Zürcher Hochschule
für Angewandte Wissenschaften

School of Engineering

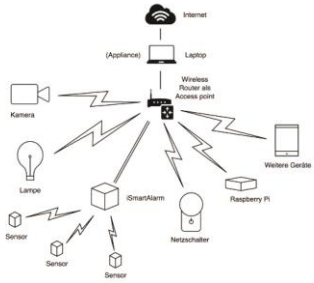
InIT Institut für angewandte Informationstechnologie

Appliance zur Erkennung von Sicherheitslücken auf Consumer IOT

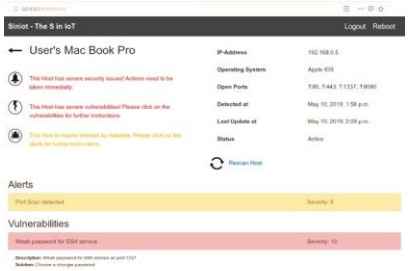
Durch die steigende Vernetzung von elektronischen Geräten und dem Bedarf an Automatisierungslösungen hat das Themenfeld des Internet of Things (IoT) stark an Bedeutung gewonnen. Die ständige Verbindung vieler Heimgeräte zum Internet rückt den Verbraucher in den Fokus von Cyberkriminellen, die IoT-Geräte z. B. für Botnetzwerke oder zum Stehlen von persönlichen Daten missbrauchen. Diese Arbeit zeigt, dass dieses Problem durch eine Appliance, die das Heimnetzwerk des Benutzers auf Sicherheitslücken und Angriffe überwacht, entschärft werden kann. Zu diesem Zweck wurde ein Prototyp einer solchen Appliance entwickelt, in eine praxisnahe Testumgebung integriert und seinen Nutzen evaluiert.
Der Prototyp ist in skalierbare Komponenten aufgeteilt. Er detektiert mit Nmap, einer führenden Port-Scanning-Applikation, die dem Netzwerk angeschlossenen Geräte. Die detektierten Geräte werden mit OpenVAS, einer verbreiteten Software zum Aufspüren von Sicherheitslücken, auf Schwachstellen gescannt. Mit Suricata, einem Echtzeit-Angriffserkennungssystem, sucht der Prototyp nach potenziellen Angriffen auf das Netzwerk. Die Gefahren werden dem Benutzer auf einer lokalen Webseite angezeigt.
Der Prototyp erkennt allgemeine Sicherheitslücken wie z. B. schwache Passwörter und steigert durch das Schaffen von mehr Transparenz das Bewusstsein des Benutzers über Cybergefahren. Er hat aber noch Schwächen. Einerseits generiert er viele Fehlwarnungen, weil kein Algorithmus existiert, der die Warnungen zuverlässig filtert. Andererseits sind nur wenige IoT-spezifische Sicherheitslücken und Angriffe bekannt, wes-halb der Prototyp keinen Komplettschutz bietet. Um dem entgegenzuwirken, braucht es bessere Tests zum Erkennen von Sicherheitslücken und verdächtigem Verhalten von IoT-Geräten. Die Entwicklung von sicheren IoT-Produkten und die Zusammenarbeit zwischen Herstellern und Sicherheitsexperten sind Voraussetzungen, um Konsumenten zuverlässig vor Cybergefahren zu schützen.

Diplomierende
Jonas Maag
Flavio Beno Nicki Viazzoli

Dozierende
Ekkehard Peter Berlich
Marc Rennhard



Aufbau der praxisnahen Testumgebung



Detailinformationen zu einem Host im Webinterface des Prototyps mit Angriffswarnungen und Sicherheitslücken