



Eesti Infotehnoloogia
Kolledž

Turvalisus

Linux (UNIX) algajale

Edmund Laugasson
edmund.laugasson@itcollege.ee

Käesoleva dokumendi paljundamine, edasiandmine ja/või muutmine on sätestatud ühega järgnevatest litsentsidest kasutaja valikul:

* GNU Vaba Dokumentatsiooni Litsentsi versioon 1.2 või uuem

* Creative Commons Autorile viitamine + Jagamine samadel tingimustel 4.0 litsents (CC BY-SA)

Mis seostub sõnadega IT ja turvalisus?

Turvalisus ja privaatsus

- *Need, kes on valmis oma vabadust ajutise turvalisuse vastu vahetama, ei vääri kumbagi.*
- *They who can give up essential liberty to obtain a little temporary safety, deserve neither liberty nor safety.*
 - Benjamin Franklin (18 saj)
 - <https://en.wikiquote.org/wiki/Freedom>
- Turvalisus (*security*) on pidev protsess (mitte seisund), mille eest peab pidevalt hea seisma
 - <http://www.linuxsecurity.com/>
 - <https://wiki.ubuntu.com/BasicSecurity>
 - <https://help.ubuntu.com/lts/serverguide/security.html>
 - <https://www.apple.com/support/security/>
 - <https://www.microsoft.com/en-us/security/default.aspx>



Turvalisus ja privaatsus

- Privaatsus (*privacy*)
 - Ubuntu: <http://www.ubuntu.com/legal/terms-and-policies/privacy-policy>
 - <https://fixubuntu.com/>
 - <https://help.ubuntu.com/community/GnuPrivacyGuardHowto>
 - <https://wiki.ubuntu.com/SecurityAndPrivacySettings>
 - <https://www.privacy-cd.org/> Ubuntu Privacy Remix
 - Apple: <https://www.apple.com/privacy/manage-your-privacy/>
 - <https://fix-macosx.com/> , <http://www.securemac.com/>
 - Microsoft: <https://account.microsoft.com/privacy>
 - Google: <https://www.google.com/settings/privacy>

Mitmekülgne maailm

- Turvalisus hõlmab endas mitmeid valdkondi:
 - Tarkvaralist, riistvaralist, füüsilist ja vaimset manipulatsiooni
- Kõike ei jõua lahata ega tõrjuda, aga oluline on arendada teadlikkust ning õppida ohte märkama, sest mida ei tea, seda ei saa ka ennetada!
- Turvalisus teadmatuses (*security through obscurity*) ei ole lahendus!
- Parem on turvalisus läbi hariduse (*security through education*)
- <https://defcon.org/>
- kui turvaline on salasõna <https://howsecureismypassword.net/>
- kas on häkitud <https://haveibeenpwned.com/>

Miks hoolida turvalisusest ja privaatsusest?

- Assapauk -
<https://www.youtube.com/playlist?list=PLjTBvsv2Ws0ja-ovwPAEfP8CY0clvFYMt>
- olulisemad rünnatavad väärtused:
 - identiteet: **identiteedivargus** (*identity theft*)
 - ressursid: kettaruum, andmesidemaht, ühenduskiirus
 - saladused: äri, isiklik
- <https://en.wikipedia.org/wiki/Cybercrime>
- <https://et.wikipedia.org/wiki/K%C3%BCberkuritegevus>
- <http://www.delfi.ee/teemalehed/kuberkuritegevus>
- <http://www.postimees.ee/teema/k%C3%BCberkuritegevus>
- <https://www.mkm.ee/et/tegevused-eesmargid/infouhiskond/kuberjulgeolek>

Miks hoolida turvalisusest ja privaatsusest?

- film “How Not to Lose Your Identity” (2007) (Bennett Arron)
 - IMDB: <http://www.imdb.com/title/tt1034313/>
 - <https://www.youtube.com/watch?v=-URDjwb0fS4>
 - intervjuu:
<http://www.zdnet.com/article/auscert-2011-firms-ignore-id-theft-risk/>
- film “Identity Theft: The Michelle Brown Story” (2004)
 - IMDB: <http://www.imdb.com/title/tt0430211/>
- film “Web Warriors” (2008)
 - IMDB: <http://www.imdb.com/title/tt2317542/>
 - <https://www.youtube.com/watch?v=I5PdtXD7Xzl>
- mitte ainult server(id) vaid ka *sysadmin*’i graafilise liidesega masina turvamine on osa turvalisusest
- [Security, privacy and why you don’t care | Reg Harnish | TEDxAlbany](#)

Statistika ja info

- RIA – Riigi Infosüsteemi Amet (*Information System Authority*)
 - <https://www.ria.ee/ee/kuberturve.html>
 - turvaintsidentidest teavitamine: CERT Eesti
 - <https://www.ria.ee/ee/cert.html>
 - vananenud tarkvara kasutamine on ohtlik
 - <https://www.ria.ee/ee/vananenud-tarkvara-kasutamine.html>
 - küberturvalisuse kokkuvõtted
 - <https://www.ria.ee/ee/kuberturvalisuse-kokkuvotted.html>
 - küberturvalisuse uudised
 - <https://www.ria.ee/ee/kuberturvalisuse-uudised.html>
 - ajaveeb (*blog*) <https://blog.ria.ee/>
- reaalajas <https://cybermap.kaspersky.com/>
- statistika <http://www.go-gulf.com/blog/cyber-crime/>



Tarkvaralised ründed

- **Heartbleed.com**
 - The Heartbleed bug allows anyone on the Internet to read the memory of the systems protected by the vulnerable versions of the OpenSSL software. (vt ka [Wikipedia artikkel](#))
- **IP-kaamerad**
 - Kes tegelikult neid pilte vaatab?
- **Miks katta kinni veebikaamera?**
 - [artikkel](#)
- **Krüptograafia ründed** (*cryptographic attacks*)
- üks võimalus lahenduseks:
 - riistvaraline turvamoodul (HSM *hardware security module*)



Riistvaralised ründed

- Riistvaraline klaviatuurinuhk (*hardware keylogger*)
- <https://www.keysniffer.net/>



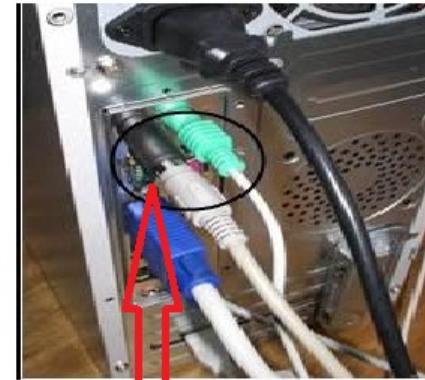
WITHOUT KEYLOGGER



WITH USB KEYLOGGER



WITHOUT KEYLOGGER



WITH PS2 KEYLOGGER

Füüsilised ründed

- füüsiline ligipääs võrkudele
 - kas võõras saab kaabliga oma arvuti võrku ühendada?
 - traadita võrkude eraldatus?
- <http://lockwiki.com/> , <http://lockpickingforensics.com/>
- eetilise häkker Walter Belgers
 - <https://www.youtube.com/watch?v=Fn6u9bKofkw>
- https://en.wikipedia.org/wiki/Physical_security
- “Kaotatud ja leitud” firma USB pulgad
- kodanikualgatused:
 - [USB Dead Drop](#), [PirateBox](#), [FreedomBox](#), [LibraryBox](#)

Vaimsed manipulatsioonid

- Me kõik oleme ainult inimesed!
- Kõik, mille ülesse panete, see sinna ka jääb... ja ärge arvake, et see ei huvita kedagi, kuna teil pole ju midagi varjata...
 - <https://www.youtube.com/watch?v=F7pYHN9iC9I>
- https://en.wikipedia.org/wiki/Social_engineering_%28security%29
- <http://www.social-engineer.org/>
- https://en.wikipedia.org/wiki/Human_security
- Nina all asjad jäävad ikka märkamata...
 - <https://www.youtube.com/watch?v=dy75GtKsOAw>
 - <https://www.youtube.com/watch?v=BjueOXCy3OM>

Lahendused...

- ... on olemas, aga selleks on vaja asjaga tegeleda
- Kõige vastu korruga ei saa, kuid tüüpvigu teades saab levinumaid ründeid ennetada
- ISKE on infosüsteemide kolmeastmeline etalonturbe süsteem, <https://iske.ria.ee/> , selle rakendamine on pidev protsess
- NB! Nõrgim lüli süsteemis on alati inimene – kasutaja või süsteemihaldur (*user error*):
 - *EBKAC Error Between Keyboard And Chair*



Lahendused...

- ISKE on infosüsteemide kolmeastmeline etalonturbe süsteem, <https://iske.ria.ee/> , selle rakendamine on pidev protsess
- *COBIT - Control Objectives for Information and Related Technologies*
- ITIL - IT haldamise tavade ja protsesside standardite kogu
- IT-halduse raamistike võrdlus
- https://en.wikipedia.org/wiki/Category:Information_technology_governance
- https://en.wikipedia.org/wiki/Category:Information_technology_audit

Küsimused?

Täna tähelepanu eest!

