



IT KOLLEDŽ
TALLINNA TEHNIKAÜLIKOOL

Turvalisus

Operatsioonisüsteemid ja nende haldamine ICA0001

Edmund Laugasson

edmund.laugasson@taltech.ee

https://wiki.itcollege.ee/index.php/User:Edmund#eesti_keeles

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

- *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>
 - <https://www.gnu.org/proprietary/>
 - <https://www.fsf.org/windows>

Privaatsus

- Privaatsus (*privacy*) - andmetele ligi pääsevad **ainult** asjaosalised
 - privaatsus: kes tegelikult ligi pääseb? Varukoopiad, e-post, andmekandjad (arvutis, võrgus, pilves, eemaldatavad (mälu-pulk, kõvaketas, optiline (CD, DVD, **Blu-Ray**, jne), vms väline andmekandja, jne))
 - 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>

Zero knowledge (ZK)

- sisuliselt tegemist privaatsuse teenuse põhimõttega – mitte keegi peale teie ei saa oma andmetele ligi: *usaldus on hõbe, ZK on kuld*
- operatsioonisüsteem: krüpteeritud paigaldus ([LUKS](#), [Bitlocker](#), [jne](#))
 - *Hacker howto*: [originaaltekst](#), [eestikeelne tõlge](#)
- tekst: Encipher <https://encipher.it/>
- pilvsalvestus:
 - <https://www.cloudwards.net/what-exactly-is-zero-knowledge-in-the-cloud-and-how-does-it-work/>
 - <https://www.cloudwards.net/best-zero-knowledge-cloud-services/>
 - <https://cryptomator.org/> - krüpteeri andmed pilvsalvestuses
 - <https://www.veracrypt.fr/en/Home.html> - krüpteeri andmed võrgukettal, arvutis
- e-post
 - ProtonMail: [turvateave](#), [.ch vs .com](#) + [ProtonVPN](#) (mitmepunkti-VPN, [Tor](#))
 - [GPG: Mailvelope](#) (veeb); [Thunderbird 78+](#); [OpenKeychain](#) + [FairEmail](#) (Android); [iPGMail](#) (iOS, ~2\$), [PGP Everywhere](#) (iOS, ~5\$)
 - veebilehitseja: [Brave](#) (sh [Tor](#))
 - <https://privacytools.io/>
- suhtlus:
 - [Cyph](#), [Keybase](#), [Signal](#), [Element](#), [Jami](#), [Jitsi Meet](#)

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/> - siin kehtib vaid sularaha (kes tahaks sellisel üritusel oma pangakaarti kasutada?)
- 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, andmesidemahut, 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=l5PdtXD7XzI>
- 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 teave

- RIA – Riigi Infosüsteemi Amet (*Information System Authority*)
 - <https://www.ria.ee/>
 - turvaintsidentidest teavitamine: CERT Eesti
 - <https://cert.ee/>
 - vananenud tarkvara kasutamine on ohtlik
 - <https://www.ria.ee/kuberturbe-nouanded/nouanded-internetikasutajale/vanenenud-tarkvara>
 - küberturvalisuse kokkuvõtted
 - <https://www.ria.ee/kuberturvalisus/kuberruumi-analuus-ja-ennetus/olukord-kuberruumis>
 - ajaveeb ((we)blog) <https://blog.ria.ee/>
- reaalaajas <https://cybermap.kaspersky.com/>
- statistika <https://www.go-globe.com/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/>



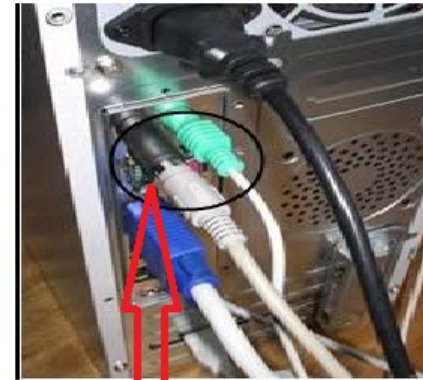
WITHOUT KEYLOGGER



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/>
- eetiline 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 korraga 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 etalon turbe süsteem (maht ~5000 lk), <https://iske.ria.ee/> , selle rakendamine on pidev protsess – kuni 2023.aasta lõpuni, ISKE asendub uue standardiga
- **E-ITS**: 31.12.2020 valmis, esimesed rakendajad 2021 lõpuks, üleminek tehtud 2022 lõpuks, iga aasta septembris uus versioon, kavas tööriista loomine, maht ~500 lk. [Lisateave](#).
- **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

Vahendeid saladuste hoidmiseks

- <https://cryptosteel.com/> - füüsiline saladuse säilitamine
- jne, <https://www.techradar.com/news/best-secure-drives>
- <https://bitwarden.com/> - vabavara, arvutis ja nutiseadmes
- FreeOTP <https://freeotp.github.io/>
- FreeOTP+ <https://github.com/helloworld1/FreeOTPPlus>
- https://en.wikipedia.org/wiki/Password_manager
- https://en.wikipedia.org/wiki/List_of_password_managers

SSH – Secure SHell

- SSH - turvaline võrguprotokoll opereerimaks üle ebaturvalise võrgu
- võimaldab klient-server arhitektuuri puhul luua turvalise andmeedastuskanali
- tavapärase port on 22/tcp (Linuxis: *grep -i ssh /etc/services*)
- MS Windows 10 build 1809, MS Windows Server 2019 kasutavad OpenSSH'd vaikimisi
 - Apps > Apps and Features > Manage Optional Features
 - OpenSSH Client / Server -> Install

https://en.wikipedia.org/wiki/Secure_Shell

<https://et.wikipedia.org/wiki/Turvakest>

https://docs.microsoft.com/en-us/windows-server/administration/openssh/openssh_overview

<http://enos.itcollege.ee/~edmund/materials/ssh/>

SSH ühenduse turvalisus



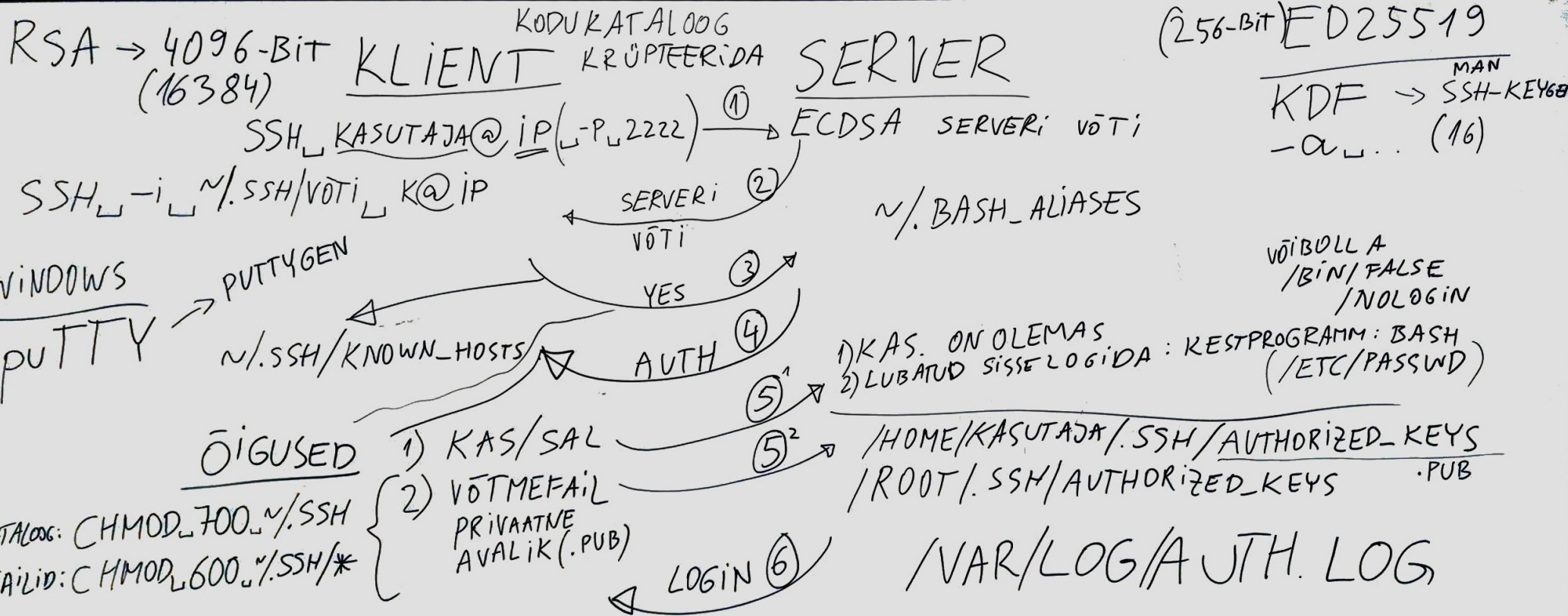
SSH ühenduse turvalisuse kontroll

- serveri paigaldamisel luuakse serveri võtmed
 - kontroll kohalikus masinas
 - *for i in /etc/ssh/*.pub; do ssh-keygen -lf \$i; done | uniq*
 - MD5 MS Windowsi jaoks (MD5 alates OpenSSH 6.8)
 - *for i in /etc/ssh/*.pub; do ssh-keygen -lf \$i -E md5; done | uniq*
 - pärimine üle võrgu
 - *ssh-keyscan host.example.org | ssh-keygen -lf -*
 - näiteks:
 - *ssh-keyscan enos.itcollege.ee | ssh-keygen -lf -*
 - juba siin näeme võtmeid ja kui valed siis probleem!

SSH ühenduse turvalisus

- enne serveriga ühendumist veenduda, et tegemist on serveriga, mida me arvame õige olevat
 - vt <https://enos.itcollege.ee/> avalehte
- ühendumisel nõustuda õige serveri võtmega, mis salvestatakse `~/.ssh/known_hosts`
- edaspidisel ühendumisel kontrollitakse `~/.ssh/known_hosts` failis asuva võtme sõrmejälge – serverivõtme muutumisel muutub ka sõrmejalg ja sellest antakse teada kui see ei klapi failis `~/.ssh/known_hosts` olevaga – seda hoiatust tuleb tõsiselt võtta ja mitte ühenduda enne kui on selge, miks serverivõti muutus

SSH ühendus



SSH ühenduse turvalisus

- kontrollime kas enos.itcollege.ee on usaldusväärsete serverite nimekirjas `~/.ssh/known_hosts`
 - `ssh-keygen -F enos.itcollege.ee #avalik võti ise`
 - `ssh-keygen -IF enos.itcollege.ee #SHA256 sõrmejälg`
 - `ssh-keygen -IF enos.itcollege.ee -E md5 #MD5 sõrmejälg`
 - failis `~/.ssh/known_hosts` on krüpteeritud kujul info masina kohta ja tema avalik võti, mille sõrmejäljega nõustuti esmakordsel SSH'ga ühendumisel
- vajadusel eemaldada enos.itcollege.ee avalik võti usaldusväärsete serverite nimekirjast `~/.ssh/known_hosts` juhul kui see seal on, et saaksime selle usaldamist kontrollida:
 - `ssh-keygen -R enos.itcollege.ee`

Viited

- <http://tarbija24.postimees.ee/4255919/need-50-telefonirakendust-varastavad-sinult-salaja-raha>
- <http://www.postimees.ee/4256285/kanada-veebileht-avaldas-eestlaste-kodused-aadressid-ja-telefoni-numbrid>
- <http://www.securityweek.com/14-million-phishing-sites-are-created-monthly-report>
- <http://www.securityweek.com/internet-providers-possibly-involved-finfisher-surveillance-operations-report>
- <https://www.bleepingcomputer.com/news/security/malware-uses-security-cameras-with-infrared-capabilities-to-steal-data/>
- <https://www.am.ee/Google-eemaldas-500-nuhkvaraappi>
- <https://thehackernews.com/2017/09/hacking-infusion-pumps.html>
- <http://securityaffairs.co/wordpress/62872/hacking/microsoft-kernel-issue.html>
- https://www.theregister.co.uk/2017/09/11/everybody_without_android_oreo_vulnerable_to_overlay_at_tack/
- <https://www.bleepingcomputer.com/news/security/bashware-malware-can-abuse-windows-10s-linux-shell-to-bypass-security-software/>
- <http://www.postimees.ee/4241009/tana-radaris-privaatset-kaamerapildid-eesti-kodudest-on-tervele-maailmale-nahtavad>
- <https://latesthackingnews.com/2017/09/06/750000-lenovo-laptops-spyware/>

Küsimused? Tänan tähelepanu eest!



IT KOLLEDŽ
TALLINNA TEHNIKAÜLIKOOL



TTÜ IT KOLLEDŽ

Raja 4C, 12616 Tallinn

tel +372 628 5800

info@itcollege.ee

<http://www.itcollege.ee/>



IT KOLLEDŽ
TALLINNA TEHNIKAÜLIKOOL

Turvalisus

Operatsioonisüsteemid ja nende haldamine ICA0001

Edmund Laugasson

edmund.laugasson@taltech.ee

https://wiki.itcollege.ee/index.php/User:Edmund#eesti_keeles

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)

1 / 23

Küsimused? Täna tähelepanu eest!



IT KOLLEDŽ
TALLINNA TEHNIKAÜLIKOO



TTÜ IT KOLLEDŽ

Raja 4C, 12616 Tallinn

tel +372 628 5800

info@itcollege.ee

<http://www.itcollege.ee/>