



The Basics of Computer Security

Gollmann 1-2



What is Security?

- Security serves the purpose of
 - Protection of the value of assets from various threats
 - Compliance with laws and regulations
- Assets may be material and immaterial
 - Equipment, people, source code, reputation
- Besides the organization's own interests security might protect the interests of customers, personnel and society
- This course focuses on an area of security known as **information security** and its technologies
 - Not physical, corporate, operations or people security
- Suomeksi: turvallisuus ja tietoturvallisuus



Basic Concepts

- Some basic concepts are needed to understand security and to define what is being done
- These concepts are needed to understand the discourse of the profession



- The secrecy of information is a concept traditionally associated with security
- Means that only authorized entities (usually people, but also computers or software) have or can acquire knowledge of the contents of some data
- The need for confidentiality is a property related to the information, meaning that the confidentiality requirement is not associated with a certain computer, but the information that is processed in it
- Example: the medical records of a person are usually considered confidential
- Suomeksi: luottamuksellisuus



- Integrity is often more important than confidentiality
- Means that only authorized entities can **change** the information or that the information can only be changed through an approved process
- Also means often that the information entered to the system must be correct or from an approved source
- Example: The integrity requirement for a person's radiation treatment record is much more important than the confidentiality requirement
- Suomeksi: eheys, myös muuttamattomuus



- Means that information or a service is available to be used
- As a property more related to the system than to the information
- Example: at an emergency room the requirement of availability of a person's medical records is greater than the confidentiality requirement
- Suomeksi: saatavuus, käytettävyys (eri asia kuin käyttöliittymien käytettävyys)



- The CIA (Confidentiality, Integrity, Availability) model is commonly used to model the requirements for a system or organization's processes
- It is important to understand that these three requirements are inherently somewhat contradictory and the solution must create a balance
 - Data can be stored in a bank vault, but then it is not available to be used
 - Thus for most security situations there is no correct answer, but the designer must weigh the different needs and strike a balance
 - And the cost must be in relation to the value of what is protected



Accountability, Non-repudiation

- Accountability means that we can know afterwards **who** did **what**
 - Example: log files
- Non-repudiation means that we can prove it afterwards to others
 - Example: electronic signatures on documents
- Suomeksi: vastuullisuus ja kiistämättömyys



Identification, Authentication, Authorization

- Identification means that we recognize an entity
 - Example: a cookie in a web browser
- Authentication means that we verify the identity
 - Example: ask for a password
- Authorization means that an entity has the right to perform an action
 - Example: having access to your own files, not having access to /etc/passwd
- Suomeksi: tunnistaminen, todentaminen ja oikeutus (valtuuttaminen)



Anonymity, Pseudonymity, Privacy

- Anonymity, nobody knows who you are
 - Example: Surfing the web through a proxy with cookies turned off
- Pseudonymity, you can be identified, but the identification can not be connected to the real person
 - Example: Nicknames on an discussion forum
- Privacy, the confidentiality of your personal information, including your identity and location
 - Example: in Europe a company may not sell your address information without your approval
 - Privacy is both a political and a technical issue
- Suomeksi: anonymiteetti, pseudonymiteetti, tietosuoja



General Actors for Security Discussion

- These names are often used to refer to certain roles in the literature
 - Alice, Bob, Carol, Dave, Ellen, Frank...: participants
 - Eve: eavesdropper
 - Mallory: malicious active attacker
 - Trent: trusted third party
 - Victor: verifier, signs keys
- Other names may also be used, these are from Bruce Schneier's Applied Cryptography
- Part of the common security discourse, Alice and Bob are always sending messages to each other



- An asset is something that has value
 - Trained people, computers, patents, reputation
- In information security we focus mostly on intangible assets
 - A computer might cost \$1000, the source code in it might have cost \$100 000 to develop
 - In a typical company the computer might be listed on an equipment register, nobody knows for sure where the source code is located and who is responsible for it
- Suomeksi: "asset" ei käänny aivan suoraan, omaisuus on lähin termi, mutta konsepti on laajempi, "kaikki millä on arvoa"



Threat, Vulnerability, Risk

- A threat is a potential for something harmful to happen
 - Example: eavesdropping to our e-mail, a hard disk breaking
- Vulnerability implies a weakness in protection
 - Example: our e-mail goes through the unprotected computer classroom network, we don't have backups
- Risk, the expectancy of a threat
 - Likelihood of threat happening * value of damage
 - The likelihood of a hard disk breaking is perhaps 0.1 yearly, damage depends on the value of data and existence of backups
- Suomeksi: uhka, haavoittuvuus, riski



- Information and systems can be classified based on the security requirements (CIA-model, threats)
 - Example: the direct telephone number of the company president: "company confidential", not to be revealed to outsiders (threat: some disturbance to the president)
 - Example: Finnish military plans for opposing the invasion from Antarctica: "top secret" (threat: losing the independence of a nation)
 - Classification provides labels to the information
- Clearance is the classification for users to access information
- Suomeksi: luokittelu, luokittelu



Organizational Security and Security Policy



Organizational Security

- Information security is part of the overall security for a company or an organization
- There are several definitions for the subcategories for security and these are usually different for corporations and government organizations



Division of Corporate Security

- This is one way to divide the work:
- Protection
 - Physical security
 - People security
 - IT security
 - Operational security
- Assets
 - People
 - Information
 - Material (physical assets)
 - Reputation
- Security management coordinates all protection



Security Management

- Current wisdom is that there should be one point where the security is managed
 - An management group or a person
 - Otherwise there will be cases, where the protection for information depends too much on weather it is on paper or in a computer
- Security management is focal in creating a security policy
- Security management needs the support of organization's management or it can not function
- Suomeksi: turvajohto, turvahallinto

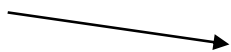


- The security policy document is the cornerstone for organization's security
 - A high level document and not always detailed enough to be practical for all staff
 - Must be renewed regularly
- It sets the goals for security work
- The assets to be protected are defined in this document
- Acceptable risk is defined
- Protection principles are defined
- Resources can be allocated in the document
- Can be public or secret
- Suomeksi: turvapolitiikka tai turvakäytäntö



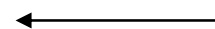
Security Policy Example (Oversimplified)

Identify
assets

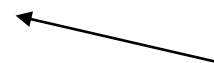


The company's main asset is the video telephone technology. Project managers produce a list of personnel, who has access to the unfiled patents and source code. This information may not leave the company premises. The ICT department will provide secure backups and storage in a remote location. All workers are required to sign this document.

Classification,
clearance



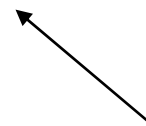
Protection



Responsibility
defined



Employee
inclusion

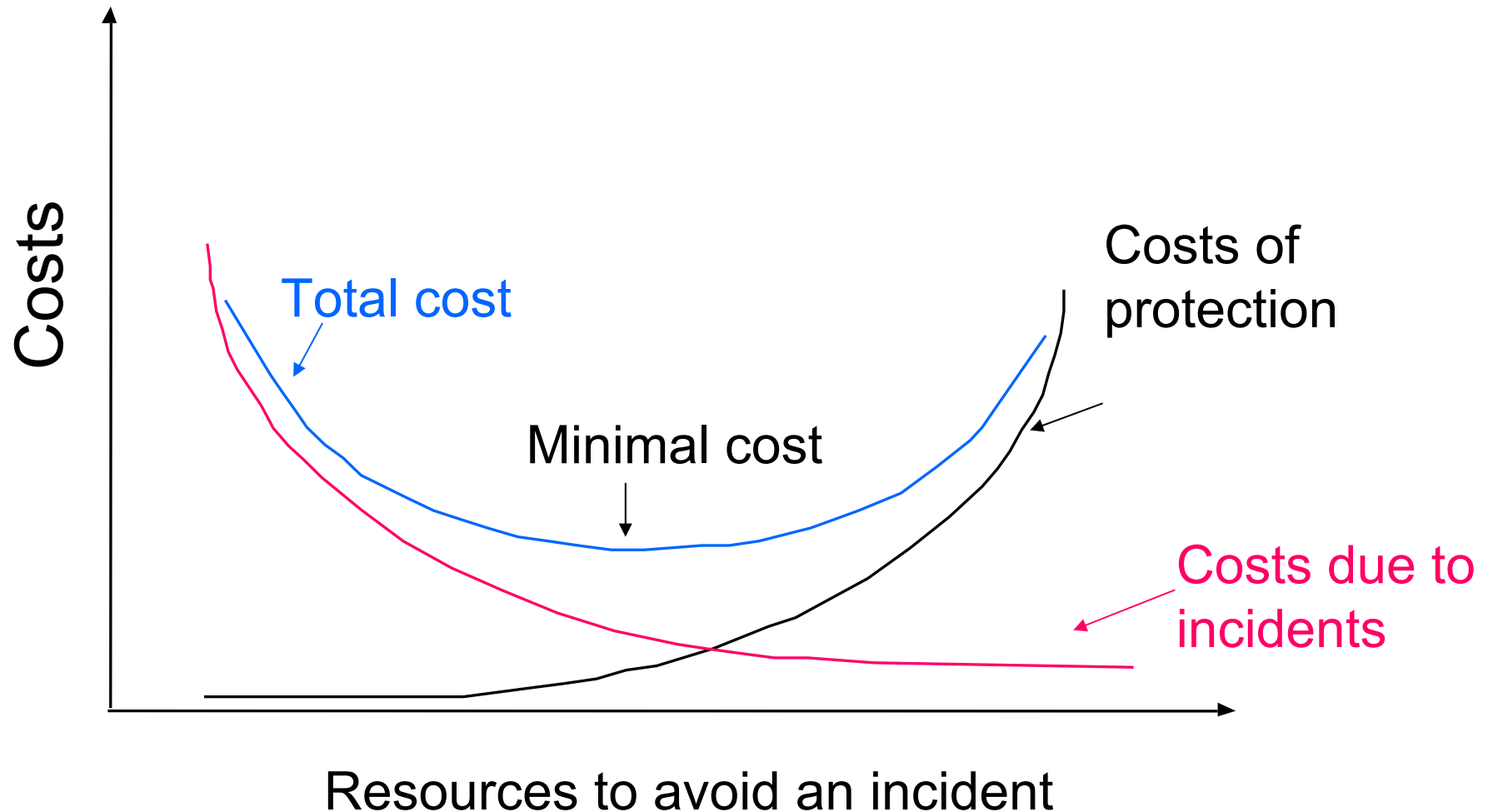




- The security policy is often based on a study called risk analysis
 - Before the risk analysis the assets and their value must be identified
 - Then the threats affecting each asset are identified and their likelihood of happening estimated
 - The risks are estimated and adjusted based on an analysis of how vulnerable we are to a particular threat
- A complete risk analysis is a big process
 - It can be simplified by grouping of assets and threats
 - Maintaining an existing analysis is easier
- Suomeksi: riskianalyysi, uhka-analyysi, haavoittuvuusanalyysi



The Balance between Risks and Costs





The Cost of Security

- Implementing security has always costs
 - Direct: implementing, software, equipment
 - Indirect: loss of work time, reduced access to documents
 - Rarely also savings: improvement of processes
- The costs must be valued against savings
- Security planning is needed to guide the use of resources, experience has shown that otherwise resources are wasted



Responses to Risks

- A risk can be reduced by security solutions
 - Technical, organizational
 - Occasionally even eliminated
- The remaining risk is to be accepted
 - Protecting against all possible risks is not cost effective
- Accepted risk can be reduced by insurance
 - Applies only to risks which are too big to carry and can be shared with others
 - E.g. fire can be insured against, wars can usually not and computing hardware is usually not worth insuring



- Security means understanding the risks relative to us and deciding what to do about them
- Organizational security means doing this in an organized and controlled manner
- The security policy is a major tool for ensuring the correct use of resources and for creating and distributing a common understanding of what is to be protected and how



Sample Exam Questions

- Which aspect of the CIA model is important for this exam before the exam date, which after the date? (2 p)
 - For questions like this, the answer should be at least two sentences justifying the answer, not just two words.
- Justify T/F (1p)
 - All risks, no matter how small, should be protected against.
 - No, cost/planning decides what to do
 - Confidentiality is the most important aspect of the CIA model.
 - No, depends on what we are protecting from what threats
 - Computer security is all about technology
 - Nyet, its about information and needs related to it
- Discuss the importance of the CIA model in the voting process of the USA presidential election. (3 p)
 - Avoid the obvious connection to the CIA in Langley, think votes are secret (C), the result must reflect the opinion of the people (I), any vote given must be counted (A), write this out in about 6 lines.



Sample Questions Cont.

- You are in charge of security for an organization collecting biological data in the Amazon jungle. Researchers are working independently traveling and recording the data on their laptops. You have: antivirus, encryption and communications software, USB-memory sticks, wireless modems and a central server in a protected location. What is the most important thing you require the researchers do to their research data daily (as written in the security policy). (2 p)
 - There is information missing. Are these university or medical corporation researchers? Make some assumptions and express them: "Assuming these are university researchers, secrecy is no requirement. Thus making a daily backup in case of intimate and lethal contact of local flora and fauna is of paramount importance..."