Basic Concepts of Information Security

Timo Kiravuo
Helsinki University of Technology
Telecommunication Software and Multimedia Laboratory

Based on slides by:
Prof., Dr. Sci. Teemupekka Virtanen
Security, why

- Protect valuable assets
- Compliance with laws
- Meet the customer requirements
- Prevent breakdowns in production
- Keep personnel happy
- Protect own reputation
Confidentiality- Luottamuksellisuus

- Secrecy of information
- Who is allowed to know something
- Bell-LaPadula – model
- A real property of information
  - Classification must be the same every place the same information is processed
Availability – Käytettävyys
(Saatavuus)

• Availability of service (information)
• What is the maximum time delay for getting service
• Sometimes probability of not losing information
• Some close areas
  – availability
  – reliability
  – usability
• A property of the system
  – The same information may have different classification in different systems
Integrity - Eheys

- The meaning of integrity has changed during time
- Originally integrity in transactions
  - There must been no partial transactions
- Now much broader definition
  - Data was correct in the beginning
  - All changes have be legal, accountable and correct
  - Data is still correct
- Accountability is usually required to maintain integrity
Threat – Uhka

• Something harmful that may happen
• Possibility to happen is the numerical value of a threat
• Examples
  – Fire
  – Death of key person
  – Malfunction of hard disk
  – Cracker breaking in
  – IRS comes to inspect the files
Risk - Riski

- The expectancy of a threat
- Two components
  - Threat (probability)
  - Damage (amount)
- Risk = threat * damage
Vulnerability - Haavoittuvuus

• Weakness in the information system
  – Makes it possible for a threat to occur
  – Increase probability of a threat
  – Increase damage

• Examples
  – Weak passwords
  – Weak encryption
  – No secondary power supply
  – A backdoor in the system
From Threat to Risk

Threat \rightarrow Vulnerability \rightarrow Loss

\begin{itemize}
\item Eliminate risk
\item Minimize risk
\item Accept risk
\end{itemize}
The Balance between Risks and Costs

- Total cost
  - Resources to avoid an accident
  - Cost of risk
  - Minimal costs
  - Costs of avoiding accidents
  - Costs of accidents
Data protection – Tietosuoja

• Privacy protection is a civil right in many countries including Finland
• Restriction on gathering personal information
  – What kind of information
  – From whom
  – How to use information
  – How to protect information
• Required by legislation
Protocol - Protokolla

- A formal description of discussion
- Vocabulary
- Order of words
- How to do handshake
- Between computers, diplomats, companies
AAA

- **Authentication - Todennus**
  - Mechanism for confirming the identity of user and integrity and authenticity of information
- **Authorization – Valtuutus**
  - Who is allowed to do what
- **Accountability – Kohdennettavuus**
  - It is possible afterward to find out who has made any operations
- **Identification – Tunnistus**
  - Connects a user to the real person
  - Usually additional authentication is needed to verify the identity
Anonymity - Anonymiteetti

• An entity can not be identified
  – Protects the privacy of the entity
• Can still be authorized to perform actions
  – By using e.g. certificates
  – E.g. when you buy something and pay only cash, the transaction is anonymous, but authorized
• This can often be a design requirement
  – E.g. government systems
Pseudonymity -pseudonymiteetti

• We can authenticate and entity and connect it to previous occurrences, but we can not identify the person connected to the pseudonym
  – E.g. web cookies
• Using the same pseudonym in different situations can lead to identification of the entity
Non-repudiation - Kiistämättömyys

• It is not possible for a user to afterward deny an operation he has made
• Methods
  – Electronic signature
  – Trusted Third Party
  – Time Stamps
  – Accountability may maintain also non-repudiation
Classification

• Classification – Luokittelu
  – Labeling sensitive information
  – CIA-model
  – (Confidentiality, Integrity, Availability)

• Clearance – Luokittelu
  – Classification of users of information
Corporate Security
The Assets

• Everything required for production
• Everything valuable
• All good reputation
• Investments
Material

- Production
  - Buildings
  - Machinery
  - Raw material
  - Stocks
- Valuables
  - Money
  - Art
- Other investments
  - Cars
People

• Production
  – Skilled workers

• Information
  – Databank

• Reputation
  – Value itself
Information

- Production
  - Prints
  - Orders
- Corporate management
  - Plans
  - Customer information
  - Personnel information
- Investments
  - Databases
- Compliance
  - Bookkeeping
  - Privacy
Reputation

- Good manufacturer
  - No malfunctions
  - No faulty products

- Good neighbor
  - Environmental protection
  - Safe traffic

- Good employer
  - Safety in work
Security Management

- Set the goals
- Define the security level
- Define the acceptance of risk
- Define protection principles
Security Policy

• A high level statement
• Defines the baseline security
• Defines the acceptable risk
• Defines protection principles
• Basic document
Legislation and security

• Assets may be protected by legislation
  – An intruder is a criminal and will be punished
• Special capabilities are guaranteed to protect assets
• Legislation sets requirements for security
Baseline Security

- The minimal required security level
- The procedures to protect others
- Usually more is required
  - Production
  - Customers
  - Legislation
Asset Management

- Recognize the important assets
- Classification
Physical Security

• Security domains
• Protection prevents outsiders from intruding
  – Fences, walls
  – Guards
• Authenticate the insiders
  – Keys, access control
• Detection
  – Alarms
  – Delay in detection
  – Precision of detection
• Active response
  – Time to reach the site
  – Amount of strength to prevent intrusion
How much is enough

- $S(T_p + T_g) > T_a + T_t$
  - $T_p$ time to go through a passive barrier
  - $T_g$ time to go to the next barrier
  - $T_a$ delay in alarm
  - $T_t$ time for a guard to reach the site
The Goal of Physical Security

- People in the domain may work efficiently
  - All the people are authenticated
  - All the people are trusted
  - No outsiders to look after
- Good working conditions
  - Safety
  - Fire prevention
- Don’t prevent or disturb working of authenticated people
Personnel Security

• Accepts insiders
  – Background checking
• Prevents accidents
  – Education
• Preserves motivation
  – Personnel management
• Personnel lifecycle
  – Hiring, working, firing
Operational Security

- Job management
  - Enough people
  - Possibility to work in a secure way
- Safety procedures
  - Safe working conditions
- Sharing of duties
- Key persons
Information Technology Security

• Computer security
• Communication security
• Security domains
• Protection against outsiders
• Authentication of insiders
• Notification of intrusion
Security in a Modern Organization

• Security requirements are part of management
• The lower level in hierarchy must meet the requirements of higher level
• The higher level must accept the cost of security
• Management in each level has to make decisions in security
Security in Outsourcing

• Security requirements as part of the service
• Defined in contracts
• Evaluation, certification
• Costs are part of the service
  – Service provider has to be able to include the costs in the price
Security Costs

• Part of normal operational costs
• Have to take into accounting when
  – calculate the investments
  – pricing products
  – pricing services
Conclusion

• Security is a prevention of incidents which may cause losses to the organization
• Security is optimization between losses and costs of protection
• There are several methods for protection