Bachelorarbeit

Protokollimplementierungen für Fuzzer

Ziel

Fuzzing ist eine etablierte Technik zur Aufdeckung von Sicherheitslücken in Software, bei der Programme gezielt mit fehlerhaften oder unerwarteten Eingaben getestet werden. Insbesondere im Bereich der Netzwerksicherheit hat Fuzzing an Bedeutung gewonnen, da hier Protokolle und Schnittstellen oft komplex und sicherheitskritisch sind.

Ziel der Bachelorarbeit ist die Entwicklung von Protokollimplementierungen für den Netzwerkfuzzer BooFuzz[1], um Schwachstellen in industriellen Kommunikationsprotokollen wie Profinet aufzudecken. Dabei sollen ausgewählte Protokolle aus dem Bereich der industriellen Automatisierung zunächst analysiert werden, bevor spezifische Fuzzing-Skripte implementiert werden. Diese Skripte sollen anschließend in einer Testumgebung mit realen industriellen Geräten erprobt werden, um die Wirksamkeit des Ansatzes zu evaluieren.

Die Ergebnisse der Arbeit sollen dazu beitragen, Sicherheitslücken in industriellen Protokollen zu identifizieren und eine Grundlage für zukünftige Sicherheitsverbesserungen zu schaffen.

Anforderungen und Voraussetzungen

- Erfahrung mit Python, da BooFuzz in Python entwickelt wird
- Grundlegende Kenntnisse in Netzwerktechnologien
- Interesse an IT-Sicherheit und Netzwerksicherheit

Ansprechpartner

Prof. Dr. Lothar Braun | lothar.braun@tha.de | +49 821 5586-3378

[1] https://github.com/jtpereyda/boofuzz

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`