FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

Analyse von Triplog-Dateien bei TomTom Navigationssystemen

Sebastian Braun

Lehrgebiet Datennetze, IT-Sicherheit und IT-Forensik

IT Forensik
FH Aachen

Übersicht

Aufgabenstellung

Analyse mit einem Hexeditor

Weiterführende Recherche

Reverse Engineering

Ausblick

Aufgabenstellung

- Was sind Triplog-Dateien?
  - Dateien zur Erfassung anonymer Nutzungsstatistiken
  - Speichert Position alle 5 Sekunden
    - Zeitstempel als Unix-Timestamp
    - Koordinate als Longitude/Latitude
- Problem: Dateien werden verschlüsselt auf dem Gerät gespeichert
  - Welcher Verschlüsselungsalgorithmus wird verwendet?
  - Gibt es Schwachstellen in der Implementierung?
  - Nur Cellebrite kann Triplog-Dateien entschlüsseln

Analyse mit einem Hex-Editor I

- Triplog Dateien je nach Gerät verschieden aufgebaut
  - Unterschiedliche Magicbytes

Offset	0	1	2	3	4	5	6
00000000	09	8D	00	05	00	00	00

Offset	0	1	2	3	4
00000000	01	13	00	03	00

- Header vermutlich Byte 0-28 oder 0-38
  - Application Version & Application Version Version Number im Header

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
00000000	01	13	00	03	00	59	EE	60	83	D6	D5	5B	71	DF	DB	1B
00000016	00	00	23	21	00	00	00	00	00	00	00	0A	08	00	BC	68
00000032	47	DE	37	40	CE	C6	0B	2B	00	A9	F6	98	F4	BD	BA	6B

Analyse mit einem Hexeditor II

- wiederkehrende Struktur innerhalb verschlüsselter Triplog-Dateien
  - Je größer Datei, desto mehr dieser Strukturen
  - Zusammenhang mit Timestamp
    - Hashwert
    - Wichtig zur Entschlüsselung?

```
00000080  56 A1 8B D1 1A 45 8D 12  C6 06 05 00 4B 63 EB 06
00000096  30 F2 51 89 0E 70 01 02  49 D6 86 32 57 B7 A6 09
```

Weiterführende Recherche

- Hinweise auf Public-Key Verfahren
  - Peter Hannay – Geo Forensics: Classes of Locational Data Sources for Embedded Devices

    (International Journal of Engineering and Technology)
  - Armando Faggiano, Ermanno Travaglino – GPS Forensics Un caso di studio: TomTom

- Hinweise auf Fehlimplementierung
  - Yuval Ben-Moshe – Challenges in Physical Extraction of Modern Smartphones and Advance Methods to overcome (SANS Digital Forensics Summit)

Reverse Engineering I

- Extraktion der Software aus ttsystem
  - Nach Vorlage des CCC
  - Blowfish wird zur Imagesignatur verwendet
    - Fest kodierter Key
- Dekompilierung mit IDA Pro
- Suche nach diversen Strings
  - Unter anderem Fund von 23CTripEncryptionBlowFish, 23CTripEncryptionStrategy, 22CDailyTripFileStrategy

```
a23ctripencry_0 DCB "23CTripEncryptionBlowFish",0 ; DATA XREF: .rodata:0...
a23ctripencrypt DCB "23CTripEncryptionStrategy",0 ; DATA XREF: .rodata:00...
aTriplog04d02d0 DCB "triplog-%04d-%02d-%02d.dat",0 ; DATA XREF: sub_1...
                DCD a17ctripfilestr    ; "17CTripFileStrategy"
                DCD a22cdailytripfi    ; "22CDailyTripFileStrategy"
a22cdailytripfi DCB "22CDailyTripFileStrategy",0 ; DATA XREF: .rodata:00473B...
```

Reverse Engineering II

- Suche nach Verschlüsselungsalgorithmen, außer Blowfish, blieb erfolglos
  - Kein Public-Key Verfahren gefunden
- Suche nach typischen Blowfishkonstanten war erfolgreich

```
dword_478A3C    DCD 0xD1310BA6, 0x98DFB5AC, 0x2FFD72DB, 0xD01ADFB7, 0xB8E1AFED
                                ; DATA XREF: sub_21B084:loc_21B0C8↑o
                                ; .text:off_21B208↑o ...
                DCD 0x6A267E96, 0xBA7C9045, 0xF12C7F99, 0x24A19947, 0xB3916CF7
                DCD 0x801F2E2, 0x858EFC16, 0x636920D8, 0x71574E69, 0xA458FEA3
                DCD 0xF4933D7E, 0xD95748F, 0x728EB658, 0x718BCD58, 0x82154AEE
                DCD 0x7B54A41D, 0xC25A59B5, 0x9C30D539, 0x2AF26013, 0xC5D1B023
                DCD 0x286085F0, 0xCA417918, 0xB8DB38EF, 0x8E79DCB0, 0x603A180E
```

Ausblick

- Blowfish wichtigster Anhaltspunkt
  - Welcher Betriebsmodus wird verwendet?
  - Was ist der Payload der Datei?
- durch Reverse Engineering Rückschlüsse auf verwendeten Key
- „Trial and Error“

Ende

Vielen Dank für Ihre Aufmerksamkeit!

Kontakt: sebastian.braun@alumni.fh-aachen.de