



Estonian Information
Technology College

Security

Operating systems 1800

Edmund Laugasson
edmund.laugasson@itcollege.ee

There has been used materials from Margus Ernits, Katrin Loodus when creating current slides.

Current document copying, distributing and/or modifying has been set out by one of the following licences by user's choice:

* GNU Free Documentation Licence version 1.2 or newer

* Creative Commons Attribution + ShareAlike licence 4.0 (CC BY-SA)

What connects with words IT and security?

Security and privacy

- *They who can give up essential liberty to obtain a little temporary safety, deserve neither liberty nor safety.*
 - Benjamin Franklin (18th century)
 - <https://en.wikiquote.org/wiki/Freedom>
- *Security* is a constant is a continuous process (not a state), which needs continuous attention
 - <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>

Security and privacy

- *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>

Versatile world

- Security involves several areas:
 - A software, hardware, physical and mental manipulation
- Everything can not be dissected and repulsed, but it is important to develop an awareness of the dangers and learn to recognize them. If you do not know, it can not be prevented!
- *Security through obscurity* is not a solution!
- Better is *security through education*
- <https://defcon.org/>
- how secure is your password (remember the time factor!)
<https://howsecureismypassword.net/>
- whether it is hacked <https://haveibeenpwned.com/>
- <http://www.catb.org/esr/faqs/hacker-howto.html>

Why to care about security and privacy?

- Assapauk (in Estonian some attack vectors, government project) - <https://www.youtube.com/playlist?list=PLjTBvsv2Ws0ja-ovwPAEfP8CY0clvFYMt>
- attacked important values:
 - identity: *identity theft*
 - resources: disk space, data volume, connection speed
 - secrets: business, personal
- <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>
- <https://www.mkm.ee/en/objectives-activities/information-society/cyber-security>

Why to care about security and privacy?

- the movie “How Not to Lose Your Identity” (2007) (Bennett Arron)
 - IMDB: <http://www.imdb.com/title/tt1034313/>
 - <https://www.youtube.com/watch?v=-URDjwb0fS4>
 - interview:
<http://www.zdnet.com/article/auscert-2011-firms-ignore-id-theft-risk/>
- the movie “Identity Theft: The Michelle Brown Story” (2004)
 - IMDB: <http://www.imdb.com/title/tt0430211/>
- the movie “Web Warriors” (2008)
 - IMDB: <http://www.imdb.com/title/tt2317542/>
 - <https://www.youtube.com/watch?v=I5PdtXD7Xzl> (also here)
- not only the server(s), but also a sysadmin'i machine with graphical interface safety is part of security
- [Security, privacy and why you don't care | Reg Harnish | TEDxAlbany](#)

Statistics and information

- RIA – State Information System Authority
 - EST <https://www.ria.ee/ee/kuberturve.html>
 - ENG <https://www.ria.ee/en/ciip.html>
 - announcing about syber incidents: CERT Estonia
 - EST <https://www.ria.ee/ee/cert.html>
 - ENG <https://www.ria.ee/en/cert-estonia.html>
 - Using outdated software is dangerous (in Estonian)
 - <https://www.ria.ee/ee/vananenud-tarkvara-kasutamine.html>
 - IT baseline security system ISKE
 - ENG <https://www.ria.ee/en/iske-en.html>
 - EST <https://www.ria.ee/ee/iske.html>
 - publications in cyber security
 - EST <https://www.ria.ee/ee/kuberturvalisuse-kokkuvotted.html>
 - ENG <https://www.ria.ee/en/publications.html>
 - cyber security news
 - EST <https://www.ria.ee/ee/kuberturvalisuse-uudised.html>
 - blog in Estonian <https://blog.ria.ee/>
- in real time <https://cybermap.kaspersky.com/>
- statistics <http://www.go-gulf.com/blog/cyber-crime/>

software attacks

- **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. (see also [Wikipedia article](#))
 - in Ubuntu: *sudo apt update && sudo apt install openssh-blacklist**
- **IP cameras**
 - Who really examine these pictures?
 - search: “*attacker surveillance IP cam*”
- **Why to cover a web cam?**
 - [an article](#)
- **Cyptographic attacks**
- One optional solution:
 - HSM *hardware security module*



software attacks

- one simple test:
 - search from Internet “fast and easy hacking”
- results?

The screenshot displays a Metasploit Meterpreter session. On the left, a file explorer shows the following structure:

- auxiliary
 - admin
 - http
 - tomcat_administration
 - tomcat_utf8_traversal
 - scanner
 - http
 - tomcat_enum
 - tomcat_mgr_login
 - exploit
 - multi
 - http
 - tomcat_mgr_deploy

The central console shows a network diagram with a root node at 192.168.1.104 (NT AUTHORITY\SYSTEM @ ACME-14E429D2B5 (ADMIN)) and three target nodes: 192.168.1.101 (Apple), 192.168.1.106 (Linux), and 192.168.1.108 (Windows). A context menu is open over the Windows target, showing options like Attack, Login, Meterpreter, Services, Host, Access, Interact, Explore, Pivoting, MSF Scans, and Kill. The Explore option is selected, showing a sub-menu with Browse Files, Show Processes, Key Scan, and Screenshot.

The bottom console shows the file list for C:\:

D	Name	Size	Modified	Mode
	Documents and Settings		2010-02-14 22:22:02 -0500	40777/rwxrwxrwx
	Inetpub		2010-02-14 22:16:37 -0500	40777/rwxrwxrwx
	Program Files		2010-10-04 10:13:32 -0400	40555/r-xr-xr-x
	Python25		2010-09-29 09:43:01 -0400	40777/rwxrwxrwx
	System Volume Information		2010-02-14 22:21:33 -0500	40777/rwxrwxrwx
	WINNT		2010-10-04 11:19:56 -0400	40777/rwxrwxrwx
	lcc		2010-09-29 12:38:25 -0400	40777/rwxrwxrwx
	learn		2010-10-16 20:02:11 -0400	40777/rwxrwxrwx
	srtFtpLogs		2010-09-30 16:04:14 -0400	40777/rwxrwxrwx
	AUTOEXEC.BAT	0b	2010-02-14 22:17:24 -0500	100777/rwxrwxrwx
	CONFIG.SYS	0b	2010-02-14 22:17:24 -0500	100666/rw-rw-rw-
	IO.SYS	0b	2010-02-14 22:17:24 -0500	100444/r--r--r--
	MSDOS.SYS	0b	2010-02-14 22:17:24 -0500	100444/r--r--r--

hardware attacks

- hardware keylogger
- <https://www.keysniffer.net/>



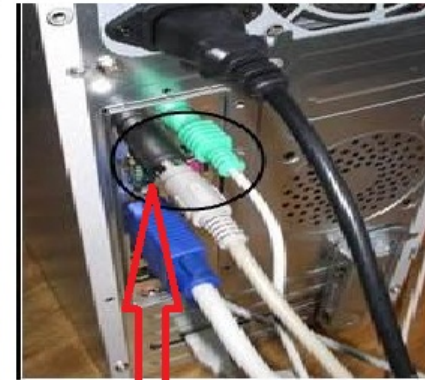
WITHOUT KEYLOGGER



WITH USB KEYLOGGER



WITHOUT KEYLOGGER



WITH PS2 KEYLOGGER

physical attacks

- Physical access to the network
 - the stranger can connect the cable to your computer network?
 - Wireless networks separateness?
- <http://lockwiki.com/> , <http://lockpickingforensics.com/>
- ethical hacker Walter Belger
 - <https://www.youtube.com/watch?v=Fn6u9bKofkw>
- https://en.wikipedia.org/wiki/Physical_security
- "Lost and Found" company USB sticks
- Citizens' initiatives:
 - USB Dead Drop, PirateBox, FreedomBox, LibraryBox

Mental manipulations

- We are all just humans!
- All that you upload to Internet, it will remain there ... and do not think that this does not interest anyone, because you do not have nothing to hide ...
 - <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
- Under the nose of the things still remain unnoticed ...
 - <https://www.youtube.com/watch?v=dy75GtKsOAw>
 - <https://www.youtube.com/watch?v=BjueOXCy3OM>

Solutions...

- ... are there but needs attention
- you cannot solve everything at once but knowing typical mistakes there can be common attacks avoided
- NB! The weakest link in the system is always a person - a user or system administrator (*user error*):
 - *EBKAC Error Between Keyboard And Chair*



Solutions...

- ISKE is the three step baseline level security system for information systems, (EST <https://iske.ria.ee/>), applying this is a constant and continuous process
- **COBIT** - *Control Objectives for Information and Related Technologies*
- **ITIL** - IT management practices and standards throughout the process
- **IT management frameworks comparison**
- https://en.wikipedia.org/wiki/Category:Information_technology_governance
- https://en.wikipedia.org/wiki/Category:Information_technology_audit

Questions?

Thank you for your attention!

