

# Advanced Security for Systems Engineering – VO 08: Digital Forensics

Clemens Hlauschek, Christian Schanes



**INSO – Industrial Software**

Institute of Information Systems Engineering | Faculty of Informatics | TU Wien

## End-to-end Encryption

Political Context

CLEAR Proposal

## Forensics – Anti-Forensics

Introduction

Acquire-Analyze-Present

## Limits of Cryptographic Solutions

Analysis of Encrypted Traffic

Disk encryption

# End-to-end Encryption

- Australia passes **Assistance & Access Act** (December 2018): allows to secretly compel companies and individuals to re-engineer IT Systems for spying
- EU Council agrees on e-Evidence proposal (December 2018): access data
- **FBI vs Apple** encryption dispute (2016)
- NSA/Snowden (2013): Dual\_EC\_DRBG backdoor, etc
- **Crypto War**: Crypto export restrictions (until 1996), Clipper Chip, weak SSL keys, PGP, A5/1

Secure access to encrypted storage for 3rd parties without risking mass surveillance abuse?

- Ray Ozzie (2018): CLEAR Proposal: Key escrow, per-device key pair for encrypting passcode, access to device and vendor request necessary, secure hardware to 'brick' phone: forensic r/o lock mode.
- Savage: Lawful Device Access without Mass Surveillance Risk (CCS'18): self-escrow of access credentials in secure time-vaulting hardware
- Wright: Crypto Crumple Zones (EuroSP'18): proof-of-work based solution.

# Mobile Encryption: Terms and Concepts

- Apple iPhone encryption, Secure Enclave
- Hardware Security Module (HSM)
- Key Escrow

# Forensics – Anti-Forensics

Traditionally, forensic science concerns itself with

- Gathering and analyzing of information on the past
- Using scientific methods
- To establish evidence to be used in court

Examples:

- Securing fingerprints, match to suspect
- Ballistic analysis, shooting reconstruction
- Analyzing plant pollen on clothes, establish geographic whereabouts



Digital Forensics can be defined as

*the collection and **analysis of data** from computer systems, networks, digital devices and storage media **to identify evidence** for an investigation*

- Often requires extensive domain knowledge
- Disclaimer: No legal advice in this lecture

# Digital Forensics: Broad Range of Players

- Digital forensics primarily performed by / on behalf of **government agencies**
  - Law enforcement agencies (LEA)
  - Public prosecution department
  - Intelligence agencies
- But also in the commercial sector
  - Incidence response / damage evaluation after network intrusion
  - Gather evidence for litigation
  - Industrial espionage: analyze digital data from competitor

## Digital Forensics: 3 Phases

- Acquisition
- Analysis
- Presentation

Acquisition and analysis phase dominated by technical issues,  
presentation phase depending very much on specific setting

Analogue: Take photographs of crime scene, fingerprints, blood-, DNA-samples, ...

- Copy all data to trusted storage device
- Seized device: modify device as little as possible
- Secure integrity of original data
- Calculate and store cryptographic hash of original data

# Digital Forensics: Examples Analysis Phase

- Establish progression of events by analyzing
  - Logfiles
  - Browser history
  - Filesystem metadata
- Recover deleted, hidden, or encrypted files
- Analyze Content of network traffic, cookies, ...
- Examine communication, social network graph, ...
- Detect malware, backdoors, system modifications

- Storage media data
  - EnCase
  - Forensic Toolkit (FTK)
  - SleuthKit
  
- Memory forensics
  - Volatility
  - Rekall
  
- Network forensics
  - Wireshark, tcpdump, ettercap, ...

# Digital Forensics: Presentation Phase

- Heavily dependent on setting
- For use in a court of law:
  - Document *chain of custody*
  - Document all steps, methodology, in detail
- Sometimes: *Parallel construction*
  - Original evidence collected illegally
  - Or do not want to disclose method
  - Find a second, plausible narrative
  - Practice exposed for DEA (US)
  - Possibly used in Silkroad (online drug market) case
  - Can constitute perjury

- The aim of anti-forensics is to
  - Disrupt the collection of information
  - Avoid the detection of events
  - Taunt the credibility and reliability of a forensic report
  - Mitigate effectiveness of forensic efforts
  - Add many man-hours and increase investigation costs
  
- Examples:
  - File wiping / HDD scrubbing
  - Encryption, steganography
  - Physical destruction (e.g., media, keys)



# Limits of Cryptographic Solutions

How much Information can be extracted from a dump of encrypted network traffic?

(E.g., given a dump containing only HTTPS connections and encrypted VOIP calls originating from a suspect.)

- Obviously Metadata:
  - HTTPS: Server visited. Exact time, duration of visits
  - ZRTP: Endpoints (IP-Addresses) talked to. Duration of talk. Call attempts
  - ZRTP - Signaling Data (SIP) not encrypted. Usernames of called contacts. Phone-Numbers, etc
  
- Anything Else?

*'We Kill People Based on Metadata'*

– Michael Hayden, former NSA director

# Analysis of HTTPS Traffic: Website Fingerprinting

Even if traffic is encrypted, much information can be extracted.

- Size of requests
- Number of resources requested and loaded
- Timing of different loads

Reveals much information, often for reliable fingerprinting. Extract user behavior. Extract user profile. Associate blog entries, comments with user, etc.

Use machine learning techniques and statistical analysis.

## Analysis of encrypted Traffic: VOIP

VOIP often use Variable Bitrate (VBR) codecs due to performance and quality concerns.

Thus, encrypted VOIP traffic often leaks tremendous information.

Researchers [White'11] have been able to derive approximate transcripts of VOIP conversations using techniques from computational linguistics, speech recognition and machine learning.

## Analysis of encrypted Traffic: Perfect Forward Secrecy

Assume you collect encrypted traffic generated by a suspect. Later in the investigation, you get access to private keys of important endpoints.

Can you post-mortem decrypt the collected traffic?

Usually not if **Perfect Forward Secrecy** was guaranteed by the cryptographic protocol.

Perfect Forward Secrecy (PFS) [Diffie'92]:

*An authenticated key exchange protocol provides perfect forward secrecy if disclosure of long-term secret keying material does not compromise the secrecy of the exchanged keys from earlier runs*

It is a security property of an *authenticated key exchange* protocol.

PFS in SSL/TLS:

You do not have Perfect Forward Secrecy, if you use

- RSA-based handshake
- (EC)DH-based handshake ((Elliptic Curve) Diffie-Hellman handshake with static keys)

You have Perfect Forward Secrecy, if you use

- (EC)DHE-based handshake ((Elliptic Curve) Diffie-Hellman handshake with ephemeral keys)

Other important protocols that support PFS:

Off-the-Record Messaging (OTR), Secure Shell (SSH), Signal protocol



Systems like

- TrueCrypt (VeraCrypt, CipherShed)
- Dm-crypt
- Bitlocker
- PGP Whole Disk Encryption
- FileVault

allow on-the-fly encryption/decryption of disk partitions, as well as full disks – Full Disk Encryption (FDE)

# Limits of Disk Encryption

If only data is encrypted,

- Swap partitions,
- Paging files,
- Hibernation files,
- Crash dumps

can reveal password or secret key data to the forensic analyst.

Therefore, **Full Disk Encryption** is often recommended.

# Limits of Disk Encryption

Attack Vector: Encryption/Decryption Key usually resides in RAM (since we use on-the-fly encryption)

RAM aquisition techniques:

- DMA-devices often have unrestricted memory access.
  - Forensic firewire device
  - Forensic PCMCIA device
  - PCI device

Attack Vector: Encryption/Decryption Key usually resides in RAM (since we use on-the-fly encryption)

RAM acquisition techniques:

- Cold Boot attack:
  - DRAM retains state, even after power down.
  - 1. Reboot computer into minimal Live-OS
  - 2. Acquire memory image
  - 3. Corrupted bits from AES keys can be recovered.

Protect against DMA-Attacks:

- Disable Firewire/PCMCIA kernel driver (Linux)
- Disable SRP-2 driver (MS Windows)
- Use Hypervisor with IOMMU (e.g., Xen 3.3). Allows DMA device restricted access to memory only

And:

- TRESOR, TreVisor: Runs encryption securely outside of RAM
- AES Key is loaded into, e.g., SSE registers, and never stored in RAM

# Anti-Anti-Forensics FDE

- Evil Maid Attack
- Infect MBR, BIOS
- Sidechannel Attacks to retrieve password.
  - Sound: Reconstruct password from keyboard sound
  - Camera
  - Electro-magnetic emanations

By Force of Law and other methods.

- Password disclosure law
- Intimidation
- Torture

## Anti-Anti-Anti-Forensics FDE

- TPM, Secure/Trusted Boot
- TEMPEST-shielded environment
- Jamming against electro-magnetic (acoustic?) emanations

And also

- $k$ -factor authentication
- Shared secret
- Rubber-hose secure cryptography

## Conclusion and Outlook

- Anti-Forensic / Cryptography very fragile
- Poor knowledge-transfer from theoretical cryptographers to system designers
- Help us change the situation: Make the Internet / digital devices more secure.
- Anonymity research / Tor, Cryptography, Privacy Enhancing Technologies, Exploit Mitigation



- Checkoway, et al: On the Practical Exploitability of Dual EC in TLS Implementations. Usenix Sec'14.
- Abelson, et al: The risk of key recovery, key escrow, and Trusted Third Party Encryption. WWW Journal 1997.
- Abelson, et al: Keys under doormats. Journal of Cybersecurity, 2015.
- Green: Why can't Apple decrypt your iPhone?. Online Blogpost, 2014.
- Workshop: Encryption and Surveillance (2018): <https://crypto.iacr.org/2018/affevents/legal/page.html>

- [Freiling'18] Freiling, et al: Advances in Forensic Data Acquisition. IEEE Design and Test, 2018.
- [Diffie'92] Diffie, et al: Authentication and Authenticated Key Exchanges. DCC'92
- [Chen'10] Chen, et al.: Side-Channel Leaks in Web Applications: a Reality Today, a Challenge Tomorrow. Oakland'10
- [Liberatore'06] Liberatore, Levine: Inferring the source of encrypted HTTP connections. CCS'06.
- [Gong'12] Gong, et al.: Website Detection Using Remote Traffic Analysis. PETS'12.

- [White'11] White, et al.: Phonotactic Reconstruction of encrypted VoIP conversations. Oakland'11.
- [Halderman'08] Halderman, et al.: Lest We Remember: Cold Boot Attacks on Encryption Keys. Usenix Sec'08.
- [Wetzels'14] Wetzels: Hidden in snow, revealed in thaw: Cold boot attacks revisited. Arxiv'14.
- [Bojinov'12] Bojinov, et al.: Neuroscience Meets Cryptography: Designing Crypto Primitives Secure Against Rubber Hose Attacks. Usenix Sec'12
- [Zhaung'09] Zhaung, et al.: Keyboard Acoustic Emanations Revisited. TISSEC'09.

- [Lenstra'12] Lenstra, et al.: Ron was wrong, Whit is right. 2012
- [Checkoway'14] Checkoway, et al.: On the Practical Exploitability of Dual EC in TLS Implementations. Usenix Sec'14. – <http://dualec.org/>
- [Adrian'15] Adrian, et al.: Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice. CCS'15. – <http://weakdh.org/>
- [Chen'17] Chen, et al: Secure In-Cache Execution. RAID'17.
- [Boneh] Dan Boneh (Stanford): Online Cryptography Class. <http://crypto-class.org>

**Thank you!**

<https://security.inso.tuwien.ac.at/>

