

Bachelor-/Masterarbeit

Benchmarking von Firmware-Rehosting-Ansätzen

Ziel

Um Embedded-Firmware effizient zu analysieren und zu fuzzen, wird sie zunehmend ohne die echte Hardware in einer Emulationsumgebung ausgeführt (**Rehosting**). Dafür gibt es zahlreiche Open-Source-Ansätze, etwa FirmAE oder Greenhouse für Linux-basierte Firmware sowie HALucinator, P2IM oder Fuzzware für Mikrocontroller-Firmware. In der Praxis scheitert die Emulation jedoch häufig, z. B. an unbekannter Peripherie, fehlender Hardware-Konfiguration, Interrupts oder Integritätsprüfungen. Welcher Ansatz für welche Art von Firmware geeignet ist, lässt sich bisher kaum vergleichen.

Ziel dieser Arbeit ist es, ausgewählte Open-Source-Rehosting-Werkzeuge **miteinander zu vergleichen**. Dazu wird ein **Benchmark** entwickelt, der verschiedene Firmware-Typen, Architekturen und Betriebssysteme abdeckt und die Ergebnisse anhand geeigneter Metriken bewertet. Es soll herausgearbeitet werden, welche Ansätze mit welcher Firmware gut funktionieren und **woran die Emulation scheitert**. Als Anwendungsfall dient das **Fuzzing von Embedded-Firmware**. Das genaue Thema wird nach Absprache festgelegt. Mögliche Schwerpunkte:

- Aufbau eines Firmware-Korpus und automatisierte Benchmark-Umgebung
- Metriken für den Rehosting-Erfolg (z. B. Boot-Fortschritt, erreichbare Dienste)
- Systematische Analyse und Klassifikation von Fehlerursachen
- Eignung der Ansätze für das Fuzzing (z. B. Durchsatz, Coverage, Crashes)

Anforderungen und Voraussetzungen

- Einarbeitung in Firmware-Rehosting, Emulation (z. B. QEMU) und Fuzzing
- Inbetriebnahme und Einordnung bestehender Rehosting-Werkzeuge
- Konzeption und Implementierung eines Benchmarks
- Durchführung und Auswertung des Vergleichs
- Linux-Erfahrung, Programmierkenntnisse (z. B. Python, C), Interesse an Embedded Security

Ansprechpartner

Prof. Dr. Lothar Braun | ✉ lothar.braun@tha.de | ☎ +49 8215586-3378

THA_innos

Das Institut für innovative Sicherheit (THA_innos) bietet eine Vielzahl von Abschluss- und Projektarbeiten im Themenfeld der Cyber Security an. Unser Team unterstützt Studierende dabei mit Know-How und Praxiserfahrung und ist zudem offen für eigene Themenvorschläge. Durch die enge Zusammenarbeit mit der Forschungsgruppe vor Ort im MRM-Gebäude lernen Studierende sowohl das Institutsleben, als auch die aktuelle Forschung von THA_innos kennen.

Weitere Informationen auch unter <https://innos.tha.de>