FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

Antiforensik auf mobilen Endgeräten

Stefan Lambertz

Betreuer: Prof. Dr. Marko Schuba

IT Forensik
FH Aachen

Übersicht

- Warum Antiforensik ?
- Was ist Antiforensik ?
- Methoden der Antiforensik
- Mobile Endgeräte
- iPhone Besonderheiten
- Antiforensische Konzepte auf dem iPhone
- Fazit

Warum Antiforensik ?

- Jemand wird es tun
- Entwicklung vorgreifen
- Wissensvorsprung der anderen vermeiden
- Verbesserung der forensischen Methoden
- Kritische Betrachtung aus Sicht der Verteidigung
- Schutz berechtigter Interessen

Was ist Antiforensik ?

- Methoden und Tools die eine forensische Untersuchung erschweren oder verhindern

- Die Untersuchung muss mehr Ressourcen benötigen als dem Ermittler zu Verfügung stehen

Methoden der Antiforensik

- Datenzerstörung
  - Sicheres Löschen der Daten
- Verstecken von Daten
  - Nutzen spezieller Bereiche der Datenträger
- Transformieren von Daten
  - Steganographie
  - .jpg -> .exe
- Verhindern von Daten
  - Wo keine Daten anfallen, können keine gefunden werden

Methoden der Antiforensik

- Weisses Rauschen
  - Erzeugung großer Menge für forensische Tools auffälliger Daten
- Nebelkerzen Prinzip
  - Verdächtige, aber unwichtige Daten zur Ablenkung
- Verschlüsselung
  - Sichere Verschlüsselung verhindert das Auslesen
- Matroschka Prinzip
  - Verschlüsselter Container in Container zu dem man das Passwort übergibt
- Angriff auf forensische Tools
  - Exploits oder blinde Flecken der Tools ausnutzen

Mobile Endgeräte

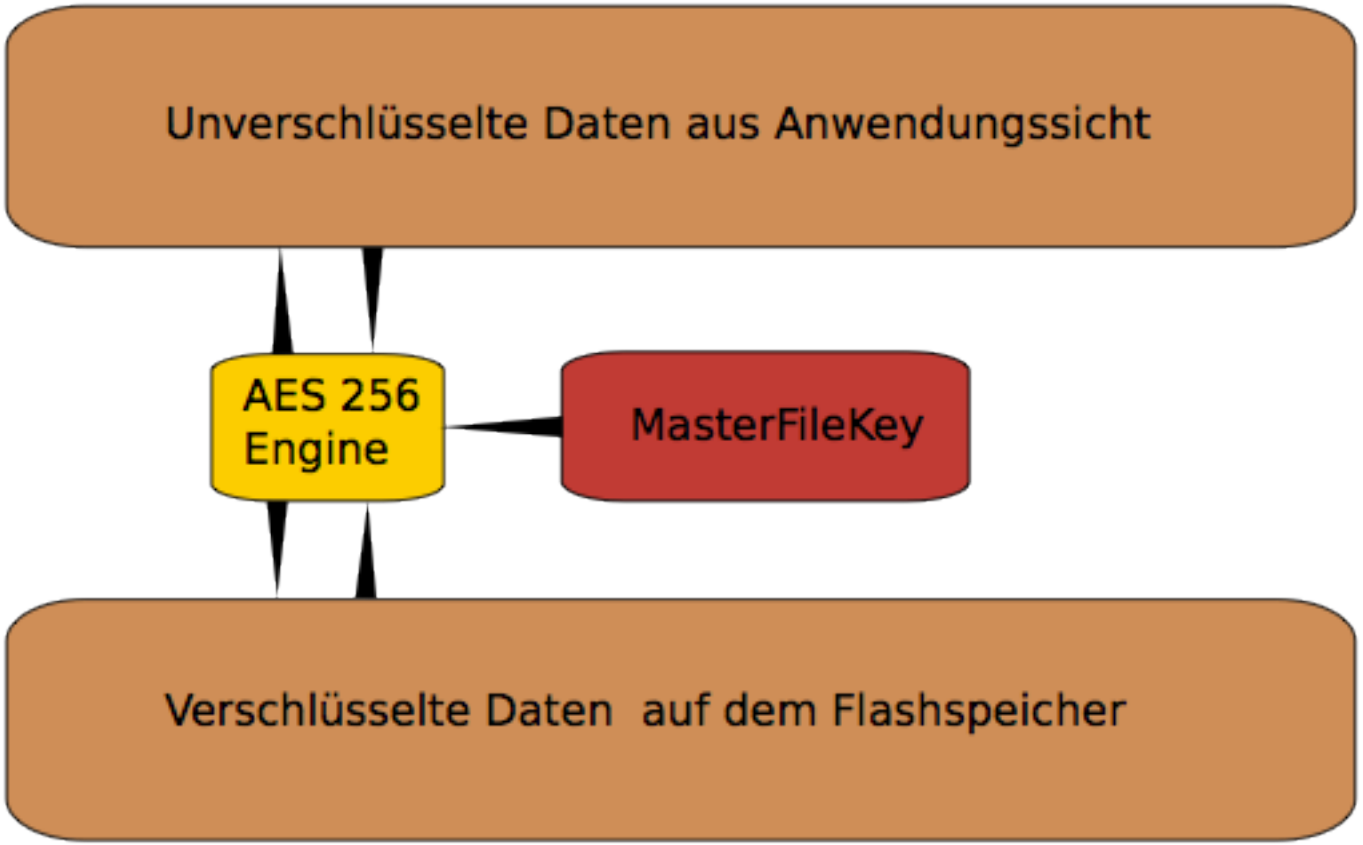
Auf dem iPhone zu finden:

- PIM
- Fotos mit GPS Koordinaten
- Google Maps Daten
- Screenshots
- Voicemail
- SMS
- Anruflisten
- 3rd Party Apps

Allg. ist der Umgang mit dem Gerät anders

iPhone Besonderheiten 1/2

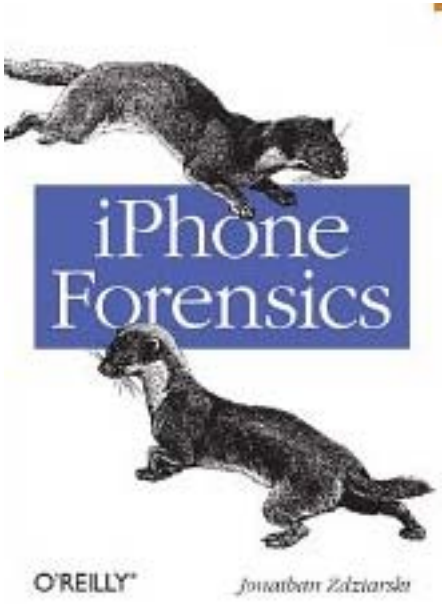
iPhone 3GS Hardwareverschlüsselung



iPhone Besonderheiten 2/2

- Read Only Systempartition
  - Nicht zu ändernde OS Daten
- Userdaten Partition
  - Alle sich ändernde Daten

- Logische Analyse
  - Über die Backup Funktion
- Physikalische Analyse
  - Zdziarski Methode



Konzepte auf dem iPhone 1/3

- Nutzung von FindMyiPhone
  - Alle Daten werden remote gelöscht
  - Sehr leicht zu verhindern
- DisableUSB
  - Verhinderung der Synchronisation über USB
  - Verhindert nur logische Analyse
  - reines Konzept
- Rootkit
  - Sehr aufwendig
  - Verhindert nur logische Analyse
  - reines Konzept

Konzepte auf dem iPhone 2/3

- EraseFreeSpace
  - Überschreiben des freien Speichers
  - Lange Laufzeit
  - Umgesetzt
- HideData
  - Ersetzen der echten Daten durch Tarndaten
  - Sicheres Ablegen der echten Daten
  - Umgesetzt
- AutoWipe
  - Löschen der Daten auf bestimmte Ereignisse hin
  - reines Konzept

Konzepte auf dem iPhone 3/3

- WhiteNoiseGenerator
  - Erzeugt möglichst viele Verdächtige Daten auf dem Gerät
  - Daten die ein Mensch sortieren muss
  - Reines Konzept
- UseUnsuspiciousPlaces
  - Daten auf der normalerweise ReadOnly Partition
  - Umgesetzt

Fazit

- Antiforensik auch auf mobilen Endgeräten
- Hersteller implementieren immer mehr selbst
- Wichtig ist es den verbundenen Rechner mit zu beschaffen und das Gerät abzuschirmen

Ende

Vielen Dank

für

ihre Aufmerksamkeit

Email: Stefan.Lambertz@alumni.fh-aachen.de

Literatur

LITERATUR

B. X. Chen, “Hacker says iphone 3gs encryption is ‘useless’ for businesses.”

M. Dan Frakes, “Inside iphone 3.0’s remote wipe feature.”

A. Developer, “ios 4: Understanding data protection.”

——, “iphone in business security overview.”

K. S. Andrew Hoog, “iphone forensics white paper.”

A. Vance, “The iphone 3gs and forensics: Encryption changes the game?”

A. Developer, “Wwdc 2010 session 209 - securing application data.”

J. Zdziarski. O’reilly webcast: iphone forensics-live recovery over usb.

——. O’reilly webcast - part 2 - iphone forensics 3g[s]. [Online].Available: http://www.youtube.com/watch?v=mvXi1CZFBT0

R. R. Kubasiak and S. Morrissey, Mac OS X, iPod, and iPhone Forensic Analysis DVD Toolkit, 1st ed. Syngress, 12 2008.

J. Zdziarski, iPhone Forensics: Recovering Evidence, Personal Data, and Corporate Assets, 1st ed. O’Reilly Media, 9 2008.

B. Blunden, The Rootkit Arsenal: Escape and Evasion in the Dark Corners of the System, 1st ed. Jones Bartlett Publishers, 5 2009.

E. Sadun, The iPhone Developer’s Cookbook: Building Applications with the iPhone 3.0 SDK (2nd Edition)

http://www.nonwovenmasks.com/pic/20105894422.jpg