Exploiting jailbreaks in a forensic fashion

Research Project 2

Jochem van Kerkwijk

Universiteit van Amsterdam
System and Network Engineering

jkerkwijk@os3.nl

June 29, 2011

Outline

- Introduction
- Theory
  - Apple Data Protection
  - Jailbreaks
  - Computer Forensics
- Practical
  - Approach
  - Results
- Conclusion

Research Question

What are the forensic possibilities on an iOS device and what are the implications of "Data Protection" with respect to a forensic investigation?

1. What is Apple's "Data Protection"?
2. How does "Data Protection" work?
3. Can "Data Protection" be circumvented in order to access confidential data?
4. What are the possibilities to make forensic guarantees with regards to the acquisition and data-integrity of the evidence?

- If it is possible to gain access to confidential data, what kind of information can be retrieved and how can this be prevented?

Apple Data Protection

- Protects the user data on an iOS device. :o)
- Hardware encryption
  - UID - unique key per device
  - GID - unique key per model
- Software protection
  - Keybag
  - Passcode

Jailbreaks

- Gains elevated rights.[a]
- Types
  - Tethered
  - Semi-tethered
  - Untethered
- Legalized thanks to Electronic Frontier Foundation (EFF).
  - Not a copyright infringement.
  - Breaks warranty though.
- Bootrom exploit

Figure: source: theiphoneaddict.com

[a] This in contrast to an FTK sales representative who was sure jailbreaking was only used to gain access to other mobile carriers.

Computer Forensics

- Tests and techniques used to gain support evidence for a crime.
- Scientific Method.
  - Audit should be repeatable.
  - Preferably 1-on-1 copy of data carrier.
  - Work on copy only, not to taint system.
- FTK, EnCase, XRY

Zdziarski's Methodology

- Custom ramdisk in volatile memory.
  - Can be performed on any iOS device, jailbroken or not.
- SSH Server (alpine!)
- iRecovery
- Outdated, no open solution for iOS 4.x

Elcomsoft iPhone Forensics Toolkit

- Claims to be compatible with iOS 4.x
- Closed source[1].
- Available for governments and forensic agencies only.

[1] *"Dear ElcomSoft, since you're using the GPLd greenpois0n code in your product, where can I download all your source code? #gplviolations"* – Zdziarski, Tweeted 7 Jun 2011

Bédrune and Sigwald

- Presented their work at HITB last month
- Open source project
- Somewhat follows Zdziarski's method.
- Pwnd Apple's Data Protection.

Approach

- Workspace
  - iPad (1G) to mess around with
  - OSX in Virtual Machine
  - Bare metal Windows 7
- Steps
  - Exploit bootrom (Syringe / Greenpois0n)
  - Get custom environment running (RAMdisk with custom tools)
  - Gain access to encrypted file system (bruteforce passcode)
  - Create sound forensic image (bitwise if possible)
  - Compare results

Troubles

- Myself
- Some exploit tools did not work through the VM
- Compiling for iOS and getting everything together takes some time.
- Incorrect imaging and non matching hashes.

Figure: source thriftyfun.com

Results

- Passcode can be bruteforced and filesystem can be decrypted with the tools of B&S.
- Netcat dump method from B&S introduces non-identical images.
- Working version of `dcfldd`[2] for iOS devices.
- Everytime the system boots (user)data gets changed.
  - Think of files such as keychain, SMS, power management and radio.
  - and the file system journal of course.

[2] *Defence Computer Forensics Lab dataset definition*, a variant of unix `dd`.

Conclusion

- iOS Devices are meant to be secure and hardened against "human" attacks.
- There are tools out there being able to crack open your iOS device when you leave it unattended.
- Regular (hard disk) forensics does not apply.
  - Working with a live system.
  - Making identical user images prone to errors.
  - Individual file hashing offer a solution, at a different granularity in combination with proper documentation of the steps of the acquisition procedure.
- If unrestricted physical access if gained, there is no way to protect yourself.

Recommendations

- Enable the extended passcode.
- Be aware of Apples trade-off between security and usability.
- Need for additional inspection tools to ease investigation of iOS database files.

Questions?