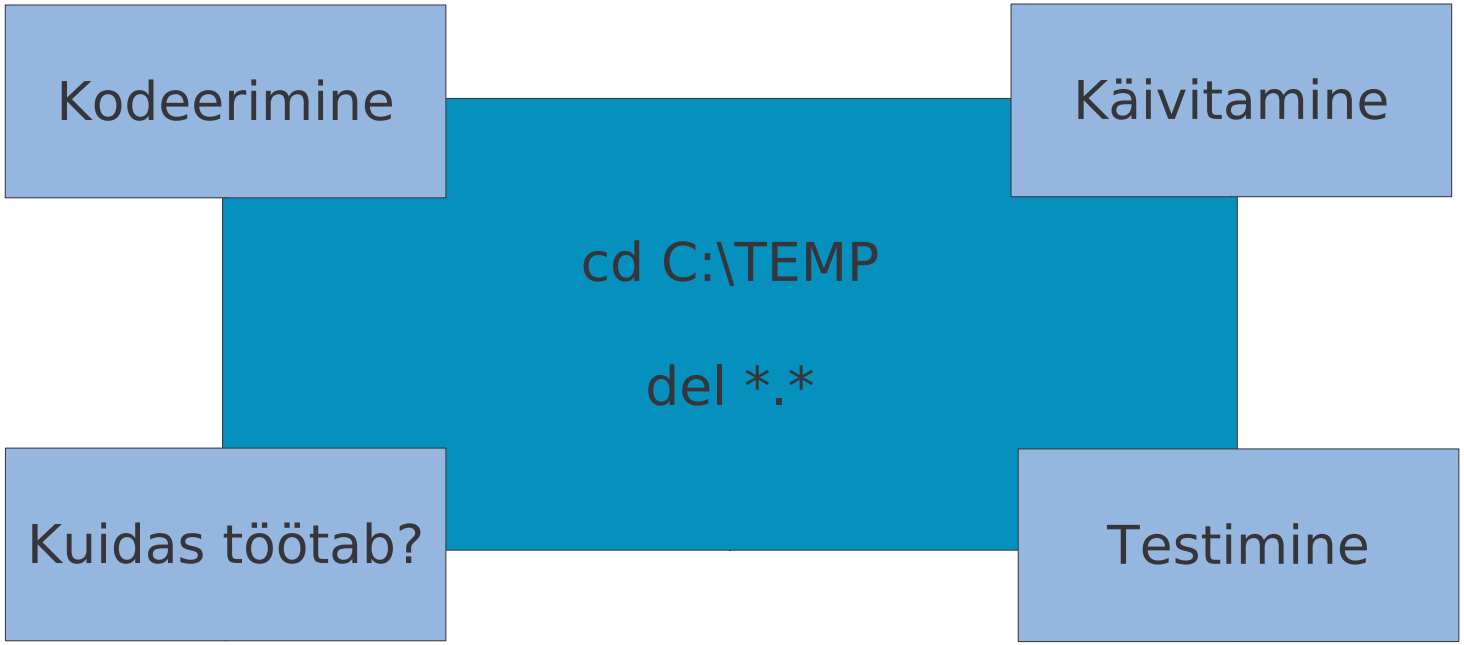
- Käivitatakse programme vales järjekorras
- Käivitatakse programme valede võtmetega

Programmide vale kasutamine

- Programmi küsimise peale antakse vale vastus
- **“Katsetamine”**
  Proovitakse katse-eksituse meetodil kindlaks teha, mida programm teeb

Programmide vale kasutamine

- Sarnased ohud kehtivad ka programmeerimisel



Süsteemsed riskiallikad

Ivari Horm
ranger@risk.ee

Süsteemsed riskiallikad

- Süsteem on valesti projekteeritud
- Disainitud süsteem on ilma muudatuste sisseviimiseta ebaturvaline

Süsteemsed riskiallikad

- Süsteemi tööd on vaja pidevalt jälgida
- Süsteemis sisalduvat tarkvara on vaja uuendada
  Veaparandused, muud uuendused
- Enne uuendamist on vaja testida!

Testimine

- Uuenduse tulemusena võib tarkvara lakata töötamast
  - Ei sobi kokku vanema tarkvaraga
  - Andmefailide formaadid on muutunud
  - Nõuab lisatarkvara paigaldamist
  - Andmete ülekandel võivad tekkida vead

Süsteemsed riskiallikad

- Puudub valmisolek ebameeldivusteks
- Tagavarakoopiate puudumine
- Taastepunktide (*roll-back)* puudumine

Süsteemsed riskiallikad

- **Administraatori hoolimatus**
  Süsteemi haldamine on koormav kohustus

- **Administraatori ebakompetentsus**
  Ei tunne tarkvara ega süsteemi põhjalikult
  Ei käi uuendustega kaasas

Süsteemsed riskiallikad

- **Turvanõuete eiramine**
  Liiga lihtsad paroolid, süsteemis töötavad kasutud teenused (nt. ftp, www jne)

- Kasutud teenused võivad sisaldada turvaauke!