

Online searches

Computer forensics

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>



- What is an "online search"?
 - Current investigative possibilities and their shortcomings
- Current legal state: Austria, Germany
 - The recent decision of the German BVerfG
- Potential legal problems:
 - Basic rights
 - Copyright, el. signatures, ...
- Technical implementation
 - Hardware
 - Software: Remote Forensic Software (RFS)
- Dangers and limitations



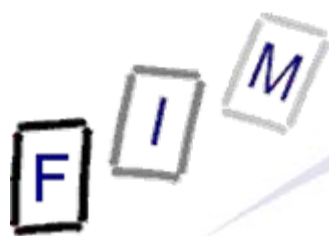
What is an "online search"?

- Online search: Investigating a computer of a suspect "over the Internet"
- Typical elements:
 - Without knowledge of the suspect (secret)
 - Inspecting data **residing on** the computer, not only that which is **sent from or to** it
 - Used to overcome cryptography and custom protocols
 - » Get at the data before/after it has been en-/decrypted
- Optional elements:
 - Without going there physically, i.e. remote installation
 - » Through hacking, infected E-Mails/websites/updates, ...
 - Realtime monitoring: Data is sent back to the police over the Internet continuously (during other online traffic)
 - Continuous monitoring \Leftrightarrow One-time remote imaging
 - By software (Remote Forensic Software, RFS)



Current investigative possibilities and their shortcomings

- Computer forensics: Impound computer and investigate
- Bugging: Copying data during transmission
 - Telephones, internet connections etc.
- Main problems are
 - Encryption: Data is sent and stored encrypted only
 - » Examples: PGP + E-Mail, Harddisk encryption, Skype (?)
 - No transmission: Plans for attacks are only stored locally but never transmitted, (hidden) physical search difficult
 - » Duplicating a large disk requires a long time!
 - Secrecy: Acquiring data without the suspect knowing it
 - » Secret physical searches are difficult and "dangerous"
 - Precautions by suspects
 - » Usually larger groups → Not everyone has a secure system



Legal state: Austria

- Ministry of the interior absolutely wants it
- 3/2008: Report by a working party of several ministries
 - Currently there is no legal basis whatsoever
 - Hidden searches as well as remote infiltration would constitute a criminal act at the moment
 - » Especially: Programming the software & deploying/using it
 - » Possible now: Listening in on communication, bugging
 - It is not completely impossible by the constitution
 - » But it would be quite difficult to do, require a lot of precautions, and could be used only rarely
 - Technical problems are not completely clear, especially regarding the value (reliability) of evidence obtained
- Legally situation is seen as comparable to Germany
 - See the recent BVerfG decision later!



Legal state: Germany

- Currently hidden online searches are illegal in Germany
 - » Decision by the BGH, GZ StB 18/06 from 31.1.2007
 - Differs from bugging and telecommunication surveillance
 - It is prohibited to combine elements from various laws allowing basic rights infraction to create a new one
- A law of Nordrhein-Westfalen allowing hidden online search found unconstitutional
 - » Decision by the BVerfG, 1 BvR 370/07 from 27.2.2008
 - Note: The decision does not disallow hidden online searches completely!
 - » Its just very difficult to match all the prerequisites
 - » The law to inspect did not match all of them
- A federal law allowing it has just been passed
 - "BKA-Gesetz"; 12.11.2008 (not yet in force!)
 - » Some states will oppose it in the Bundesrat

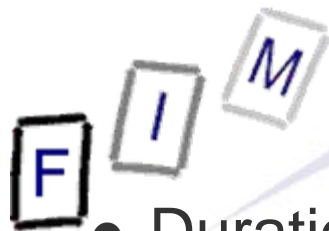


German BVerfG decision

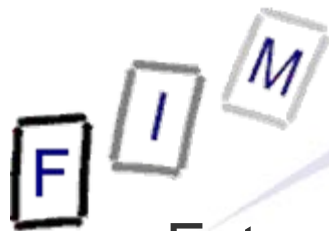
- Requirements defined by the court:
 - General basic constitutional right on the confidentiality and integrity of information systems
 - Actual evidence for a concrete danger for an outstandingly important legally protected right
 - » E.g.: Physical integrity, life, freedom of persons; common goods whose endangerment affects the foundations of the state or the existence of humans
 - » Could be possible if not yet sufficiently probable that the danger will materialize soon, but specific facts hint at a danger by specific person(s) in a concrete instance
 - Previous permission by a judge
 - Must protect the inner core of private life
- Value as evidence might be doubtful, but it need not be criminal proceedings → Usable for "investigation"



- Includes various other provisions
 - Audio/Video surveillance in private homes
 - Telecommunication surveillance
- Requirements for RFS:
 - Certain facts support the conclusion, that there are
 - » Even if there is no real proof that without this measure such a threat will materialize in the near future
 - Requires three elements: Single case, temporal closeness of conversion of threat to damage and specific person as cause
 - threats for the physical integrity, life, or freedom of persons
 - threats for common goods whose endangerment
 - » affects the foundations or the existence of the state
 - » affects the foundations of the existence of humans
 - It must be necessary and other possibilities cannot be expected to be sufficient or would be significantly more difficult



- Duration: Maximum of three months
 - 3 months extension (repeatedly, as long as necessary)
- Protection of the tools used / data collected
 - Only according to state of technology, not of science
- Does not necessarily require consent by a judge
 - If "urgent", the president of the BKA can allow it
 - » Permission must be confirmed by a judge within three days
- Excluded from surveillance are
 - Representatives, clergy, advocate of the investigated person
 - Not included: Doctors, journalists, lawyers
- Changes must be reverted after the end (autom. or man.)
- Deciding on exclusion of specially protected material
 - Done by BKA itself: Privacy officer + 2 others (one must fulfil the requirements for appointment as a judge)
 - » Note: Only the privacy officer is independent (no orders) ...



- Extensive logging:
 - Description of the software
 - » Only very generally; no technical details!
 - » BKA should store a copy of the software for possible later investigation by an independent expert
 - Identification of the system under surveillance
 - All changes made
 - » Unless purely RAM-based; This can be very difficult!
 - Must happen on the computer or be transmitted to the BKA
 - Metadata on the collected data
 - » Filename, version number, modification date, file size
 - Organisational unit performing the surveillance
- Log data may only be used for deciding on the lawfulness of the surveillance
 - Must be deleted after end of one calendar year after storage
 - » I.e., not after the end of surveillance, notice of suspect of it, ...!



Potential legal problems:

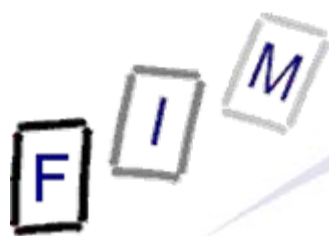
Basic rights

- Three main aspects are touched:
 - Privacy: The collection of the data as such
 - Freedom of communication: Inspecting E-Mail/VoIP(...
 - Inviolability of home: Physically installing the RFS
- Basic rights are not absolute: Appropriateness limitation
 - » Necessary, but not sufficient argumentation!
 - Public interest: Scope limited by the ECHR!
 - » Seen as problematical by the German decision
 - Suitability: Technical solution must be reliable and useful
 - Appropriateness: Less intrusive way possible?
 - » Reduced by control, oversight, etc.
- General problem: Should be available in very early stages, but need for a very strong suspicion!
 - "We don't know much, but we fear the worst!"



Fair trial: Self-incrimination

- Self-incrimination: Helping yourself in decrypting material, which might be damaging for you
 - Usually excluded: What can be obtained through compulsory powers, e.g. bodily tissue (→ DNA testing), blood samples, physical keys, etc. but exists independent of the will of the accused (motives, knowledge,)
 - » Independently existing: Can be very reliable
 - » Depends on the will of the suspect: Unreliable (lies!)
 - Here: Because "hidden" → Quite reliable (but not completely; the suspect might have caught on to the RFS!)
 - One approach: You are not required to disclose the keys, but if the police finds them out independently, they are admissible
 - » Murder weapon: Admissible; telling where it is: Disallowed
- "Bending the will": Does not happen here



Potential legal problems:

Electronic signature

- One key aspect of online searches is cryptography
 - This can be a conflict with electronic signatures!
- According to the law, the important legal consequences of a qualified electronic signature will not apply if the security measures have been compromised
 - If someone has access to the computer used for signing, he might modify the data sent to the external device used for signing, i.e. modify the content
 - » PIN/private key typically does not leave the smartcard reader, so they can not be accessed by RFS
 - These signatures are then invalid!
 - » This could mean, that a crime has not been completed, but only attempted
 - » This could lead to problems for innocent persons, where third parties could claim this



Potential legal problems: Copyright

- Copyright: RFS changes other SW to remain undetected
 - Is this allowed?
 - Currently completely unknown!
 - » There exists an exception for criminal proceedings and public security
 - » But: Exception must be seen narrowly
 - » But: Little incentive for protests from copyright owners
- Copyright for the RFS itself
 - Must probably be adhered to even then
 - » Modification of a program allowed, but the trojan must be programmed by the police, not copied from somewhere
 - Authors would not claim their work → Hacking tools are forbidden!
 - Otherwise secret services would not have to pay for any software they use, as it is employed for public security!



Potential legal problems:

Damages

- Through modifying the security elements of a computer and the modifications themselves, damages can occur
 - "Normal" search: The suspect can tell the police what might be dangerous. If he doesn't do this, surprising damages will not be compensated.
- Examples:
 - Other malware might reach the computer
 - The RFS might have a bug and damage something
 - When adding hardware, something gets broken
 - Additional costs because of the RFS communication
- Austria: Plans for a compensation obligation independent of guilt → Only causality required



Potential legal problems:

Various

- International jurisdiction: Searching computers in other countries (Laptops!) would be problematic
 - Especially with electronic "infection": Location very difficult to ascertain!
 - Searching not suspect but someone else who is communicating with him, because this person is "available"?
- Specially protected persons: It is not the area of a specific person, that is searched, but a machine
 - Which can be used by anyone, including special persons
 - Examples: Priests, medical doctors, attorneys, ...
 - » Searching their documents would be extremely difficult, if not completely illegal, in the "physical" world
 - » How to distinguish their data from that of someone else on a shared computer?
 - » How to know whether the suspect is such a person?



Technical implementation

Hardware

- Adding a hardware keylogger to the system
 - Requires physical access to the computer
 - Depending on the location (in cord/within the keyboard) they are easy/extremely hard to detect
 - Drawbacks:
 - » Radio → Easy to find
 - » Storage → Requires physical presence for data extraction; no realtime monitoring possible
 - » Difficult to evaluate the data
 - » No access to stored data, only to one newly added
 - » Detection and possession usually do not allow reuse or reengineering for other purposes
 - » Requires storage of the data on the suspect's system
 - Advantages: Reliable, proven technology, hard to detect, little potential for misuse by others
- Theoretical option: Hardware screenshot taking



Technical implementation

Hardware

- Recording electromagnetic emissions
 - Possible through the air (especially tube monitors), but also over the wires (data and power cables)
 - » Also possible indirectly: Heating pipes, air condition, ...
 - Depending on the equipment, the building, and the technology (esp. antennas) used, distances up to 500 m are possible
 - » E.g. serial data cables: 40-50 meters over the air
 - Difficult to distinguish between multiple data sources
 - No searching possible, only "viewing" what the suspect currently views and enters
 - No possibility of detection by the suspect
 - Impossible to prevent for non-experts, with normal materials, or for normal equipment
 - Depends largely on external influences (building, noise,...)
 - Misuse extremely hard (equipment expensive, use complex)



Technical implementation Software (RFS)

- Installing a software for inspections
 - Also called: "State trojan", "Remote Forensic Software"
- Allows inspection of the whole computer, i.e. remote control to execute arbitrary commands
 - Can take screenshots, log keystrokes, copy files, search disks with regular expressions, copy E-Mail, ...
 - Has access to every single bit of data on the system
 - Access to all those external systems reached/logged in to with the same rights as the user
 - » Note: External logging can be a problem then!
- Possible completely over Internet → Unknown location
- (Partially) deactivating security measures:
 - Antivirus, personal firewall, rootkit detection, ...



How to "infect" a system

- Physical visit (twice!)
 1. Gather necessary data for building a custom RFS
 2. Install RFS on the system
- Using a hack to smuggle it in
 - Known software bug (buying zero-day exploits?)
 - Update/software download (company/ISP cooperation?)
 - » ISP can modify webpages, downloads, ... on the fly
 - E-Mail attachment to be clicked on by suspect (reliable?)
- Other persons using the same computer (motivation?)
- Company/ISP personnel (legal obligation?)
- "If the police could infect my system, others might have done this too → It wasn't me!"



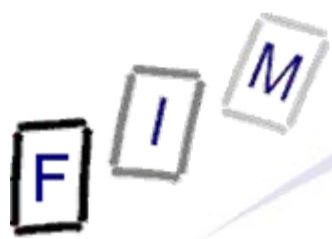
Dangers of RFS

- Detection of the RFS
 - "Feeding" the police with incorrect data (suspect, thirds)
 - Using the software for criminal activities
- Trustworthiness
 - Installation is a (usually extensive!) modification of the system to search
 - How is the person performing the search monitored?
- Detection by Antivirus/IDS
 - Not that large because of special production
- Destruction of data/evidence by installation and use
 - File system area overwritten, system integrity, speed, ...
- How to counter virtual machines?
 - Rebuilding it from a write-protected area every time?



Limitations of RFS

- Difficult to ensure targeting the correct system when installed remotely
 - E.g. E-Mail → Internet café comp. somewhere is infected
- Removing it afterwards
 - For innocents as well as criminals
 - How to remove it from backups?
 - How to ensure everything is left as it was?
- Must be built separately for each system:
 - Windows vs. Linux vs. Solaris, ...
 - Various antivirus and firewall vendors
 - Computer configuration
- Hiding the transmission of data
 - Only when other data is sent, compression (amount!)
 - None: Physical visit and no interactive gathering



Problems: Evidentiary value

- How reliable is data from a compromised system?
 - If the police could "hack" it, others could have done the same (and then put in illegal material, changed data, ...)!
- Official search: The suspect is present and can log objections, other persons are present as well
 - How to ensure that the police (or even a single policeman) cannot make changes?
 - » Can RFS be built that such changes are absolutely impossible?
- How to ensure unmodified and secure transmission?
 - Encryption + signing/checksums on suspect's computer
- Planned measures:
 - Logging (de-)installation, transmission, changes
 - » Where? How done securely? Data overwritten?
 - » To avoid arguments: "The RFS deleted/added this file"



Conclusions

- Some kind of hidden online search will be introduced
 - Securely encrypted communication must be broken somehow in some cases
- What needs to be addressed in addition:
 - Accidental finds
 - Informing communication partners and third persons
 - International aspects (partners in other countries)
 - » E.g. where listening in on a communication is illegal ...
 - Who investigates the content and excludes material which is either irrelevant or is prohibited to be used
- Technical solution quite open: Hardware/Software?
 - RFS is a dangerous terrain, as the software will "escape"

F I M

Questions?

Thank you for your attention!