

TIES327 – Network Security (3-7 ECTS)

L1: Introduction to the networking security



DELETED FROM TRINITY

HACKING

Prof. Timo Hämäläinen
timo.t.hamalainen@jyu.fi
IT Faculty
University of Jyväskylä

Some Malware&attack statistics

Malwares:

- <https://www.av-test.org/en/statistics/malware/>

Realtime Attack Trackers:

- <https://www.secureworld.io/industry-news/6-live-cyber-attack-maps>

Securelist by Kaspersky:

- IT threat evolution in Q2 2022
 - <https://securelist.com/it-threat-evolution-q2-2022/107099/>
- DDoS Report Q2 2022
 - <https://securelist.com/ddos-attacks-in-q2-2022/107025/>

TRAFICOM

- <https://www.kyberturvallisuuskeskus.fi/en/>

What is security ?

- The overall objective is to ensure that the information systems will always do to what their purpose is, and nothing more
- The aim is also to protect the systems from the expected and the unexpected risks and threats
- Security is also always the balancing of security level and usability
- Paranoia can be a good thing, but one must rely on something
 - Often, this means that at least we can trust eg. to the system administrators
 - So keep administrator staff satisfied 😊

Objectives of Security (CIA)

- **Confidentiality**
 - Aims to limit the information only to those who are right to use it
- **Integrity**
 - Goal to prevent unauthorized data modification by the user
- **Availability/usability**
 - Aim to guarantee the availability of the IT- systems, networks, etc. whenever the user has the right to use those
- From these objectives can be derived other goals:
 - Authenticity
 - Indisputable
 - Acces control

What kind of systems are protected ?

■ Everything !

- Banks, hospitals, armed forces, e-shops, homes
- Different environments require different degrees of data security
- Different environments call for different requirements and challenges for data security
- Now there is a network connection for each pocket, IoT-devices etc., so the security is carried out in the same places
- There has already been for a “long” time more other IP devices than PCs

What can be lost ?

- Knowledge capital (IPR, protection depends on value of the information)
 - Lost
 - Changed
 - Leakage to a competitor

- Reputation
 - Because of this, companies rarely tell, that they have been under attack
 - "defacements" changing web- pages
 - Hacked machines can be used in other attacks => the organization can be accused of the attack

What can be lost ?

■ Money

- Phising, email forwarding&monitoring, fake invoices => money to the criminals
- Blackmail eg. With customer's personal information of e-shop or bank
- Working time losses => wasted money for company

■ Time

- Admin time for cleaning the computers
- Working time losses due to eg. Network breaks

Who or what is threatening ?

- Careless users
- Device faults, cable/electricity breaks etc.
- Burglars
- Unhappy workers
- Attacks from the outside (Internet)
 - Script kiddies
 - organized cybercrime [FBI's term]
 - Industrial spying
 - Terrorism
- Does security companies dramatize threats ?
 - Very old example: Symbian Community blamed one virus making company for overstating symbian-virus threats

Why threats (motive)?

- Almost always **The** reason is money
 - Selling R&D information to competitors
 - Selling hacked machines forward to eg. To spam- servers
 - Selling identity is world wide problem
 - Credit card details
 - Email addresses (spam purposes)
- It is argued that, for example, banks have been tightened large sums of money from the stolen customer data
- Challenges, adventures, reputation in hacker networks
- Revenge
 - nickname- fight in some can be led to DDoS attack 😊
 - Malcontent worker

How to gather data for the attack: port scanning

- <http://nmap.org/>
- <https://tools.kali.org/information-gathering/nmap>
- Netstat, tcpdump
- Shields up from Gibson Reserach Co.
 - <https://www.grc.com/x/ne.dll?bh0bkyd2>

And other FREELY available tools. Just explore ;)

How to gather data for the attack: Social Engineering

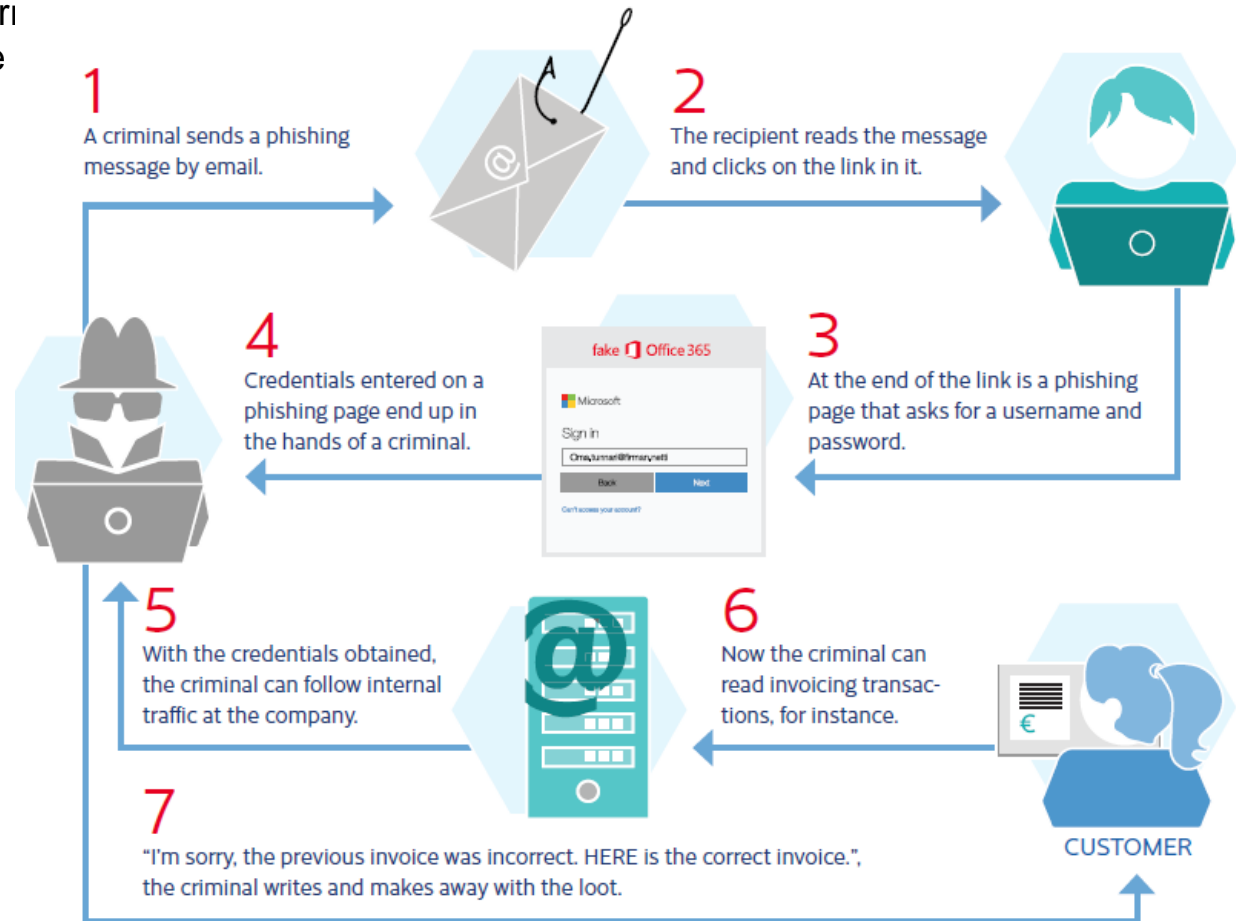
- At the most cases easiest way to get access to the closed systems
- Footprinting
 - Collect information before the attack
 - Dumpster diving
- Phone calls
 - Act as a security chief
 - Helpdesks often quite vulnerability (workers unpaid and uneducated)
- Checking desktops (userid/passwd written into desk)
- Book in <https://jyu.finna.fi/?lng=en-gb>: [Hacking the Human: Social Engineering Techniques and Security Countermeasures](#)

How to gather data for the attack: Phishing

- Phishing email messages, websites, and phone calls are designed to steal money.
- Cybercriminals can do this by installing malicious software on your computer or stealing personal information off of your computer.
- Cybercriminals also use social engineering to convince you to install malicious software or hand over your personal information under false pretenses.
- They might email you, call you on the phone, or convince you to download something off of a website.
- **Real example:** The company's Office 365 cloud service was hacked by means of phishing. Messages containing a link to a phishing site were sent to two of the company's employees. The criminals monitored the company's emails for several months and made changes to email forwarding without the company knowing. Financial company A did not know how long its emails had been monitored or what information had potentially leaked. In addition, the criminals tried to use fake invoices to make the company transfer funds to their account. The criminals used information obtained from monitored emails to prepare these fake invoices, attempting to make the invoices look as real as possible.

How to gather data for the attack: Phishing

- Real example:** The company's Office 365 cloud service was hacked by means of phishing. Messages containing a link to a phishing site were sent to two of the company's employees. The criminals monitored the company's emails for several months and made changes to email forwarding without the company knowing. Financial company A did not know how long its emails had been monitored or what information had potentially leaked. In addition, the criminals tried to use fake invoices to make the company transfer funds to their account. The criminals used information gathered from the phishing site to attempt to make



What does a phishing email message look like?

Hello!

As part of our security measures, we regularly screen activity in the Facebook system. We recently contacted you after noticing an issue on your account.

Spelling

Our system detected unusual Copyrights activity linked to your Facebook account , please follow the link bellow to fill the Copyright Law form:

http://www.facebook.com/application_form

Links in email


Note: If you dont fill the application your account will be permanently blocked.

Threats

Regards,

Facebook Copyrights Department.


Popular company

Nordea **Netbank** 

In English www.nordea.fi

Please be very attentive filling the fields to avoid errors.

Please enter your user ID, type of account and e-mail address in this field.

 Customer number:

Account Type: Choose

E-mail:

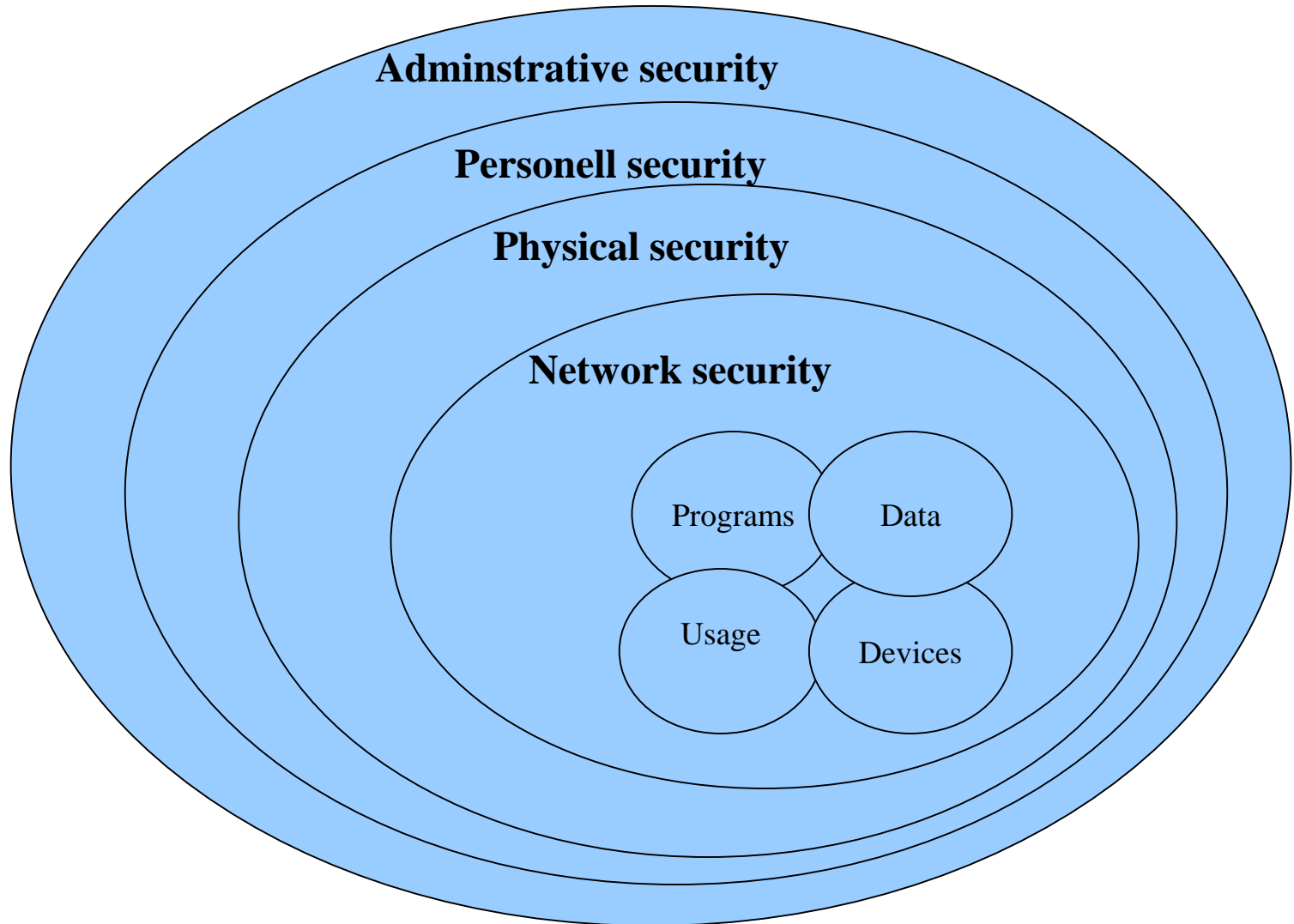
Please enter unused passwords in this field. Please note that passwords should be indicated in direct order starting with the FIRST unused one. For example: If you used 11 passwords you should indicate 4 passwords starting with the twelfth one (12, 13, 14, 15) in the form.

= = = =

You should indicate your payment confirmation codes here. Letter of the form should correspond to the letter in your code chart.

A	=	<input type="text"/>	F	=	<input type="text"/>	L	=	<input type="text"/>	R	=	<input type="text"/>
B	=	<input type="text"/>	G	=	<input type="text"/>	M	=	<input type="text"/>	S	=	<input type="text"/>

Sub-areas of the security- Onion model



Administrative Security

- Organization's security guidelines
- Creating a safe practices
- Security policy
- Business conduct guidelines and local regulations.

Personell Security

- Personnel-related security risks
- Human precautions
- Staff training and guidance
- Working tasks / responsibilities
- User rights
- **Voice:** Private branch exchange phone system, voice gateways, voice mail services and instant messaging.

Physical Security

- Physical protection of the buildings and rooms
 - Server/device rooms

- Access control
 - Firewall doesn't help, if you can access to the device room and take a server with you...

- One big physical security risk is laptops, memory sticks, mobile devices
 - Steal
 - Forget somewhere
 - Data deletion after usage
 - We can't trust physical security of these devices

Networking Security

- All aspects related to data transfer, design and building of data networks
- Local area network switches, routers, firewalls, wireless, intrusion prevention systems, remote access servers, protocols, network operating systems (OS) and wide area networks.
- Often this is the most invested in
- It includes:
 - Application security
 - Data security
 - Usage security
 - Device security
- Endpoint Devices: Printers, scanners, desktops, laptops, tablets and smartphones.

Different levels of the security

- ***The chain is as strong as its' weakest point***
- Often this weakest point is normal user
- We can't trust only to the one level, because applications and operating systems are full of vulnerabilities (you'll heard about those daily).
- See eg Firefox: <http://www.mozilla.org/security/known-vulnerabilities/>

Security Policies

- What are those ?
- Why we need them ?
- Are those "just antoother instructions" ?
- Related standards and RFCs
- What kind of things are included ?

Security Policy

- ... is document made by organization's management
- ... is formal rule set, which defines how organization's material should be used and covered by the personell
- ... shows goals of the practical security solutions
- ... shows how and what purposes users can use organization's devices, network and applications
- ... gives the possibility to punish from misusing

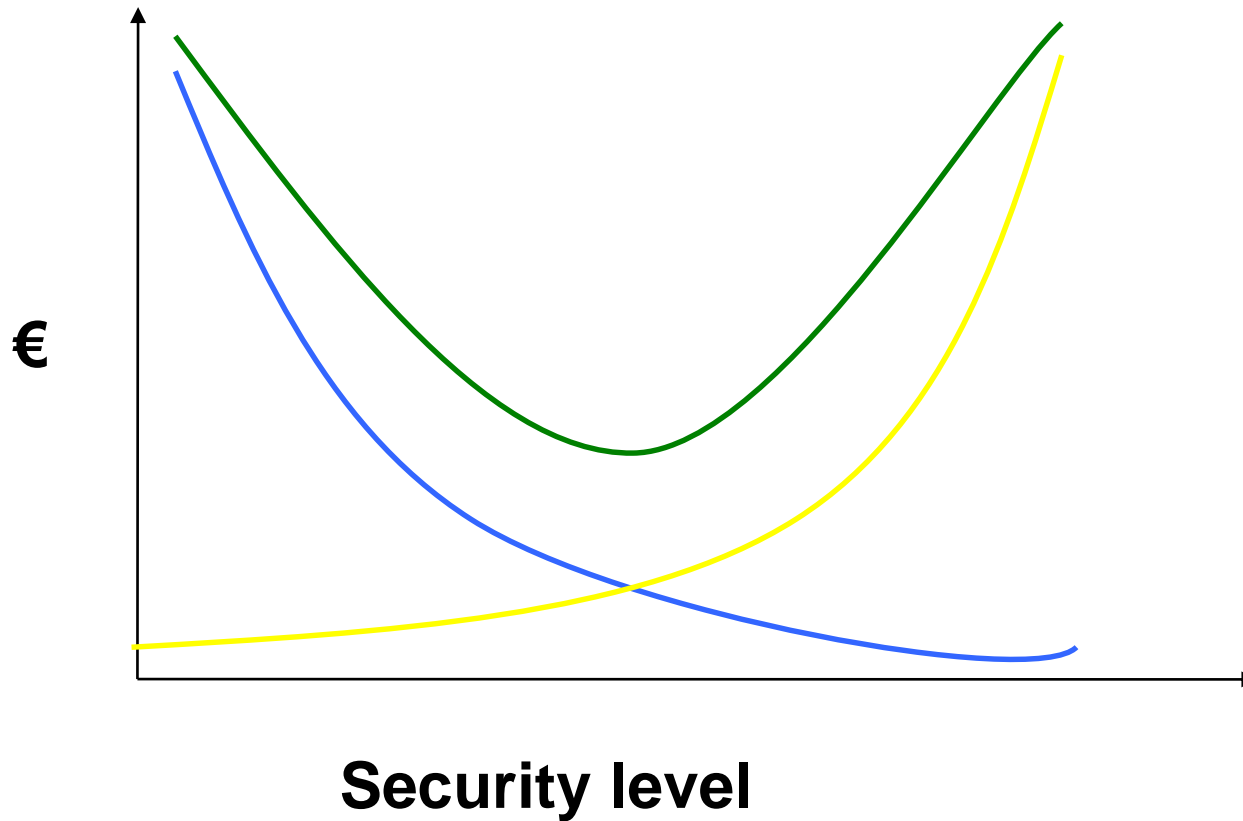
Estimation and analysis of risks

- In order to deploy security policy deep estimation of risks should be evaluated
- It includes estimation of the capital and risks
 - Identifying the covered targets
 - Devices, applications, data, ...
 - Peoples, documentation, archives, ...
 - Identifying threats
 - Unauthorized access to the confidential information
 - Showing confidential information
 - Preventing availability of the services

Risk calculations

- When the protected targets and threats have been estimated, can be moved to the risk calculation
- Thumb rule: do not pay more to the security than what is the real value of the protected information
- The goal is to optimize the total costs of the security
- Simplified model for the risk calculation:
 - Calculate costs, which the threat will cause if it realizes
 - Calculate costs, which are needed to protect
 - Conclude from the difference is it worth of protect
- Real life risk calculations are/might be much more complex

Risk calculations



- Damage cost
- Protection cost
- Total cost

Good security policy is

- ... can be implemented
- ... possible to confirm with the security tools and devices
 - If this is not possible, define sanction from the misuse
- ... defines clearly responsibilities inside the organization

Content of the security policy

- Instructions for delivering new devices and applications
- Privacy policy concerning at least: email, www- surfing etc.
- Acces control, user rights
- Policy for identification users
- Issues related to availability, users expectations for the services
- Administration policy, who and how can access to manage devices and services
- Misusing- notification policy, how to report misusing and to whom
- Audit policy
- + many many organization's spesific issues..

Content of the security policy

- The security policy does not itself contain any device/application specific rules
- Based on the policy, more concret technical documents are written in order to implement the policy
- These instructions can include the following documents:
 - Introduction of new desktops and servers
 - Maintenance of the network devices
 - Management of user accounts
 - Configurations of Firewalls
 - Configurations of WLANs
 - Etc..

Compromises of the security policy

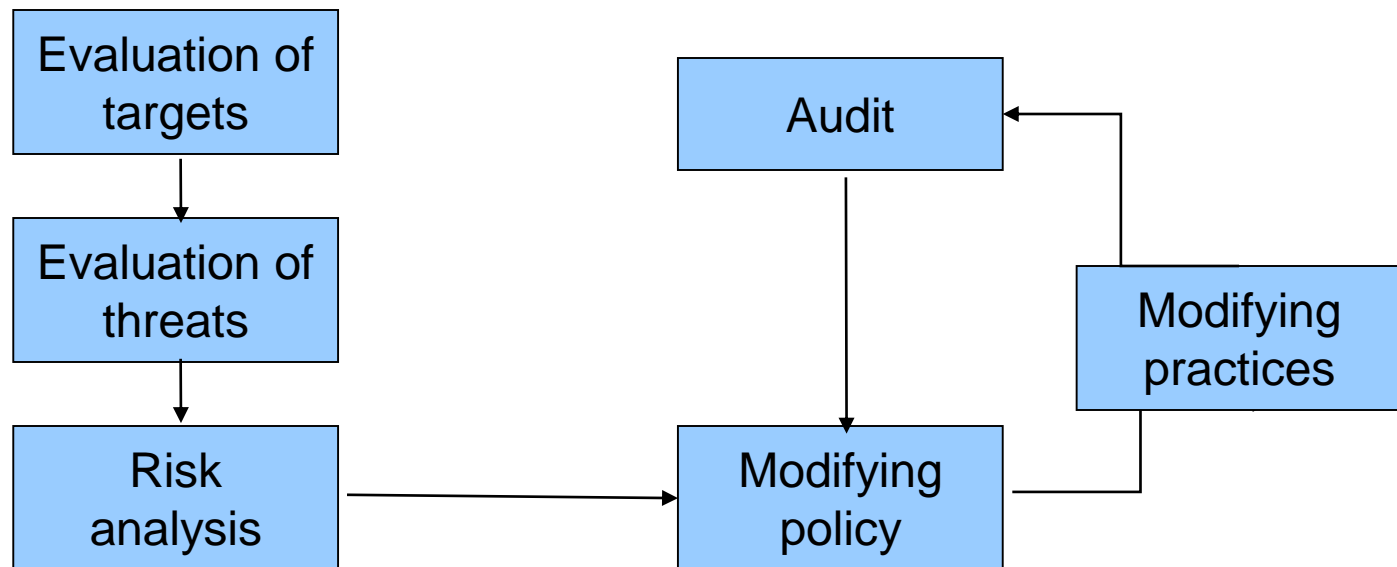
- There are always security risks when offering services
 - Administration staff should analyze risks against usefulness of the
 - Easiness of use or security
 - Roughly saying usability and security are almost vice versa with each other
 - For example 50 characters long passwords are quite secure, but difficult to remember
- Cost efficiency
 - Security devices, programs and other solutions will always cost something (money, time, performance, ...)
 - Again one has to analyze risks against the cost of solutions

Security policy (standards and RFC:t)

- "Site Security Handbook", RFC 2196, IETF.
 - Basic instructions (old, Sept. 1997, but has good points)
 - <http://tools.ietf.org/html/rfc2196>
- ISO/IEC 27001
 - Standardized instructions for the security policy
 - Describes in detail the whole process
 - Makes possible to external audit and if it is succesful get certificate. Then organization can show to others it has proper security solutions to its partners

Security process

- Security policy should be flexible, so it can be adapted to the new, unknown, situations fastly (in general level enough)
- In the other hand it should be possible to change the policy if needed



Audit

- Testing the security policy
 - Interviews
 - Scanning weak points
 - Checking settings of the operating systems and applications
 - Analyses of the network drives
 - In practice all inside the policy and even more
- The testers know organization's IT –systems and compare it against to the policy
- Can be executed
 - internally
 - Externally (consult)
- Different than penetration testing, where one tests only one resource without knowing organization's IT- system. Eg. Service attack outside from the Internet

Security violations

- Security violation is the case with any organization, individual, or other information integrity, availability or confidentiality of legally changed
- **NCSC-FI** handles violations in Finland
 - <https://www.kyberturvallisuuskeskus.fi/en/>
- Recovery plan should be in the policy
- Police can start investigation if there is crime situation or proper wants it

Sorting out security violations

- There exist companies who are doing this
- They are looking for evidences against IT criminals
- Hard work and expensive
- Most of the cases do not even attempt to trace

Recovering from the violation

- Normal user should contact immediately to IT- support
- First must be solved is it really violation
- Checking logs, processes etc.
- Sorting out if any information lost or modified
- Repairing the security holes (normally clean to whole computer)
- Try to contact to the organization where the attack came
- Contact to the organization where the attack hit

Security legislation


- Central crime police has IT- crime specialized investigation group
- IT security issues in settings and laws
- IT related violations crimes are:
 - Security violation (fine or jail max. 1 year)
 - Illegal use (fine or jail max. 1 year)
 - Sabotage (fine or jail max. 1 year)
 - Outrageous violation of communication security (max. 3 years jail)
- Office of the communication controls obeying the law of electrical communication

★ Some scary IoT security scenarios that could unfold in the not too distant future:

- You enter your house, and the thermostat is set to 120 degrees. An email arrives in poorly written English asking for \$500 to return control of your home heating system.
- It's not all that far-fetched, as a trio of University of Central Florida researchers demonstrated at BlackHat 2014 (<https://www.blackhat.com/>) by hacking into the [Nest Learning Thermostat](#).
- In less than 15 seconds, they showed how an attacker can remove the Nest from its mount, plug in a micro USB cable, and backdoor the device, unbeknownst to the owner.
- The compromised Nest could be used to spy on the home, attack other devices on the network, or steal wireless network credentials.

Some scary IoT security scenarios that could unfold in the not too distant future:

- If you are in the market for the least hackable car this year, your best bet is the Audi A8, according to automobile vulnerability researchers Charlie Miller and Chris Valasek.
- Miller and Valasek's [latest study](#) looked for ways a hacker could access the car's network by breaking into its wireless-enabled radio, for instance, and issuing commands to the automated steering, parking, braking, or driving mechanisms.
- The research is bad news for owners of a 2014 Jeep Cherokee, a 2014 Infiniti Q50, or a 2015 Escalade.
- Yes, your car has cool, state-of-the-art network technology. But it's also most likely to get attacked via Bluetooth, telematics, or the onboard phone app.



Some scary IoT security scenarios that could unfold in the not too distant future:

- Hackers are finding new ways to exploit smartphones through apps, photos, videos, social media, and GPS.
- The most recent example of photos becoming a target: Thousands of photos and videos from the Snapchat service were put online, apparently taken from sites such as Snapsaved.com, which, according to news reports, allowed people to log in using their Snapchat username and password to offer access to the site -- and also the chance to store photos meant to be deleted within seconds of being viewed.
- This year, owners of Mac and iOS devices found their iPhones and iPads held for ransom through a hack that targeted Find My iPhone and Find My Mac to trigger a remote lock of the device.

Some scary IoT security scenarios that could unfold in the not too distant future:

- Security researchers Billy Rios and Terry McCorkle warn that a widely deployed TSA carry-on baggage scanner could be easily manipulated by a malicious insider or outside attacker to sneak weapons or other banned items past TSA airport checkpoints.
- Among the blatant security holes: storing user credentials in plaintext and a feature that could project phony images on the X-ray display.
- Rios has also flagged weaknesses in two TSA detection systems at San Francisco International Airport.
- One of the systems included 6,000 Kronos time clocks open on the public Internet, two of which also are deployed at other US airports.



Some scary IoT security scenarios that could unfold in the not too distant future:

- Researchers are identifying holes in [satellite ground terminal equipment](#) that could be used to disrupt communications to ships, airplanes, and military operations.
- Ruben Santamarta, principal security consultant with IOActive, showed this year that an attacker could compromise the satellite systems, run malware, install malicious firmware, and even send a phony SMS text to trick a ship to follow a certain path or to rescue another ship.
- In the air, Santamarta said, an attacker could gain control over subsystem interfaces by taking advantage of the weak password reset feature, hard-coded credentials, or insecure protocols in cockpit communications.



7 scary IoT security scenarios that could unfold in the not too distant future:

- The threat scenario surrounding medical devices would be a patching problem with an embedded device (like a pacemaker) or a malware infection on network-connected equipment such as pregnancy monitors, insulin pumps, or MRI picture storage.
- Though researchers have been raising security concerns about these devices for some time, the [US Food and Drug Administration](#) has only recently begun to address the problem.

Summary

- Take into account all the levels of security
- The weakest link orders the level
- Attacker goes there where the lowest wall is
- Security policies make things clearer and give better total view
- Value of the information tells the security level
- Security is always a compromise between cost, security and usability

Links

- IT Security Standards and Best Practices
 - <https://www.infosec.gov.hk/english/technical/standards.html>
- Phishing
 - <https://apwg.org/>
 - <http://www.millersmiles.co.uk/>
- IT- legislation in Finland
 - <https://www.kyberturvallisuuskeskus.fi/en/our-activities/regulation-and-supervision>
- Vulnerabilities
 - <http://www.securityfocus.com>
- Advanced Persistent Threat service example
 - <https://www.secureworks.com/capabilities/threat-intelligence/advanced-threats>