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.

Über die Autoren

Marcel Mangel verfügt über mehr als eine Dekade praktischer Erfahrung in IT-Sicherheit. Sowohl im defensiven als auch im offensiven Bereich war er mehrere Jahre für renommierte Unternehmen tätig und hat neben einem Master in Informatik noch über eine ganze Reihe von anerkannten Zertifikaten. Nebenbei arbeitet Marcel Mangel bereits seit mehreren Jahren im Rahmen von Lehraufträgen und Gastvorlesungen an diversen Universitäten und Fachhochschulen als Dozent. Zurzeit hält er die Master-Vorlesung »Vertiefung der IT-Sicherheit« an der Fachhochschule Rosenheim.

Sebastian Bicchi begann bereits in seiner Jugend mit dem Aufspüren von Sicherheitslücken in Webseiten und Anwendungen. Nach seinem IT-Security-Studium gründete er in Wien gemeinsam mit Studienkollegen das Unternehmen »Security Research« (sec-research.com) und beschäftigte sich insbesondere mit den technischen Aspekten der IT-Security. Die Synergien seiner Ausbildungen in verschiedenen Bereichen (Elektrotechnik/industrielle Informationstechnik, Informationstechnologien und Telekommunikation, IT-Security) schufen die Basis für sein fundiertes Wissen über IoT- und Hardware-Hacking. Sebastian Bicchi betätigt sich darüber hinaus freiwillig in nicht kommerziellen Organisationen für Informationssicherheit, zum Beispiel als Co-Chapter-Lead bei OWASP für das Chapter Vienna.

Danksagungen

Marcel Mangel

Mein besonderer Dank gilt meiner Lebensgefährtin Sarah sowie meiner gesamten Familie, die mich bei der Erstellung des Buchs außerordentlich unterstützt haben.

Daneben möchte ich mich ganz herzlich bei meinem Koautor und Freund Sebastian Bicchi bedanken, ohne den dieses Buch nicht entstanden wäre.

Außerdem bedanke ich mich sehr herzlich beim mitp-Verlag für die Möglichkeit der Veröffentlichung sowie insbesondere bei unserer Lektorin Frau Janina Bahlmann für die tolle Unterstützung und Zusammenarbeit.

Und zu guter Letzt bedanke ich mich ebenfalls sehr herzlich bei Christian Salzmann, der die Abschnitte über Bluetooth und Zigbee beigesteuert hat, und bei Tobias Eggendorfer für den stetigen Austausch und das Vorwort.

Sebastian Bicchi

Mein besonderer Dank gilt meiner Freundin Sandra, die mich in allem, was ich mache, unterstützt und mir, während ich dieses Buch geschrieben habe, alle nur erdenklichen Lasten abgenommen hat.

Weiterhin möchte ich mich bei Marcel Mangel bedanken – für die Möglichkeit, dieses Buch zu schreiben, und für die Zusammenarbeit bei der Erstellung des Buchs und allen weiteren spannenden Projekten, die wir zusammen bearbeitet haben.

Ein großes Dankeschön möchte ich an dieser Stelle auch dem Verlag und Frau Bahlmann für ihre Unterstützung während des gesamten Erstellungsprozesses des Buchs und für das außerordentlich gute Feedback ausrichten.

Mein weiterer Dank gilt den Personen, die meine Ausbildung zu einem besonderen Weg gemacht und mir letztendlich ermöglicht haben, dieses Buch zu schreiben: Manuel Koschuch (FH Campus Wien) und Bernd Stanzl (HTL Mödling). Beide haben mich über alle Maßen unterstützt, sämtliche Fragen, auch über den Lehrplan hinaus, immer mit genügend Zeit und Geduld beantwortet und mich inspiriert, Wissen weiterzugeben.

Ich möchte mich ebenfalls bei Zlatko Sehanovic und Herbert Dowalil für das Vorab-Review und das inhaltliche Feedback bedanken.