Computer Forensik

Lerneinheit 4: Fall 3: Android Malware

Prof. Dr. Christoph Karg

Studiengang Informatik
Hochschule Aalen

Wintersemester 2013/2014

Ausgangssituation

- Auf einem Android Smartphone wurde eine verdächtige App entdeckt. Die APK-Datei der App liegt vor
- Es liegt ein Netzwerkmitschnitt als PCAP Datei vor
- Es wird vermutet, dass sich der Angriff im lokalen Netzwerk abgespielt hat

Zu klärende Fragen

1. Welche Systeme (gekennzeichnet durch IP-Adressen) waren in den Vorgang involviert?
2. Welche Kommunikation fand zwischen den Systemen statt?
3. Gibt es in der Android App irgendwelche Unstimmigkeiten?
4. Auf welchem der Systeme ist die App aktiv gewesen?

Zu klärende Fragen (Forts.)

5. Hat die App Daten übertragen?
6. Falls ja, wie wurden die Daten verschlüsselt?
7. Falls ja, kann man die Daten entschlüsseln?
8. Welche Aktionen hat die App auf dem Handy ausgeführt?
9. Wie läuft die Kommunikation der App mit dem Server ab?

Nützliche Werkzeuge

- Wireshark/TShark $\rightsquigarrow$ Analyse des Netzwerkmitschnitts
- dex2jar $\rightsquigarrow$ APK Datei in eine JAR Datei konvertieren
- JD-GUI $\rightsquigarrow$ Sourcen in einer JAR-Datei anzeigen
- Eclipse $\rightsquigarrow$ Java Entwicklungsumgebung
- Google $\rightsquigarrow$ Recherche