Fuzzing von Industriellen Geräten zur Identifikation von Denial-of-Service Schwachstellen

Ziel

Industrielle Geräte werden in vielen kritischen Infrastrukturen und in der industriellen Produktion zur Steuerung der physikalischen Prozesse eingesetzt. Angreifer einer solchen Infrastruktur sollten nicht in der Lage sein, den Ablauf des Prozesses durch das Senden von Netzwerkverkehr zu stören.

Durch Fehler in der Programmierung der Geräte kann es jedoch passieren, dass ein gezielt durch einen Angreifer erstelltes Netzwerkpaket einen sogenannten Denial-of-Service erzeugt. Das Gerät stellt daraufhin den Dienst ein und der physikalische Prozess kann nicht mehr weiter gesteuert werden. Hersteller und Betreiber der Geräte möchten dies natürlich vermeiden und solche Programmierfehler möglichst schnell finden und beheben.

Fuzzing ist eine Methode, mit der solche Fehler in verschiedenster Software identifizierte werden kann. Im Rahmen der Abschlussarbeit sollen Fuzzing-Tests für verschiedene industrielle Protokolle entwickelt werden. Hierzu sollen zunächst einige relevante Protokolle aufgearbeitet und verstanden werden. Im Anschluss sollen Tests im Framework *BooFuzz* entwickelt und in einem Laboraufbau mit echten industriellen Geräten getestet werden.

Anforderungen und Voraussetzungen

- Programmierkenntnisse in Python
- Grundlagen der Datenkommunikation

Ansprechpartner

Prof. Dr. Lothar Braun | lothar.braun@hs-augsburg.de | +49 821 5586/0000

HSA_innos

Das Institut für innovative Sicherheit (HSA_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 HSA_innos kennen.

Weitere Informationen auch unter www.hsainnos.de