Proposal Masterarbeit

Untersuchung von Methoden für die Firmware-Analyse von eingebetteten Linux Geräten als Vorbereitung für Sicherheitstests / Fuzzing

Michael Kraus
kraus17@hm.edu

Betreuer: Prof. Dr. Lars Wischhof

Hochschule für angewandte Wissenschaften München
Masterstudiengang Informatik

1 Hintergrund:

Hintergrund dieser Forschungsarbeit ist die tägliche Arbeit eines Teams von Penetrationtestern im IoT-Umfeld bei Siemens Corporate Technology. Dabei müssen immer wieder eingebettete Geräte auf ihre Sicherheit überprüft werden. Gerade im IoT-Umfeld handelt es sich oft um Linux-basierte Geräte, die sowohl eine Netzwerkschnittstelle haben, als auch unverwalteten, hardwarenahen Code ausführen. Diese Umstände machen das Thema Fuzzing sehr interessant. Um ein Gerät fuzzen zu können, oder andere Untersuchungen durchzuführen, sind oft sehr aufwändige Vorbereitungen nötig.

2 Thema:

Um diese Arbeit zu erleichtern, soll erforscht werden, ob und wie einige Arbeitsschritte bei der Vorbereitung von eingebetteter Firmware für Sicherheitstests automatisiert werden können. Dazu muss die Firmware zunächst entpackt und analysiert werden. Lässt sich das Zielsystem emulieren? Was läuft zur Laufzeit auf dem System? Wie, wo und wann werden Programme gestartet? Können diese Programme gefunden, extrahiert und/oder gestartet werden? Welche Kommunikationskanäle gibt es? Was ist zu tun, um das System auf Sicherheitslücken zu überprüfen? Wie können die Programme am schnellsten an ein bereits existierendes Fuzzing Framework angebunden werden? All diese Fragen beschäftigen den Penetrationtester bei seiner Arbeit und kosten jedesmal sehr viel Zeit. Dabei gibt es vielleicht einiges an Automatisierungspotenzial. Dies soll hier untersucht werden. Neben der Entwicklung einer prototypischen Anwendung sollen die folgenden Fragestellungen im Fokus stehen.

3 Forschungsfragen:

- Erkennung der im Betrieb laufenden Programme
  Ist es möglich, die im Betrieb laufenden Programme einer Firmware zu erkennen? Dazu müssen zunächst geeignete Methoden gefunden und evaluiert werden. Diese können sowohl statischer als auch dynamischer Natur sein. Also eine Erkennung durch reine Analyse des Image und seines Dateisystems oder durch Virtualisierung des Systems. Kann die Mehrzahl der für Security Assessments relevanten Programme in den Beispielen für typische Siemens Endgeräte gefunden werden?

- Generierung von Schnittstellen aus den Ergebnissen
  Sind die Informationen über die gefundenen Programme im Ergebnis ausreichend, um Schnittstellen zu erkennen? Nach einer Auswertung und Prüfung der Ergebnisse soll versucht werden, diese auch zu nutzen und Aufgaben in Security Assessments zu automatisieren. Können bereits einige der Programme vollautomatisch mit Security Tools angegriffen werden? Kann eine Schnittstelle für die Anbindung an ein Fuzzing Framework generiert werden?

4 Related Work:

- Fraunhofer FACT
- FAT
- Firmalyzer
- firmadyne

Es gibt bereits einige Forschungsarbeiten, Quellen und Tools, die sich mit den Themen Firmware-Analyse und Virtualisierung mit QEMU beschäftigen. Diese Arbeit soll nicht wiederholt, sondern aufgegriffen werden. Nur ein kleiner Teil davon bildet bereits eine ausreichende Grundlage, um in Security Assesments eingesetzt zu werden. Es soll ein größtmöglicher Teil aus den gängigen Open Source Tools wiederverwendet, evaluiert und kombiniert werden, und im Bereich automatisierte Sicherheitsprüfung als Basis für neue Einsatzmöglichkeiten dienen. Fragen und Einschätzungen zu diesen Technologien sollen nur am Rande betrachtet werden, lassen sich aber nicht ganz vermeiden, da als erster Schritt meist eine Virtualisierung des vorliegenden Image nötig ist. Inwieweit lässt sich die Firmware gängiger eingebetteter Linux Geräte aus dem Siemens Portfolio überhaupt mit QEMU virtualisieren?

5 Ziele:

Hauptziel ist, konkrete Antworten, Aussagen und Einschätzungen auf die Forschungsfragen zu finden und dabei insbesondere zu klären, wie das Thema in Zukunft verfolgt werden soll. Kann eine Basis für weitere Forschung geschaffen werden? Soll das Thema überhaupt weiter verfolgt werden? Außerdem soll zur Erarbeitung und Verdeutlichung der Ergebnisse ein prototypisches Programm entwickelt werden. Die entwickelten Funktionalitäten sollen im besten Fall bereits die tägliche Arbeit in Security Assesments erleichtern und einige Aufgaben bei der Vorbereitung und Analyse von typischen Embedded Linux Geräten automatisieren. Gerade im Bereich Fuzzing ist noch sehr viel händische Vorbereitung nötig. Das Tool soll im Rahmen der Masterarbeit in erster Linie dazu dienen, verschiedene Konzepte zur Beantwortung der Forschungsfragen auszutesten und dadurch Einschätzungen bezüglich der Verwendung der verschiedenen Mechanismen liefern. Nach Möglichkeit sollen also verschiedene betrachtete Methoden bereits prototypisch implementiert werden.

6 Organisatorisches:

Zeitrahmen: Sommersemester 2019, Teilzeitstudent, Forschungsprojekt bei Siemens CT, Eigene Gestaltung (Open-Source Projekt)

Michael Kraus, 12.06.2019