Forensische Analyse proprietärer Hardware – Untersuchung und Extraktion relevanter Daten

Studiengang: MAS Digital Forensics & Cyber Investigation

Diese Arbeit untersucht eine proprietäre Hardware-Plattform mit dem Ziel, zu bestimmen, ob forensisch relevante Daten direkt auf der Hardware gespeichert sind. Dazu wurden die verbauten Komponenten, das Betriebssystem, die Applikation und die Kommunikation zwischen den Systemkomponenten analysiert. Basierend auf diesen Erkenntnissen wurden Methoden zur nicht-invasiven Extraktion relevanter Daten entwickelt, die eine gezielte Sicherung und Untersuchung ermöglichen.

Herausforderung und Zielsetzung der Untersuchung

Die Analyse proprietärer Hardware im forensischen Kontext stellt besondere Herausforderungen dar, insbesondere wenn Dokumentationen fehlen oder spezifische Schutzmechanismen den Zugriff erschweren. Ziel dieser Arbeit war es, zu ermitteln, ob forensisch relevante Daten direkt auf der Hardware gespeichert sind und wie diese extrahiert werden können. Hierzu wurden verschiedene Untersuchungsbereiche definiert:

- die Hardware selbst
- das Betriebssystem
- die Applikation
- die Kommunikation zwischen diesen Komponenten

Hardware-Analyse

Zunächst erfolgte eine detaillierte Analyse der Hardware, um zentrale Komponenten, Speicherbereiche und Schnittstellen zu identifizieren. Die Untersuchung konzentrierte sich auf die verbauten Flash-Speicher und EEPROMs sowie deren Zugriffsmöglichkeiten. Methoden wie In-System Programming (ISP), JTAG und Chip-Off wurden getestet, um herauszufinden, ob auf die gespeicherten Daten zugegriffen werden kann und in welcher Form diese vorliegen.

Betriebssystem-Analyse

Das Betriebssystem basiert auf einer modifizierten Linux-Umgebung mit einem angepassten SquashFS-Dateisystem. Die Analyse umfasste den Bootprozess, den Kernel und die Dateisystemstruktur. Dabei stellte sich heraus, dass einige Mechanismen den direkten Zugriff auf gespeicherte Daten erschweren. Durch gezielte Systemmanipulationen konnte jedoch Root-Zugriff erlangt werden, wodurch eine detaillierte Untersuchung der gespeicherten Daten möglich wurde.

Applikations-Analyse

Die proprietäre Applikation, die auf der Hardware betrieben wird, wurde auf ihre interne Datenverarbeitung und Steuerungsfunktionen hin analysiert. Dabei zeigte sich, dass sie über eine spezifische Schnittstelle mit der Hardware kommuniziert und dabei Steuerbefehle sowie Statusinformationen verarbeitet. Wichtige Daten wurden nicht ausschliesslich im Betriebssystem, sondern auch direkt auf der Hardware gespeichert und konnten durch gezielte Steuerbefehle extrahiert werden.

Entwicklung von Extraktionsmethoden

Basierend auf den gewonnenen Erkenntnissen wurden Methoden zur automatisierten und nicht-invasiven Datenextraktion entwickelt. Diese kombinieren hardware- und softwaregestützte Verfahren, um mit minimalem Eingriff eine effiziente Sicherung forensisch relevanter Daten zu ermöglichen. Der Schwerpunkt lag auf der Nutzung bestehender Schnittstellen, um den Zugriff auf gespeicherte Informationen zu erleichtern.

Ergebnisse

Die Untersuchung zeigt, dass forensisch relevante Daten tatsächlich direkt auf der Hardware gespeichert sind und unter bestimmten Bedingungen extrahiert werden können. Die entwickelten Methoden und Werkzeuge ermöglichen eine gezielte Sicherung dieser Daten für weitere forensische Analysen. Die Ergebnisse sind spezifisch für die untersuchte Plattform, können aber als Grundlage für die Bewertung vergleichbarer Systeme dienen.

Gaston Hänni
gaston.haenni@gmail.com

Florian Kaufmann
flo@floka.com