

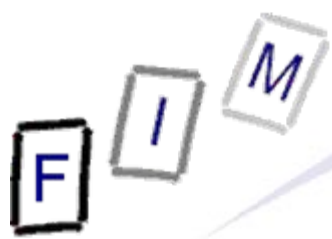


IS/ICT Security and Privacy

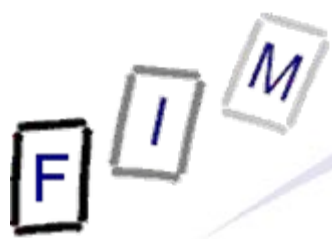
IDIMT 2007, Budweis

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>

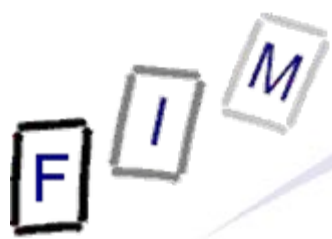


- Changing security needs: Real/Perceived
 - Security for non-specialists
 - Legacy security
 - Phishing
 - Online searches
 - Mashups/CBSE (Component-Based Software Engineering)
- Privacy – A new assessment?
 - Video surveillance
 - Data retention
 - Data destruction vs. computer forensics
 - The "digital curriculum"
- Conclusions and outlook



Changing security needs

- Security is discussed broadly today
 - Large amounts seem to be missing!
 - » Especially regarding computers and networks crime seems to be absolutely soaring!
 - Compare this to actual numbers of investigations/judgments!
- A shift of responsibility to others exists:
 - "I must be protected"
 - » Best example: Phishing!
 - Instead of "I protect myself as far as possible"
 - » Use of common sense, firewall, and virus scanner
- Additionally: All crime must be prevented or at least punished
 - No place for small crimes to be handled "inofficially"
 - Example: Video surveillance in English school toilets
 - » No destruction, graffiti, etc. any more! +
 - » No protests, experiencing crime, nonconformity, privacy -



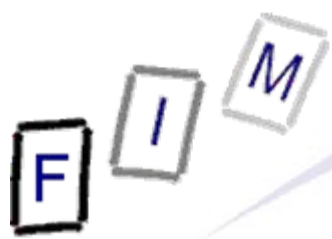
Changing security needs: Consequence for software design

- Bringing security to the end-user
 - Not everything can and should be kept from them
 - » Example: Brake lights on cars → Security device for others
 - Not helpful for you at all
 - » Comparable: Firewall
 - Not helpful for you (false positives!); protects others from zombies
- Guidelines:
 - Secure default configuration, difficult to "unsecure"
 - » End-users will not buy security services or read the manual
 - Ease of use in fully secured mode
 - » Doesn't work → disable security → works ⇒ Will stay disabled!
 - Logging to ensure traceability
 - » Instead of continuous monitoring, keep evidence (securely)
 - Rules for destroying information
 - » Sometimes information should just be destroyed
 - Otherwise: It will be used very soon...



Security problems: Restricted security

- Security for non-specialists
 - Simple security configuration
 - » Example: Bluetooth keyboard: Press button, enter keycode
 - Or: Wizard for configuring a secure customized configuration
 - "Security driving license"
 - » Computer driving license → How to use something
 - Not: How to **secure** something/use something **securely**!
 - » Advantage: No relocating to an "insecure" country!
 - Spam senders can relocate, but they cannot move their zombies!
- Legacy security
 - Often legacy systems must be used which do not support or even allow (complete) security
 - » Example: Application does not support encryption
 - » Example: Software conflicts with security patch
 - More focus on "stable" interoperability and wrappers
 - » Not everyone will always, immediately, and only use latest version
 - » Especially important for computer science education



Security problems: Voluntary disclosure

- Phishing

- Combating phishing is extremely difficult
 - » The user does what he intends to do and should be able to do!
 - » Move security back to the user!
- Changing security methods is very dangerous
 - » From TAN to iTAN to mTAN, ... → Users enter TANs everywhere
- Start with very high security from the start, so there is no need for a later "upgrade"
 - » And use internal configuration to reduce security if performance, laws etc. require it for now!
 - Example: Use el. signatures → reduced key length for interoperability, speed etc.

- Online searches

- Currently hotly disputed, especially in Germany
 - » Already occurred in reduced form in the USA
- Secret online search of computers
 - » How to do this securely? The police should be able to access the computer, but not hackers!



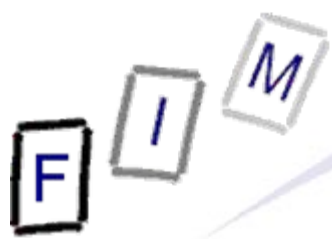
Security problems: Loss through assembly

- Mashups/CBSE are based on assembling elements from third-parties into a single "unit" for deployment
 - Security danger from compound =
 - » Security loss from each and every element
 - Chain – Weakest element is the limit!
 - » Security loss from the assembly
 - Elements previously separated are now operating in the same space
 - When users enter information → Where is it sent to?
 - » To which system(s)?
 - » What is the privacy policy of the system as a whole?
 - Special mashup problem: Was element intended for mashup, i.e. exists a semantic description what is really does?
 - Special CBSE problem: Research focus on assembly at runtime → What about investigating the search profile?
 - Logging is special here:
 - » Inside-logging difficult/rare; Interface logging large effort
 - » But absolutely necessary to identify the "culprit" element!



Privacy - A new assessment?

- Continuous erosion of privacy
 - More security → Less privacy
 - » "I don't have anything to conceal"
 - So: A webcam in every single room at home and at the office!
- Privacy is only appreciated "after the fact"
 - When one was target of a breach of privacy
 - See also: Users read more privacy policies if they understood the ones they read before!
 - » Lawyers - TODO: Write understandable policies!
- One possible reason:
 - Past: Reciprocity and local restriction
 - » You knew everyone in your hamlet and they knew you...
 - IS/ICT:
 - » Observation is one-way only:
You are watched, but you cannot observe the watcher
 - » Practically (not legally!) unrestricted distribution



Video surveillance

- Study of the Great Britain home office:
 - Small benefits in certain areas through video surveillance
 - » Improvements: Small closed areas & premeditated crimes
 - Especially: Car theft from parking lots
 - Increased feeling of safety
 - » See bank robberies: 100% surveillance, but
 - From the police perspective: Video surveillance is a replacement for many guards with perfect memory
 - » But: Best results come from manually guided cameras!
 - See also: London city center car tax ⇔ divorce proceedings
 - » Employing the law to uphold morality!
- Against terrorism: Identifying the persons afterwards
 - Will only help against certain attacks sometimes
- As soon as video can be "searched" for persons reliably, privacy will almost be gone!
 - Tracking the location of every person in London the whole day



- Data retention = Keeping logs for future use
 - No problem at all, depending on who stores/may access them
 - Similar to video surveillance
 - » No prevention, only detection and prosecution is enhanced
- Not really usable against serious crime
 - Music sharing cannot be transferred to other countries
 - But serious hackers, terrorists can easily relocate!
- Data retention (IP address, E-Mail, VoIP) according to the EU directive can easily be circumvented
 - Closed group: Trivial protection (example: Alternate port)
 - Current use of retained data: Identifying filesharing users
- Very important is, when the information can be used
 - I.e., which initial suspicion is required for disclosure
 - » Recent reports revealed, that an IP address in many instances would not be a good source at all!
 - Open WLANs, incorrectly configured DSL, time differences, ...



Data (non-) destruction

- Merging security and privacy: Data often disposed incorrectly
 - Privacy laws require deletion of data after some time/event
 - » But what about backups? Removing single records?!?
 - Harddisks with sensitive information: Formatted, not wiped
- Many precautions are easy, they just must be "done"!
 - There exists no "conscience of privacy"
 - » If people thought about it, they would wipe harddisks
 - » If people thought about it, software would have deletion facilities
 - » ...
 - Somewhat different in the USA:
 - » Identity theft is an actual and widespread problem
 - » This lead to more secure data disposal
 - Privacy still seen as less important, but that level is "enforced"!
 - Example: Shredding of invoices against dumpster diving



Computer forensics – A replacement for data retention or online searches?

- Computer forensics can recover a whole lot of information
 - Often much more than data retention!
 - » Example: Local file content which was already deleted, traces of encrypted traffic, ...
 - But "local" data can always be deleted or modified
 - » The evidence value is typically rather low for information to be missing (as opposed to information still present!)
 - Finding deleted child pornography images → Conviction
 - Finding a wiped harddisk → Inconclusive (many reasons possible)!
- Some programs actively try to protect privacy
 - Deleting personal information on request/automatically
 - This increases the drive for hidden searches
 - » Such information would not be available in data retention and can be difficult or impossible to find through computer forensics



A backside: The "digital curriculum"

- Prospective employee history has always been important
 - But some filtering existed:
 - » What was presented
 - » What could be obtained from previous employers
 - Legal requirements also figure largely as protection
- But traces remaining on the Internet change this
 - Searching newsgroups for postings from many years ago
 - Profiles on sites: Dating, hobbies, picture/video-sharing, ...
 - » Not all are created by yourself
 - » Difficult to remove later: Copies, RSS syndication, web archives!
 - Problem: Persons with the same name, forgeries etc.
- Countermeasures are difficult
 - Use pseudonyms/anonymity right from the start
 - Insist on deletion, no permission for publication, time limit, ...



- The more privacy is enforced or used, the more anti-privacy measures will be asked for!
 - This contradiction can only be solved politically
- Investigation must focus on professionals
 - Data retention working only against "amateurs" is useless!
 - » 31% of incidents are hackers, 60% stolen hardware, insider abuse/theft, administrative errors, accidentally exposing data
 - » **But:** 45% of disclosed data happened through hackers!
 - Hackers are therefore "professionals"!
 - » Measures against them must take this into account!
- Collecting data "just in case" is therefore not going to help!
 - This is just data which will later be "mis-"used
 - More "extreme" measures, but only for the "hard" cases!

The first counter-example, the dig. curriculum, has just arrived



- Lacking privacy:
 - Drawbacks will be felt increasingly and by more and more people in the next years
- Erosion of security:
 - Information is stored (retained) in more places
 - Explicit subversion of security for monitoring
- Measures to be introduced:
 - Neither forensics, data retention, nor hidden online searches can fulfil all requirements
 - » A combination of all of them may be required
- Possible countermeasures:
 - Users should be educated regarding security
 - Technical requirements and legal obligations for security
 - Strict and permanent safeguards for investigative measures

F I M

Questions?

Thank you for your attention!