



Mag. iur. Dr. techn. Michael Sonntag

IS/ICT security in the newly forming society

České Budějovice, 13.-15.9.2006

Institute for Information Processing and
Microprocessor Technology (FIM)
Johannes Kepler University Linz, Austria

E-Mail: sonntag@fim.uni-linz.ac.at
<http://www.fim.uni-linz.ac.at/staff/sonntag.htm>



Agenda

- The different dimensions of "security"
- Selected aspects of security
 - Secure system design and implementation
 - Digital Rights Management
 - Phishing
 - Data retention
 - Privacy
 - Liability for and because of security
 - Specific applications
- Current trends: Technical and legal
- Outlook



Introduction

- In the past, security was typical "physical" and "on-site"
 - Treasure vaults, herald for "secret" messages, ...
- Today, attacks can come from any distance and target intangible things, where theft may go unnoticed
 - Internet allows access into companies from all over the world
 - A copy doesn't change the original
- Security now touches everyone
 - Every company and most persons own computers with broadband access and valuable data on it
- The "information society" leads to a hunger for information
 - Google analytics → Inspect the internal visits on webpages
 - E-Commerce: Identify & track customers
 - Police: (Nearly) Everyone is a suspicious & dangerous person
 -



The different dimensions of "security"

- Technical: Using IT to prevent access, modifications etc.
 - Encryption, certificates, secure hardware, ...
- Organisational: Make sure technical means are actually used
 - Prevent passwords under the keyboard!
- Legal: Deterrents against undesirable behaviour
 - Criminal law, indemnification, etc.
- Sociological: An atmosphere of fear
 - The risk of acts of terror compared to traffic accidents
- Psychological: Constant surveillance is problematic
 - Monitoring employees in certain ways is forbidden, but for security it is obligatory!

Take care, **where** security of **which kind** is appropriate
(and where **none** might be better!)



Selected aspects of security

- Security is typically explained in a very technical way
 - Encryption algorithms, bugs, protocol analysis, ...
- Instead, we focus on the various other dimensions:
 - Do they lend themselves easily to abuse?
 - How will security predominantly have to be ensured?
 - » Technical, organisational, human aspects, ...
 - From the view of the users and the designers/programmers
- Security, privacy and their interdependence
- Liability for and because of security



Secure system design and implementation

- Software system development is predominantly "feature development" - with security being a "non-feature"!
 - "If in doubt, postpone security and add a new function"
 - This is partly at the end: See office suites, but also OS
 - » UI, integrating other services etc. → Still important
 - » "New" technologies, e.g. Ajax: Getting it to work seems to be more important than its security!
- Security is seen similar as testing by developers
 - I don't like it, its unnecessary, my code is secure anyway, ...
 - Trying to break ones own program is not a happy occupation
 - » Even thinking about how this could be done won't be successful
 - Separate developers for implementing security might help
 - » They generate "obstacles", feature developers must overcome



Secure system design and implementation

- Main problem: Retrofitting security is very difficult
 - Security affects all parts of the system and at different levels
 - Component reuse difficult in this regard
 - » Different or missing security models, wrappers are not always enough, adaptation not possible/allowed, ...
- Security must predominantly be ensured through the process
 - Secure software is not the result of adding "security" to the (finished) product, but rather of a process involving security at all stages of the development
 - » Designing appropriate protocols
 - » Fine-grained permissions for accessing data
 - Aspect oriented programming might help



Digital Rights Management (DRM)

- Resented by end users, but desired by data owners
 - Implementations typically impact privacy significantly
- A hazard for availability: Locking yourself out
 - Or simpler: The responsible person is ill, on holiday etc.
 - New vulnerability: Just change/delete the encryption key ...
- Still, helps a bit against "inside attacks", which are the majority of all security breaches!
 - The focal point is then secure identification of the person and "intentional circumvention"
 - » When security is just too cumbersome to do the work
 - Not foolproof: All "export" methods must be secured!
 - » Including mobile phones, USB ports, disk/CD drives, printers, ...



Phishing

- In its various forms the oldest attack: Social engineering
 - Bringing the persons to reveal the information themselves
- Reduction only by education and organisation!
 - Technical measures can't solve it, but make it more difficult!
 - » Example: Tokens instead of passwords
 - » Entering a TAN is much easier to achieve than requiring an electronic signature with a smartcard
 - But see the "helpers " for exploiting the results of phishing:
Receiving money and sending it on with e.g. Western Union
 - » Compare to "traditional" security: Drop a bank transfer form into the post box of the bank
 - Organisational changes can reduce the danger too
 - » Require two persons for access or verification by someone else
 - Education: Instigating fear is bad for a company/society too!
 - » E.g. not every visitor is a spy; it might be a customer!



- Possible solutions:

- Automate the unimportant acts so only few, but important ones, must be performed consciously
 - » A widely applicable approach, see e.g. RFID
 - But not everything can be automated
 - » Better "automation" would be: Humans do in unconsciously!
- **Everywhere** avoid techniques used for phishing
 - » Example: Austrian E-Mail law changed recently
 - ⇒ Sending out mails asking users to confirm their accounts ...
- Add more "procedures" to underline the importance
 - » E.g. PIN/TANs on a **formal** sheet of paper
- Standardisation and education on typical procedures
 - » So deviations can be recognized more easily
- IT education in schools is typically "feature" education: How to use (or do) something: Security should be taught too!



Data retention

- The opposite of privacy: The personal association is stored
 - For later use by the police or other interested parties
 - To enable/ease the prosecution of "crimes" using ICT
- Technically rather easy to subvert
 - Use an anonymizer in a third country without data retention
 - Danger: Computers hacked and used as attack sources
 - » Third persons will be "criminals" - No logs on their computers!
- Important change in policy:
 - Previously: Information gathered only on "suspicious" persons
 - Now: Information is collected on everyone
- Problem: Data present **will** be used for ever more cases
 - See Germany: Data collected for road pricing!
- One result: Simple attackers lose their anonymity, sophisticated ones can blame others more easily....



- Security and privacy are anathemas to a certain extent
 - Securing access requires identifying users
 - Reducing security to increase privacy can be detrimental
 - » Less security → More data accessible to third parties!
- A possible solution: "Compartmentalization"
 - Data is partitioned and encrypted, so only specific users can access it; perhaps several must act together
 - » Even the administrator has/can gain no access alone
 - Requires the keys to be stored separately, e.g. secure tokens
 - » Not really usable in its direct form ⇒ See DRM!
- Privacy can be its own enemy
 - Access to personal data must be logged
 - » This is new personal data on the actions of users
 - » But such data may **not** be used for other purposes (legally....)
 - Example: Time of entering work-time may not be used for verifying it!



Liability for and because of security

- Liability for (defective) security
 - Anti-Virus software is a **must** for companies
 - » Not using it is negligence → Liability, no/reduced compensation!
 - In other areas: Lacking security = administrative penalties
 - Continuous increase of the required measures in the past
 - » Now it could start even for private persons!
 - Software without security features might not fulfil a contract, even when not mentioned explicitly
 - No success required, only reasonable precautions!**
- Liability because of (defective) security
 - Criminal acts through own computer → **You are the criminal**
 - » Example: Placing illegal/inappropriate material on it
 - When the computer is subverted, traces of this can be removed too as the last action!



Specific applications: Voice over IP (VoIP)

- Two versions: Private vs. public systems
 - Private systems are typ. secure(d): Within company, VPN, ...
 - Public ones are mostly insecure: Unencrypted, ...
- Two main areas of security problems in public VoIP
 - Signalling: With (one) central server
 - » Communication pattern analysis or misdirection possible
 - Data: Still sent unsecured
 - » Allows creating a speech library to construct fake messages!
 - » Security standards exist, but are not (yet) implemented
 - » Sent directly, so problematic for firewalls
- Often additional functionality, e.g. application sharing
 - "Hiding" functionality in a different protocol creates dangers
- Encrypting signalling and/or data might be contrary to data retention and forbidden in the future!



Specific applications: Radio Frequency Identification (RFID)

- Basic RFID idea: No physical contact needed for chip access
 - This eases unauthorized reading (privacy!)
 - » With special equipment (direction antennas) connection to the tag possible across several meters
 - But "automates" security, e.g. granting access
 - » Allows concentrating on the more important areas
- Security for the information on the tag rarely considered
 - No authentication needed for access
 - But: Often only a serial number and no direct information
 - » Might change in the future: Complex tags become cheaper
 - Various techniques for improving security exist
 - Require typically more expensive tags and readers; more complex
 - » Removing/clipping the antenna, authorization required for access, encrypted transmission, ...



Current trends: Technical

- "Mainstream" security isn't changing very much
- There seems to be a security gap
 - Masses of "simple" attacks, e.g. using ready-made programs
 - » Still successful as especially private computers are often completely unsecured!
 - Very few "complex" attacks, but these seem to be more targeted (organized criminals instead of hackers)
 - » Very difficult to avert for "normal" companies
- Security is increasingly outsourced to specialists
 - At least for network and perimeter defence
- Technical issues mostly solved
 - Lacking: Integration, systematic security, user acceptance
- Gathering all data is possible and therefore done
 - Privacy is often forgotten → See later today!



Current trends: Legal

- Privacy is reduced continuously
 - Access to more information for more persons
 - "Security" in various forms is seen as paramount
- Security features are used to restrict user's options
 - Debate necessary, where these restrictions should be added
 - » E.g., most companies physically secure only few data
 - » But electronically the trends moves to securing everything
 - Consumer protection necessary?
 - Subverting security becomes more and more illegal
 - » Even if the result/aim **IS** legal!
- Both **security** and its **circumvention** becomes **obligatory**
 - Liability and criminalisation of missing security
 - Data retention → See later today!



- Retrofitting security is difficult – More focus in development
 - When something is in widespread use without security, adding it later is almost impossible
- Security needs (desires?) change over time
 - Techniques posing no risk at first become major loopholes
- Even simple security is subverted by users
 - What will they do with really annoying security?
 - The result: Ever more perfect (and obstructing) security
- The danger of security increases
 - "It's all secured, I don't have to think about it..."
- Information hunger vs. information usage
 - Data evaluation falls behind data collection

F I M

Questions?

Thank you for your attention!