Vorwort

Eine bei Minusgraden gehackte smarte Heizung führte in Finnland zu eingefrorenen Rohrleitungen in einer Wohnanlage mit einigen Hundert Einheiten. US-Behörden riefen Herzschrittmacher zurück, weil Hacker sie angreifen konnten. Zwei Forscher schafften es, einen Jeep Grand Cherokee über das Internet vollständig fernzusteuern, von Aircondition über Fahrtrichtung, Geschwindigkeit und Sitzverstellung bis hin zur Zentralverriegelung.

Längst betrifft IT-Sicherheit nicht mehr nur den klischeehaften Hacker in seinem mit Pizzakartons zugemüllten dunklen Kabuff, sondern jeden von uns. Mit Cyber-Physical-Systemen haben Programmierfehler und Sicherheitslücken Auswirkungen auf das tägliche Leben.

Marcel Mangel und Sebastian Bicchi sind professionelle Penetration Tester, sie demonstrieren regelmäßig Sicherheitslücken. Auf Basis ihres Wissens und ihrer praktischen Erfahrungen ist das folgende Buch entstanden, in dem sie darlegen, wie Angreifer arbeiten – am Beispiel smarter Geräte.

Sie zeigen auf, wie oft simple Fehler zu gefährlichen Angriffen führen und wie die Angriffe funktionieren. Damit bieten sie Sicherheitstestern eine hervorragende Anleitung dazu, wie sie zur Qualitätssicherung vor der Markteinführung ihre Produkte testen sollten.

Gleichzeitig lernen die Entwickler, wie sie die Angriffsflächen in der Zukunft verringern und so die Sicherheit deutlich erhöhen.

Ich bin ein Verfechter von Qualitätssicherung in der Softwareentwicklung. Zur Qualitätssicherung gehört es, sowohl die Fehlermöglichkeiten zu kennen, um sie zu vermeiden, als auch durch gründliches Testen Fehler zu identifizieren. Zu beidem leistet dieses Buch einen wertvollen Beitrag.

Von Praktikern für Praktiker anhand praktischer Beispiele mit qualifiziertem theoretischem Hintergrund – eine lohnende Lektüre, für die ich den beiden Autoren sehr dankbar bin.

Prof. Dr. Tobias Eggendorfer
Lehrstuhl für IT-Sicherheit
Hochschule Ravensburg Weingarten

Einleitung

Die Vernetzung der Welt schreitet immer weiter voran. Das betrifft nicht nur traditionelle IT-Systeme, sondern mehr und mehr alle möglichen »smarten« Geräte. Diese können alle unter dem Stichwort **I**nternet **o**f **T**hings (IoT) subsummiert werden. Für die Hersteller technischer Geräte ist es heutzutage quasi ein Muss, diese in irgendeiner Weise »smart« zu machen. Ein Gerät wird in der Regel dadurch »smart«, dass es mit anderen Geräten oder Systemen vernetzt ist und Informationen austauschen kann.

Dieser Informationsaustausch geschieht dabei in aller Regel über standardisierte Protokolle und Infrastrukturen wie z. B. das Internet. Für potenzielle Angreifer eröffnet diese Vernetzung eine ganze Reihe neuer Angriffsmöglichkeiten. Anstatt besonders gehärtete klassische IT-Systeme anzugreifen, ist es für Hacker deutlich interessanter geworden, ihren Fokus auf IoT-Geräte zu verlegen. Darunter finden sich eine Menge Geräte, die praktisch überhaupt nicht abgesichert sind. Da kann es, wie das Mirai-Botnetz[1] eindrucksvoll unter Beweis gestellt hat, schon ausreichen, die Geräte einfach mit Standardpasswörtern zu übernehmen und für weitere Angriffe zu missbrauchen. Es wurden insgesamt 64 verschiedene Standardpasswörter getestet, um Zugriff auf die entsprechenden Geräte zu erlangen. Eine genauere Analyse des Sourcecodes sei dem Leser an Herz gelegt.

Die Situation verschärft sich jedoch dramatisch, wenn es sich bei den angegriffenen Geräten nicht mehr um Router oder Kameras handelt, sondern um Geräte aus der Medizintechnik. Auch in dieser Branche werden die Geräte immer »smarter« und bieten damit immer größere Angriffsflächen. Viele Hersteller sind sich aktuell gar nicht richtig im Klaren über die Gefahren, die von der zunehmenden Vernetzung ausgehen. Nicht nur die Medizintechnik ist ein Beispiel für die wachsende Verzahnung von Security und Safety. Weitere Bereiche, für die das gilt, sind die sogenannten »kritischen Infrastrukturen«. Darunter fallen z. B. Energieversorger, der öffentliche Personenverkehr oder auch Krankenhäuser. Werden solche Systeme kompromittiert, kann das fatale Folgen haben. Ein sehr bekanntes Beispiel ist der Stromausfall in Brasilien. Nachdem Angreifer Industrial-Control-Systeme unter ihre Kontrolle gebracht hatten, kam es zu flächendeckenden Stromausfällen, von denen Millionen Menschen in Brasilien über mehrere Stunden betroffen waren.[2]

1 https://github.com/jgamblin/Mirai-Source-Code
2 https://www.wired.com/2009/11/brazil/

Auch hier waren nicht abgesicherte Systeme, die über das Internet erreichbar waren Ausgangspunkt des Angriffs.

Die Hersteller werden jedoch immer mehr zur Verantwortung gezogen. Während man das Thema Cyber Security vor einigen Jahren noch sehr stiefmütterlich behandeln konnte, wird es in den kommenden Jahren mehr und mehr an Wichtigkeit gewinnen. Zum Teil wird dies auch schon durch die Einhaltung von Compliance-Richtlinien wie der Datenschutzgrundverordnung erzwungen.

Ziel des Buchs

Als wir anfingen, uns mit dem Thema Penetration Testing für Internet-of-Things-Geräte zu beschäftigen, gestaltete es sich als überaus schwierig, Bücher zu diesem Thema zu finden. Insbesondere auf dem deutschsprachigen Markt war zu diesem Zeitpunkt kein geeignetes Buch verfügbar. Auch im englischsprachigen Raum gab es zwar schon einige Bücher, doch diese wurden alle nicht dem gerecht, wonach wir suchten. Im Internet auf diversen Blogs fanden wir einige sehr interessante und hilfreiche Informationen, jedoch keine, die das Thema umfassend abdeckten. Mit diesem Buch versuchen wir, genau diese Lücke zu schließen. Das Buch soll zum einen eine umfassende Informationsquelle zum Thema sein und zum anderen als eine Art Referenzwerk zum praktischen Testen von Geräten dienen.

Die OWASP IoT Top 10 stellen ein erwähnenswertes Projekt dar, in dem man sich ebenfalls mit der Sicherheit von IoT-Geräten beschäftigt. OWASP steht für **O**pen **W**eb **A**pplication **S**ecurity **P**roject, und es handelt sich dabei um eine Non-Profit-Organisation, die insbesondere durch die »OWASP Top 10«, eine Liste mit den am häufigsten vorkommenden Schwachstellen in Webanwendungen, bekannt geworden ist. Neben dieser Liste für Webanwendungen gibt es die »OWASP Mobile Top 10« sowie seit 2014 auch die »OWASP IoT Top 10«, in der die zehn am häufigsten vorkommenden Schwachstellen für IoT-Geräte aufgelistet sind. Nach der letztmaligen Aktualisierung im Jahr 2018 sind dies:

1. Schwache, erratbare oder hartcodierte Passwörter
2. Unsichere Netzwerkdienste
3. Unsichere Schnittstellen innerhalb des IoT-Ökosystems
4. Unsichere Update-Mechanismen
5. Verwendung unsicherer oder veralteter Komponenten
6. Nicht ausreichender Schutz von Benutzerdaten
7. Unsichere Transfers und unsichere Speicherung von Daten
8. Unzureichendes Management der Geräte
9. Unsichere Standardeinstellungen
10. Unzureichender Schutz gegen physische Angriffe

Aufbau des Buchs

Das Buch behandelt in acht Kapiteln die einzelnen Aspekte, die beim Testen eines IoT-Geräts vonnöten sind.

Kapitel 1 – Vorbereitung

In diesem Kapitel werden organisatorische sowie technische Projektvorbereitungen dargestellt, die für ein erfolgreiches Security-Testing-Projekt unabdingbar sind. Neben dem Thema Scoping wird auch intensiv auf den Aufbau eines entsprechenden Testing-Labors eingegangen. Abschnitt 1.3 »Das Labor« zeigt den praktischen Aufbau eines Elektroniklabors, welche Geräte benötigt werden und wofür. Die Grundbegriffe der Elektronik werden erläutert sowie Arbeitsweisen im elektronischen Labor.

Kapitel 2 – OSINT

Zu Beginn dieses Kapitels wird der Begriff *OSINT* (**O**pen **S**ource **Int**elligence) im Kontext der Sicherheit vernetzter Geräte erklärt. Weiterhin wird beschrieben, wie die systematische Sammlung und Analyse offen zugänglicher Informationen durchzuführen ist und wie diese zur Sicherheitsanalyse verwendet werden können.

Kapitel 3 – Hardware

Das Kapitel »Hardware« erklärt zunächst die notwendigen Elektronikgrundlagen und die verschiedenen Bauelemente in einer kleinen Baustein-Lehre. Zusätzlich werden Bussysteme und Schnittstellen theoretisch beleuchtet und integrierte Bausteine sowie verschiedene Aspekte der Herstellung, wie Layout und Schemata einer Platine, beschrieben.

Kapitel 4 – Physische Sicherheit

Das Kapitel »Physische Sicherheit« beschäftigt sich mit der Sicherheit des Gehäuses und Tamper-Protection-Maßnahmen. Außerdem werden Hardwaredesign-Grundlagen erklärt (8-/32-Bit-Controller) und verschiedene Angriffspunkte erläutert. Zu guter Letzt wird gezeigt, wie bei einem physischen Zugriff auf das Gerät die Firmware extrahiert werden oder ein Zugriff auf andere Daten in Bausteinen erfolgen kann (JTAG/SWD/UART/SPI).

Kapitel 5 – Firmware

Die Firmware ist quasi das Herzstück eines jedes IoT-Geräts und besitzt damit einen besonderen Stellenwert bei der Sicherheitsanalyse eines solchen. In diesem Kapitel werden zunächst unterschiedliche Möglichkeiten dargestellt, an die Firmware eines Geräts zu gelangen. Im Anschluss beschreibt das Kapitel ausführlich das Entpacken, die Analyse und die Emulation von Firmware-Images.

Kapitel 6 – IoT-Referenzarchitekturen und Netzwerkprotokolle

Das Kapitel beginnt mit einer Einführung in das Thema Protokolle und stellt zwei verschiedene in der Praxis relevante IoT-Referenzarchitekturen vor, bevor auf zwei konkrete Netzwerkprotokolle (Bluetooth Low Energy und Zigbee) im Detail eingegangen wird. Diese beiden Protokolle werden von zahlreichen IoT-Geräten verwendet und stellen damit ein oftmals zentrales Thema bei vielen Security Assessments dar. Neben den Grundlagen der beiden Protokolle werden praktische Angriffe und Tools vorgestellt.

Kapitel 7 – MQTT

Das achte Kapitel widmet sich dem wohl wichtigsten Protokoll auf Anwendungsebene im IoT-Umfeld: MQTT. Hier steht insbesondere eine ausführliche Darstellung der Funktionsweise sowie der wesentlichen Pakettypen im Vordergrund.

Kapitel 8 – Apps

Das App-Kapitel umfasst einen kurzen Einstieg in die OWASP-App *Security* und erklärt, welche Sicherheitsanforderungen an Apps allgemein gestellt werden.

Vertiefend wird auf die Spezifika vernetzter Geräte und Apps eingegangen, insbesondere auf sämtliche Verbindungen (direkt und indirekt) zum vernetzten Gerät.

Kapitel 9 – Backend, Web und Cloud

In diesem Kapitel werden zum einen die Rahmenbedingungen erläutert, die beim Testen von Backend-Systemen zu beachten sind, und zum anderen wird die am weitesten verbreitete Methodik zum Testen von Applikationen nach OWASP erläutert.

Zielgruppe

Das Buch richtet sich in erster Linie an Personen, die Penetration Tests von Internet-of-Things-Geräten durchführen möchten.

Neben den eigentlichen Testern kann das Buch durchaus auch für Projektmanager oder Security-Verantwortliche aufseiten der Hersteller interessant sein.

Was Sie benötigen

Als Leser dieses Buchs sollten Sie bereits über grundlegende Kenntnisse in IT-Sicherheit, insbesondere in den Bereichen Netzwerk- und Applikationssicherheit, verfügen. Zudem wird ein routinierter Umgang mit Linux vorausgesetzt.

Trotzdem legen wir Wert darauf, dass auch interessierte Einsteiger den Inhalten des Buchs gut folgen können.