Mag. iur. Dr. techn. Michael Sonntag

Towards un-personal security

IDIMT 2008, 10.-12.9.2008, Jindrichuv Hradec

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

The current state of privacy

Introduction

- Security:
  - → The state of being free from danger or injury — Facts
  - → Freedom from anxiety or fear — **Feelings**
- Privacy:
  - → To be in control of what is known about you — **Facts**
  - → To feel unobserved by others — Feelings
- Both contain irrational elements
  - → Last years: Security always dominating (Feelings > Facts)
  - → Suddenly, privacy becomes interesting!
    - » Computers/CDs sold with financial information of thousands
  - → Result: Politicians want to forbid any selling of personal data
    - » Note: Even privacy officers think this is a bad idea …

Can we build the fence with other material/differently?

Security vs. Privacy – Or both?

- Often both are seen as incompatible
  - → Better security → Less privacy
    - » E.g. video surveillance: Deterrent/Identification vs. Observation
  - → Better privacy → Less security
    - » Example: Anonym. Internet access → Terrorist communication
- But what about
  - → Fences? Increased security, no privacy implications
  - → Curtains? Increased privacy, no security improvement
  - → Anonymous whistleblowing hotline?
    - » Better privacy **PLUS** better security!
- Result: Categorization of security measures
  - → Personal security: Positive, Neutral, Negative
    - » Invariably tied to a person (e.g. key, password)
  - → Un-personal security: Nobody is identified at all

Positive personal security

- The person to be granted access must be identified
  - → But attackers and other persons remain anonymous
- Examples:
  - → Key, password: Presence of the person carrying/using them becomes known; but might be member of a group only
    - » Attackers (stolen key, lockpicks) remain anonymous
  - → Automatic locking: Screensaver locks computer
    - » Idle time of the user currently logged in is measured
  - → Encryption: Persons knowing the key
    - » Breaking the encryption → Anonymous
  - → Signed code: Identity of signer known
    - » Users, illegal copying, … → Anonymous
- Not a perfect solution (attackers remain anonymous), but at least does not affect the privacy of third persons!

A securely locked ladder on the outside

Neutral personal security

- Everyone is identified or (identifiable with additional data): Users, attackers, and third persons
- Examples:
  - → Mandatory ID cards: Advertising the identity even in non-security related areas (→ especially with RFID chips!)
  - → Video surveillance: Every person passing the area is affected
    - » Regardless whether the object to secure is "manipulated"
  - → Automatic unlocking: Detecting the presence through tokens, speech recognition, etc. → Constant monitoring of everyone!
  - → Data retention: Data is collected in case the person might do something illegal in the future, even if this never happens
  - → Intrusion Detection Systems: Like video surveillance
- Worst case! Data is "tainted", as everyone is suspicious
  - → Strong incentive to use the data, as it is present (costs!)

Video surveillance of the whole fence + surroundings

Negative personal security

- Identifies only attackers, but not authorized users or unrelated third persons (passers-by)
- Examples (rare!)
  - → Honeypots: Such systems will never be used, except when you are an attacker looking for victims
  - → Quick-freeze measures: If a problem occurs, data is retained after an initial report (by a human!) for later disclosure
- Ideal class, as only the anonymity of attackers is broken, which is usually seen as reasonable!

Hidden barbed wires on top of the fence

Identification – Is it really necessary?

- The typical non-anonymous security process looks like this:
  1. Identify the person wishing access
     - » How to do this reliably? False acceptance/Rejection rate?
  2. Check whether this person should be granted access
     - » Actually it is often "should **not** be allowed to access"!
- Basic assumption:
  - → We can pre-define in advance who is an attacker or who is not
    - » Problem: "No data" or "we don't know for sure"
    - » Spam: Blackhole lists vs. SPF/Sender-ID/DKIM
    - » Necessity for: Guest accounts? Open WLan?
  - → Classifying persons = A less secure way exists
    - » Fingerprint registered? → Bypass passport check!
    - » No/less restrictions for the administrator …
    - » Beat the identification? No more security measures!
      - – Some help: Defence in depth!

Identification – Is it really necessary?

- Better: Security independent of identity
  - → Don't look at passports, search for explosives!
  - → Ignore mail sender, investigate content for SPAM!
  - → Packet illegal? Just drop it!
  - → Restrict administrator too (second person, additional step, …)
  - → Guest accounts are physically separated (VLAN, …)
  - → Different (more strict) firewall rules for open WLAN
    - » E.g. web browsing only, but no sending of E-Mails
- Prerequisite: Danger can be detected directly
  - → No identification of the person needed!
  - → These are actions, which are dangerous "absolutely", i.e. nobody should be allowed to do them
    - » Baseline of security; separate from permissions

Un-personal security

- Security which never identifies anyone
  - → Only proactive security: Attackers remain anonymous too
  - → We can detect that an attack occurred, but absent other measures (traces) we cannot identify who it was
    - » Almost everything in the Internet currently has this effect
      - – Anonymous proxy, …; Data retention might reduce this somewhat
- Not suitable for everything, but for some:
  - → Sandbox and unsigned code: Applets may only perform non-critical actions → No identification of author/user needed

"Fence"

    - » The same applies to JavaScript in browsers!
  - → Code verification: Inspection of the code is independent of all persons; might have been modified by anyone

"Search"

  - → Tripwires: Regular checks for modifications

"Seal"

    - » Only checks the content; how the modification occurred cannot be determined → Otherwise negative personal security!

Very high & smooth walls instead of fence

Un-personal security: More examples

- Firewalls: Block undesirable connections
  - → Logging → Negative personal security, but possibility for DoS!
- Anti-virus/spyware: Look for trojans and viruses
  - → Sender IP is usually forged/from a botnet → Useless anyway!
- Application gateways: Similar; block known exploits/threats
- Write protection: Works trivially against all modifications
  - → Un-personal only if nobody is allowed access!
- Checksums/Integrity checks: Against transmission errors
  - → Note: Insecure. MAC requires key → personal security!
- Double execution with variance: Do twice and compare result
  - → Execute code two times (stack ↑,↓), perform query in different ways/other database, …
  - → Extremely difficult to circumvent, but costly!

Un-personal security - Classification

- Three main approaches possible for un-personal security
  - → Fences: Everyone is kept out/restricted
    - » "Doors" might have keys, but also other possibilities exist
      - – Physical access required, time delays etc.
    - » Only "secure" entities can pass through the "hole"
      - – Shape of the hole is important; this is not a locked door
    - » **Cat door keeps out dogs, birds, …**
  - → Automatic anonymous searches: Detecting unwanted entities
    - » = Negative personal security if matching entities are identified afterwards (if this is possible)
    - » **Metal detector in the archway + automatic door lock**
  - → Seals: Authenticity through design, not by a signature
    - » We know the issuer, but not the user
      - – Issuer might be able to identify users depending on "seal"
    - » **Guard inspects tokens issued by inhabitants**

Examples for privacy-enhanced security: Automatic anonymization

- Continuous surveillance (=personal security!) + automatic searching for suspicious activity + deletion of anything else
  - → Not completely un-personal, but going in that direction
- Example: Network intrusion detection systems
  - → Every packet on the network is investigated for content and for communication patterns
    - » Patterns are general and not person-specific (=anonymous)!
  - → If it doesn't match, it is thrown away
    - » After updating the model for "normal" behaviour, which is anonymous, i.e. independent of packets, senders, etc.
  - → If it matches, an alarm is raised
    - » Identification of the attacker might still be impossible
- Example: Video surveillance with automatic deletion after some time/if no suspicious activity was detected

Examples for privacy-enhanced security: The data safe

- A third party confirms a fact: Only un-personal towards the third party, not the single confirming one
- Personal virtual safe deposit box for electronic documents
  - → Proving something from the box: Three options
    1. Retrieve document and pass it on: Non-anonymous
    2. Allow interested person access to box/this document: Non-anon.
    3. Safe administrator confirms existence and validity to the interested third party: Seal
       - Example: Credit card payment protocols – CC company affirms validity of card&payment to merchant, but doesn't disclose card itself!
  - → Advantage of third approach: Other (or any!) data is not transmitted to the person, which still receives assurance
- Cigarette vending machines: You must be 16 in Austria
  - → Banking cards store a Bit whether this age has been reached
    - » Note: They don't disclose the birth date (which the bank knows!)
  - → Machines do not (cannot) read the rest of the card

Examples for privacy-enhanced security: Four eyes approaches/Pseudonyms

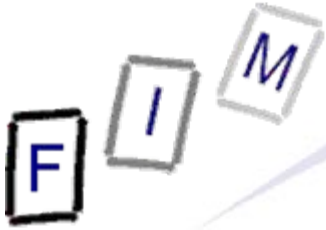
- Multiple persons are required to identify a person
  - → The identifying elements are split and stored separately
- In normal operation it is un-personal security, as nobody can identify anyone alone
  - → But possible through a special procedure, if necessary
- Example: Extensive logging, statistics
    - » Hopefully: Data retention!
  - → First part: Identifying information (IP, name, …)
  - → Second part: Rest of the data
  - → Both are connected through a random ID
- Dual approval required: Several persons must act, but everyone of them doesn't know who the others are
  - → ICT manages the necessary workflow

Conclusions

- When implementing security, think whether identification is really necessary and for whom/to what degree
  - → Anonymous tokens: Seals confirmed by a trusted third party
  - → Separating personal data: Most of the time the identification is not needed; only in case of problems!
  - → Automatic anonymisation: It won't be done manually, but after some time/event it becomes useless anyway
  - → Look for problems, not culprits: E.g. lock USB ports instead of bodily searching employees for USB sticks
  - → Blacklists or whitelists: What is more reliably to identify
    - » Ideally blacklists of persons and whitelist of behaviour!
- Un-personal security is not ideal for all situations…
  - → Better aim too high, than too low!
- More approaches to better combine privacy and security are urgently need, or ….

this might happen!

"Apparently, protecting our way of life has now become our way of life."



Questions?

Thank you for your attention!