Penetration Test für IoT-Geräte

Zugehöriges Modul

Diese Aufgabe kann im Rahmen des Moduls „**Neueste Entwicklungen in der Informatik**“ im Master-Studiengang durchgeführt werden.

Hintergrund

Im Projekt “EMERGE IoT” arbeiten wir gemeinsam mit dem Landeskriminalamt Mecklenburg-Vorpommern an der Verbesserung der Sicherheit von IoT-Systemen. Erfahrungsgemäß zeigt sich oft, dass in der Software solcher Systeme eklatante Sicherheitsmängel bestehen.

Immer mehr Leute lassen sich durch smarte Helfer wie Staubsaugroboter unterstützen. Im Rahmen des Projekts wurde daher ein iRobot Roomba 960 beschafft. Dieser kann mithilfe einer Kamera die Umgebung scannen um in seiner Tätigkeit nicht mit Gegenständen zu kollidieren.

Da es sich dabei um ein IoT-Gerät handelt, das per Definition mit dem Internet verbunden ist, ergeben sich durch den Einsatz einer Kamera besondere Datenschutz- und Sicherheitsbedenken. Beispielsweise könnte ein gehackter Staubsauger unbeachtet durch anwesende Personen durch die Wohnung fahren und so als unauffälliger Spion für den Angreifer dienen.

Ziel

Im Rahmen des NEidI-Projekts soll in einer Gruppe von 2-4 Personen ein Penetration Test des Roboters durchgeführt werden. Dabei wird die Rolle eines Angreifers eingenommen um mögliche Angriffsvektoren zu identifizieren und zu überprüfen.

Hierbei kommt es vor allem auf ein strukturiertes und umfassendes Vorgehen an. Die einzelnen Angriffsvektoren sollen dabei auch dokumentiert und als Angreifersicht (Risiko, Aufwand) bewertet werden. Stellt sich am Ende heraus, dass keine Angriffsvektoren ausnutzbar sind ist das dennoch ein wertvolles Ergebnis.

Mögliche Arbeitsschritte

1. Hardware explorativ untersuchen
2. Schnittstellen und Protokolle ermitteln
3. Zugangsmöglichkeiten zur Firmware finden
    a) Update-Datei entpacken
    b) Hardwarezugriff
4. Tools zur Unterstützung sichten und bewerten

Kontakt

Johann Bauer und Thomas Mundt (Lehrstuhl IuK):

johann.bauer@uni-rostock.de, thomas.mundt@uni-rostock.de

API-Clients für IoT-Geräte

Zugehöriges Modul

Diese Aufgabe kann im Rahmen des Moduls „**Komplexe Softwaresysteme**“ oder „**Projekt B.Sc. Informatik**“ im Bachelor-Studiengang durchgeführt werden.

Hintergrund

Im Projekt “EMERGE IoT” arbeiten wir gemeinsam mit dem Landeskriminalamt Mecklenburg-Vorpommern an der Verbesserung der Sicherheit von IoT-Systemen. Erfahrungsgemäß zeigt sich oft, dass in der Software solcher Systeme eklatante Sicherheitsmängel bestehen.

Immer mehr Leute lassen sich durch smarte Helfer wie Staubsaugroboter unterstützen. Im Rahmen des Projekts wurde daher ein iRobot Roomba 960 beschafft. Dieser kann mithilfe einer Kamera die Umgebung scannen um in seiner Tätigkeit nicht mit Gegenständen zu kollidieren.

Da es sich dabei um ein IoT-Gerät handelt, das per Definition mit dem Internet verbunden ist, ergeben sich durch den Einsatz einer Kamera besondere Datenschutz- und Sicherheitsbedenken. Beispielsweise könnte der Staubsauger beim Durchfahren der Wohnung persönliche Daten (Einrichtung, anwesende Personen, Größe) für den Hersteller sammeln.

Ziel

Im Rahmen des Projekts/KSWS soll in einer Gruppe von 2-4 Personen ein eigener Client zur Steuerung des Roboters entwickelt werden. Dabei können etwa Open Source Bibliotheken wie „dorita980“ verwendet werden. Der entwickelte Client soll über den Funktionsumfang der Herstellerapp hinaus sicherheits- oder datenschutzrelevante Funktionen bieten.

Vorstellbar wäre etwa eine der folgenden Funktionen:

- Erkennen von Personen im Raum (als Roboter-Alarmanlage)
- Überprüfen der Wohnung auf offene Türen
- Identifizieren von Objekten wie Sofas oder Säcke voller Geld

Mögliche Arbeitsschritte

1. Überblick über API-Funktionalität
2. Basisfunktionen (Geräte-Verbindung, Start/Stop) implementieren
3. Algorithmen zur Objekterkennung auswählen und implementieren

Kontakt

Johann Bauer und Thomas Mundt (Lehrstuhl IuK):

johann.bauer@uni-rostock.de, thomas.mundt@uni-rostock.de