Economic Aspects Of Information Security

Hannes Federrath

Department Management of Information Security
University of Regensburg
Agenda

- What is information security?
- Technical building blocks
- Risk management cycle
- Return on Security Investment
- Architecture for Collecting quantitative historical data
What is information security?

- Communication networks
  - a lot of users
  - quite a lot of operators

Threats

- Unauthorized acquisition of information
- Unauthorized modification of information
- Unauthorized impairment of functionality

Protection goals

- Confidentiality
- Integrity
- Availability
Potential attacks

Nodes (computers)

outside (electromagnetic radiation)

inside (Trojan Horses)

communication channels

(Fixed) lines

Radio waves

outside only
Typical attack sequence

1. Gaining information
   - IP addresses, passwords, entry points

2. Attack (mostly via the Internet)
   - exploits, weak protocols, misuse of data/passwords etc.

3. Extension of access privileges
   - particularly installation of a back door

4. remove traces
   - delete or manipulate log files

Protection goals
- Confidentiality
- Integrity
- Availability
## Protection Goals

<table>
<thead>
<tr>
<th>Subject of communication</th>
<th>Circumstances of communication</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>WHAT?</strong></td>
<td><strong>WHEN?, WHERE?, WHO?</strong></td>
</tr>
<tr>
<td>Confidentiality</td>
<td>Anonymity</td>
</tr>
<tr>
<td>Hiding</td>
<td>Unobservability</td>
</tr>
<tr>
<td>Contents</td>
<td>Sender</td>
</tr>
<tr>
<td></td>
<td>Location</td>
</tr>
<tr>
<td></td>
<td>Recipient</td>
</tr>
<tr>
<td>Integrity</td>
<td>Accountability</td>
</tr>
<tr>
<td>Contents</td>
<td>Legal Enforcement</td>
</tr>
<tr>
<td></td>
<td>Billing</td>
</tr>
<tr>
<td></td>
<td>Recipient</td>
</tr>
</tbody>
</table>
Types of attacks

- **Passive attacks**
  - eavesdropping
  - traffic analysis

- **Active attacks**
  - masquerading
    - man-in-the-middle attack
  - modification of data
  - injection of data
    - replay
    - flooding, spamming
  - denial of service
Technical building blocks

**Confidentiality**
- Hiding

**Integrity**
**Accountability**
**Legal Enforcement**

**Anonymity**
**Unobservability**

**Availability**

- **Symmetric Encryption:**
  - one key, two copies

- **Asymmetric Encryption:** two keys
  - public key: everybody knows it
  - private key: known by recipient

- **Steganography:**
  - hiding the existence of content
Symmetric Encryption

- one key, two copies

random number r

key generation $k := \text{gen}(r)$

secret key

plaintext $x$ → Encryption $k(x)$ → ciphertext

Decryption $k(x)$ → plaintext $x$
Steganography

- hiding the existence of content

Diagram:
- Cover: c
- Message: x
- Secret key: k
- Embedding
- Extraction
Asymmetric Encryption

- two keys: public key and private key

Random number $r$

(key generation)

plaintext $x$

Encryption

$c(x)$

ciphertext

Recipient

Secret area of recipient

plaintext $x$

Decryption

private key (for decryption)

(c,d):=gen(r)
Technical building blocks

Confidentiality
Hiding

Integrity
Accountability
Legal Enforcement

Anonymity
Unobservability

Availability

- Symmetric Encryption:
  - one key, two copies

- Asymmetric Encryption: two keys
  - public key: everybody knows it
  - private key: known by recipient

- Steganography:
  - hiding the existence of content

Encryption and Steganography
- Fast, secure and cheap!

PGP.com
GnuPG.org
Technical building blocks

Confidentiality
Hiding

Integrity
Accountability
Legal Enforcement

Anonymity
Unobservability

Availability

• Message Authentication Codes
  – based on symmetric encryption
  – protects from modification by external attacks
  – fast, secure and cheap

• Digital signatures
  – based on asymmetric encryption
  – two keys
    • public key: everybody knows it
    • private key: known by recipient
  – private key used to sign a document
  – public key used to verify
  – allows legal accountability and enforcement (similar to contract signing in the real world)
**Digital Signature**

- only the sender can generate a signed message

![Diagram of digital signature process]

**Sender**
- message
- secret area of sender

**Recipient**
- msg/w signature and verification result
- "ok" oder "failed"

**Key Generation**
- random number
- public key (testing of signatures)
- private signature key

**Signieren**
- msg/w signature
- x, sig(x)

**Testen**
- x, sig(x), "ok" oder "failed"
Technical building blocks

Confidentiality
Hiding

Integrity
Accountability
Legal Enforcement

Anonymity
Unobservability

Availability

- Digital signatures
  - based on asymmetric encryption
  - two keys
    - public key: everybody knows it
    - private key: known by recipient
  - private key used to sign a document
  - public key used to verify
  - allows legal accountability and enforcement (similar to contract signing in the real world)
Technical building blocks

Confidentiality
Hiding

Integrity
Accountability
Legal Enforcement

Anonymity
Unobservability

Availability

• Digital signatures in the real world are
  - Fast, secure, but:
    • Expensive!

More exactly:
  Tech. cheap
  Orga. expensive

• Digital signatures
  - based on asymmetric encryption
  - two keys
    • public key: everybody knows it
    • private key: known by recipient
  - private key used to sign a document
  - public key used to verify
  - allows legal accountability and enforcement (similar to contract signing in the real world)
Technical building blocks

Confidentiality
Hiding

Integrity
Accountability
Legal Enforcement

Anonymity
Unobservability

Availability

• Public key infrastructure (expensive)
  – authenticity of public keys has to be ensured by technical (cheap) and organizational (expensive) means:
  • digital key certificates (e.g. X.509)

• Certification authority has to
  – check physical identification documents
  – process is handled by paper (legal issues)
  – for every user, year after year

• Costs (for handling paperwork and the physical process)
  – 10 - 150 EUR per certificate p.a.

• 80 Mill. Germans: > 1 billion EUR
  – Who should pay for the security?

☐ The signer  ☒ The recipient
Technical building blocks

- **Confidentiality**
- **Hiding**
- **Integrity**
- **Accountability**
- **Legal Enforcement**

- **Anonymity**
- **Unobservability**

- **Protection of privacy**
  - Anonymity: Protection of the identity of a user while using a service (e.g. counseling services)
  - Unobservability: Protection of the communication relations of users

- **Internationally agreed privacy principles** (e.g. EU Privacy Directive of 1995)
  - no covert collections of personal information
  - informed consent to purpose prior to collection
  - retention and use only according to agreed purpose
Technical building blocks

Confidentiality
Hiding

Integrity
Accountability
Legal Enforcement

Anonymity
Unobservability

Availability

• Reality:
  – organizations ignore privacy
  – international

• Privacy activists
  – develop anonymization tools
    • http://tor.eff.org
    • http://www.anon-online.org

• To respect the privacy laws is
  1. a matter of legal compliance,
  2. a marketing issue (acceptance of privacy friendly systems) and
  3. cheap!

No storage of personal data, no effort for privacy protection.
Technical building blocks

- **Confidentiality**
- **Hiding**
- **Integrity**
- **Accountability**
- **Legal Enforcement**
- **Anonymity**
- **Unobservability**

- **Availability:**
  - Ensures that data and services are accessible to the user within a certain period of time

- **Two Mechanisms:**
  - **Redundancy:** duplication of components or repetition of operations to provide alternative functional channels in case of failure
  - **Diversity:** functional identical channels with a variety of designs provide reliable functionality in case of (software) failure

- **Redundancy and diversity:**
  - **Expensive**

Risk management
Management of Information Security

Prof. Dr. Hannes Federrath

Risk management cycle

Identification

Security management is a risk management task

Assessment

Control

Checklists
Workshops
Histor. data
Experts

Baseline
Qualitative
Quantitative

Best Practice
Scoring
Quant. Methods

Monitoring

Checklists
Scorecards
Business Ratios

Criticality

Low

Control weaknesses
Identification of threats

- **Question**
  - »What are the threats?«

- **Methods & Tools**
  - checklists
  - workshops
  - attack trees
  - fault trees

- **Challenge**
  - cover all threats
Assessment of threats

• **Question**
  - »What are the probabilities and consequences of threats?«
  - Risk = probability * consequence

• **Methods & Tools**
  - qualitative assessment
  - quantitative assessment
  - game theory

• **Challenges**
  - dependency from assets
  - strategic attackers
  - correlations between threats
  - source of (quantitative) input
Control of threats

- **Question**
  - »How to handle risks?«

- **Methods**
  - best practice approaches
  - baseline protection

![Diagram showing risk management stages: Risk assessment, Risk avoidance, Protection measures, Damage limitation, Shifting, Insurances, Emergency plan, Security architecture, Entire Risk, Residual risk. Each stage is connected by arrows showing the flow of risk management.](image-url)
Monitoring of risks and measures

- **Questions**
  - »Were the measures effective and efficient?«
  - »What is the current protection level?«

- **Method**
  - scorecard approaches

according to: Loomans, 2002
Risk management cycle

Identification

Quantitative security management needs quantitative data

Assessment

Baseline Qualitative Quantitative

Control

Best Practice Scoring Quant. Methods

Monitoring

Checklists Workshops Histor. data Experts

Criticality

Checklists Scorecards Business Ratios

Control weaknesses
Return on Security Investment (ROSI)

- based on the calculation of an annual loss expectancy for a certain undesirable event (threat): (FIBS 1979)
  \[ ALE = SLE \cdot ARO \]

- aggregation of ALEs of several events: (Soo Hoo 2000)
  \[ ALE = \sum_{i=1}^{n} S(O_i)F_i \]

- Return on security investment: (Wei et. al 2001)
  \[ ROSI = ALE_0 - ALE_1 - \text{cost} \]

- if ROSI > 0 then investment was advantageous
Return on Security Investment (ROSI)

- **ROSI**
  - Alternative calculation as a ratio: (Sonnenreich et. al. 2006)
    
    \[
    ROSI = \frac{(\text{risk exposure} \cdot \% \text{ risk mitigated}) - \text{cost}}{\text{cost}}
    \]

  - Another variation: (Pfleeger and Pfleeger 2003)
    
    \[
    \text{risk leverage} = \frac{(\text{risk exp. before red.}) - (\text{risk exp. after red.})}{\text{cost of risk reduction}}
    \]

- **Advantages**
  - Different security measures can now be compared.
  - Security investments can now be compared with other investments (non-security).
Quantitative data is needed

- Risk assessment needs input:
  - probability of a security-related event and
  - level of damage (cost in case of ...)
- Problem:
  - enterprises are not willing to reveal such information
  - loss of reputation/trust

Some information from the past

<table>
<thead>
<tr>
<th>cost</th>
<th>benefit</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>= nothing happens</td>
</tr>
</tbody>
</table>

Detailed information (numbers) on past events

<table>
<thead>
<tr>
<th>cost</th>
<th>benefit</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>= nothing happens</td>
</tr>
</tbody>
</table>
## Potential Sources for Quantitative Data

<table>
<thead>
<tr>
<th>Mechanism</th>
<th>Example</th>
<th>Evaluation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expert Judgements</td>
<td>Interviews with internal or external experts, CSI/FBI Survey</td>
<td>Used frequently, but not originally quantitative Subjective, incomplete</td>
</tr>
<tr>
<td>Simulations</td>
<td>Historical simulations, Monte Carlo simulations</td>
<td>Good, however reliable input data is needed</td>
</tr>
<tr>
<td>Market Mechanisms</td>
<td>Capital market analyses, Exploit derivatives, Bug challenges</td>
<td>Not applicable to all situations Not yet available</td>
</tr>
<tr>
<td>Historical Data</td>
<td>CERTS collect data on security events, Internal incident reporting</td>
<td>Widely used in other areas (e.g. insurances) Past != Future Hardly available so far</td>
</tr>
</tbody>
</table>
Idea: Collecting quantitative historical data

• Idea
  – Building a system for the collection of quantitative historical data on security incidents from different organizations

• Goal
  – A database that gives information about impact and frequency of security incidents

• Existing approaches have a different focus

• Microeconomic theory shows the utility of that concept

• Various possibilities to use that data
  – Risk assessment, investment decisions
  – Benchmarking between organizations
  – Examination of statistical distribution functions, correlations
Basic Architecture

- **Participant A**
- **Participant B**
- **Participant C**

- **External Sources** (CERTs, Honeynets, Experts, Surveys)

- **Additional Data**
- **Aggregated Data**
- **Incident Data**
Input and Output

- Incident Description
- Incident Effects
- Incident Handling
- Organizational Setting

Data Collection
Harmonization
Aggregation
Interpretation

Data Submission
Data Distribution

Reports
Risk Parameters
Fairness Requirements

- Two major problems known from economics
  - Free-riding
  - Truth-telling

- Mechanisms
  - Incentive system
  - Reputation system
  - Legal framework
  - Statistical checks for plausibility
Current State of Implementation

- **Web-based multi-tier Application**
  - Java Servlets, JavaServer Pages PostgreSQL
- **Taxonomy realized as XML-schema**
  - All incident reports in XML
- **Already implemented**
  - Data collection/transfer
  - Data storage
- **Next steps**
  - Data analysis mechanisms
  - Interface for ext. data
  - Deciding on mechanisms to provide fairness
Conclusions

- Security management becomes more challenging
  - Increasing dependence on information systems
  - Growing number of threats
  - Compliance requirements

- Security management is a risk management task
  - Measuring costs and benefits of security is challenging
  - Quantitative data is needed for modern security management
  - Historical data might be a solution for that problem