

REMOTE FORENSIC SOFTWARE

Do investigators need an instrument to remotely access the computer of a suspect?

10th August 2007, Chaos Communication Camp

Dr. Marco Gercke
Lecturer at the University of Cologne, Germany
Expert for the Council of Europe

STATEMENT

“Observing private communication (by using remote forensic software) is indispensable for life.”

W. Schaeuble, Minister of the Interior, Germany

THE CURRENT DISCUSSION

- Some countries do currently discuss if secret services, police and prosecution need an instrument that enables them to secretly and remotely access computer systems
- Reports about the use of such software in Germany and the US were currently published

GEMANY

BUNDESTROJANER (www.ccc.de)

Picture removed in print version

- The Federal Prosecution requested the permission to use a remote forensic software in criminal investigations
- The Federal Court of Justice refused the request by pointing out that there is no sufficient legal basis for such instrument in the current CPC
- Within the discussion about the need for such instrument it was discovered that such software was already used by the office for the protection of the prosecution.

GEMANY

BUNDESTROJANER (www.ccc.de)

Picture removed in print version

- Within the discussion it is important to divide between the authorities that should be enabled to use the remote software:
 - Police (prevention of crime)
 - Prosecution (investigation and prosecution of crime)
 - Secret services

US

MAGIC LANTERN

Picture removed in print version

- In 2001 reports pointed out that the FBI developed a keystroke logger that can be remotely installed on the computer system of a suspect
- In 2007 the FBI requested an order to use a software (CIPAV (Computer and Internet Protocol Address Verifier) to identify an offender that used measures to hide his identity while posting threatening messages

POSSIBLE FUNCTIONS

BUNDESTROJANER (www.ccc.de)

Picture removed in print version

The remote software could be used to:

- Search for evidence on the suspects computer
- Preservation of communication data
- Keylogger
- Activation of hardware that can be used for room surveillance
- Identification of the offender

SEARCH

- The software could be used to search for illegal content (child pornography, illegal copies of copyright protected artwork, illegal software)
- In general the physical access to computer systems enables more precise forensic analyses (especially maintaining the integrity of the computer system)
- The advantage of a software that is installed via the Internet is the fact that the suspect will often not recognise the ongoing investigation (similar to telephone surveillance)
- Questionable if a secret online installation is possible - Current plans of the BKA regarding the installation are based on physical access to the computer

PRESERVATION OF COMMUNICATION DATA

VOICE OVER IP (www.skype.de)

Picture removed in print version

- The communication data are in general not stored
- Within classic search procedures the investigator cannot access these information
- An option would be the interception of communication
- This can go along with difficulties if the communication partners use encryption technology
- The software could be used to store these communication data

KEYLOGGER

PGP (www.pgp.de)

Picture removed in print version

- By using a proper encryption software and an adequate key the offenders can prevent that investigators access stored files.
- A number of countries do therefore restrict the use of encryption technology
- The keylogger could be an option to restrictions of encryption technology as it would enable the investigators to identify the key

ACTIVATION OF HARDWARE

WEBCAM

Picture removed in print version

- Installing surveillance hardware in the flat or office of a suspect goes along with the threat of detection
- The secret activation of hardware (microphone, webcam) could enable the observation without physical access to the flat

IDENTIFICATION OF SUSPECT

JAP

Picture removed in print version

- If the offender uses means of anonymous communication this can hinder the investigation
- Detecting the “real” IP-address of the offender could improve investigations

SUMMARY POSSIBILITIES

- The development of new technology allows the creation of new instruments
- A remote forensic software could improve the work of law enforcement agencies
- The permission to use the software could prevent broader prohibitions (ban on encryption technology and means of anonymous communication)

QUESTION

Possible from a technical point of view = necessary ?

TECHNICAL CONCERNS

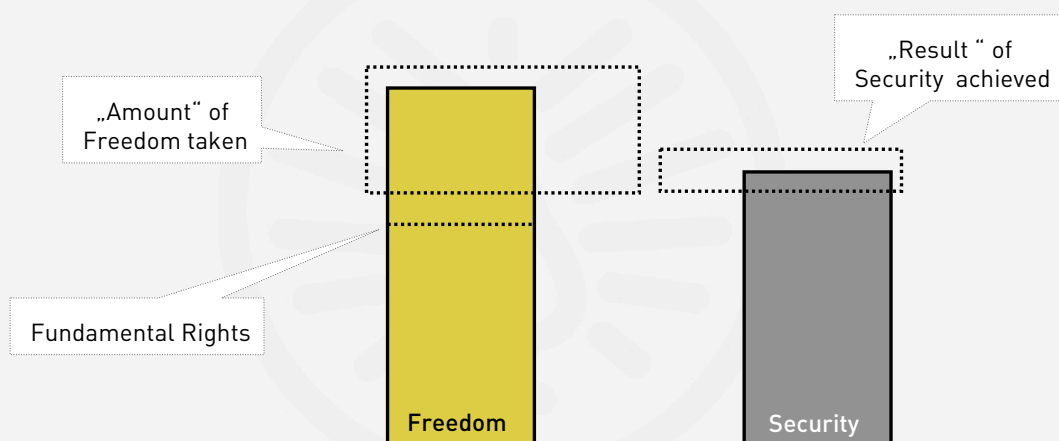
- Installation of the software is a great challenge
- Circumventing protection systems might require the cooperation between law enforcement and private businesses
- This goes along with the fear that the maximising computer security is not in the focus of state anymore

LEGAL CONCERNS

- Protection of the suspect (retreating room)
- Which crimes justify the use of such intensive instruments?
- Depending on the use (investigation outside the territory) the instrument could violate the fundamental principle of national sovereignty

LEGAL CONCERNS

- Well balanced adjustment



LEGAL CONCERNS

- Most Cybercrime have an international dimension
- The current legislative approaches are only a **national approach**
- International investigations require a harmonisation of laws

CONCLUSION

- There are serious legal and technical concerns regarding the use of such software
- It is not likely that it remote forensic tools will be useful in the majority of Internet cases
- If the instrument is implemented and limited to the most dangerous offences it could prevent the implementation of stricter laws

CONTACT

THANK YOU FOR YOUR ATTENTION



Dr. Marco Gercke
www.cybercrime.de