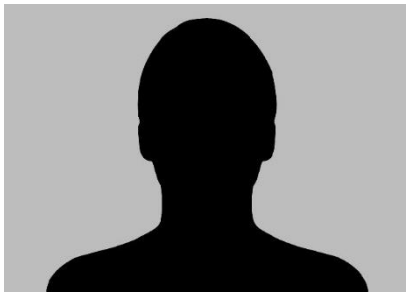
Zürcher Hochschule
für Angewandte Wissenschaften

School of
Engineering

InIT Institut für angewandte
Informationstechnologie

Red teaming einer sicheren Infrastruktur im Bereich Gebäudeautomation [IoT]



Diplomierende
Cédric Bühler
Marco Studerus

Dozent
Stephan Neuhaus

Das Internet of Things (IoT) findet bereits Anwendung in unterschiedlichsten Bereichen, so auch in der Gebäudeautomation. Es ist wünschenswert, IoT-Geräte autonom und sicher in ein solches Gebäudenetzwerk aufnehmen zu können. Die IETF-Arbeitsgruppe ANIMA beschreibt in einem RFC-Entwurf ein Protokoll, bei dem Geräte mithilfe von digitalen Identitäten autonom und wechselseitig authentifiziert in ein Netzwerk eingebunden werden können. Die Umsetzung eines Prototyps am Institute of Embedded Systems (InES) der ZHAW soll die Realisierbarkeit aufzeigen. Es soll untersucht werden, ob einerseits das Protokoll Sicherheitsrisiken aufweist und anderseits der Prototyp sicher implementiert wurde.

Mit einem Red Teaming wurde dies vertieft untersucht. Der verfügbare RFC-Entwurf und die verwendete Mesh-Netzwerktechnologie wurden analysiert und daraus potenzielle Schwachstellen abgeleitet. Der Prototyp des InES wurde umfangreich auf Sicherheitslücken getestet.

Boarder Router des Mesh-Netzwerks OpenThread

Durch die durchgeführten Angriffe konnten verschiedenste Handlungsempfehlungen ausgearbeitet werden. Diese tragen massgeblich dazu bei, die Sicherheit und Qualität des Entwicklungsprozesses zu optimieren.

Statische und manuelle Quellcodeanalysen ergaben, dass Daten ohne Prüfung der Länge in einen Buffer geschrieben werden. Daraus resultierte ein Proof-of-Concept bei dem ein Buffer-Overflow während des Verarbeitens von UDP-Paketen ausgenutzt werden kann. Dies ermöglicht, den internen Zustand des Programmes zu verändern, sodass Variablen sicherheitsrelevanter Bibliotheken manipuliert werden können.

Leaf Node mit nRF52840-Board

Aus diesem Red Teaming folgt, dass grundlegende Mängel in der Sicherheit dieses Protokolls zur autonomem Bereitstellung von Geräten festgestellt wurden. Weiter konnten aufgrund von Bugs in der Implementation Angriffe auf die entwickelte Applikation und beteiligte Frameworks durchgeführt sowie sicherheitsrelevante Mängel an einem externen Service festgestellt werden.