SEC556: **IoT Penetration Testing**

3 Day Course	18 CPEs	Laptop Required

You Will Be Able To

- Assess IoT network-facing controls, web applications, and API endpoints with an IoT focus
- Examine hardware to discover functionality and find interaction points and use them to obtain data from the hardware
- Uncover firmware from hardware and other means, and explore it for secrets and implementation failures
- Sniff, interact with, and manipulate WiFi, LoRA, and Zigbee wireless technologies and understand security failures in implementation
- Interact with Bluetooth Low Energy (BLE) for device manipulation
- Automate recovery of unknown radio protocols to perform replay attacks and additional analysis

You Will Receive With This Course

- BusPirate 3.6a and cable
- SPI Flash integrated circuit
- Solderless breadboard
- HackRF One with antenna
- HackRF ANT500 antenna
- USB Logic analyzer
- Dupont wires
- RaspberryPi 4 8G Vilros Kit (32 Gig SD card) (Note: this comes with a U.S. plug, so international students will need to bring an adapter)
- USB wireless adapter
- TP-Link Bluetooth Low Energy USB adapter
- 433Mhz IoT remote-controlled outlet (110/120V only, EU and APAC students will need to bring a voltage converter)
- A pair of CC2531 custom-flashed USB Zigbee adapters
- USB 3.0 4-port hub
- Ethernet cable
- Custom Slingshot Linux Virtual Machine
- Custom Raspberry Pi image (PIoT.01)

A growing trend in recent years has seen small-form factor computing devices increasingly accessing networks to provide connectivity to what typically used to be disconnected devices. While we can debate if your home appliances truly need Internet access, there is no debate that the Internet of Things (IoT) is here to stay. It allows for deeper connectivity of many devices that are indeed useful, with great benefits to homes and enterprises alike.

Unfortunately, with this proliferation of connected technology, many of these devices do not consider or only minimally consider security in the design process. While we have seen this behavior in other types of testing as well, IoT is different because it utilizes and mixes together many different technology stacks such as custom Operating System builds, web and API interfaces, various networking protocols (e.g., Zigbee, LoRA, Bluetooth/BLE, WiFi), and proprietary wireless. This wide range of diverse, poorly secured technology makes for a desirable pivot point into networks, opportunities for modification of user data, network traffic manipulation, and more.

SEC556 will familiarize you with common interfaces in IoT devices and recommend a process along with the Internet of Things Attack (IoTA) testing framework to evaluate these devices within many layers of the Open Systems Interconnection (OSI) model. From firmware and network protocol analysis to hardware implementation issues and all the way to application flaws, we will give you the tools and hands-on techniques to evaluate the ever-expanding range of IoT devices. The course approach facilitates examining the IoT ecosystem across many different verticals, from automotive technology to healthcare, manufacturing, and industrial control systems. In all cases, the methodology is the same but the risk model is different.

Once we ve been empowered to understand each individual challenge, we can understand the need for more secure development and implementation practices with IoT devices.

Authors Statement

"It has been amazing to watch the progression and widespread adoption of what we now know as the Internet of Things in both our homes and enterprises whether you realize it or not! However, while IoT-enabled technologies have arguably made our lives better by improving conveniences and our ability to obtain more accurate data about our environment, we unknowingly increase our attack surface through their use."

"In other words, the benefits often come at a cost, in many cases because of lackluster development practices by many IoT manufacturers that fail to consider the entirety of the attack surface of their device ecosystem. This failure is largely seen as financial; baking security in from the start is an expense that reduces the already low profit margins on IoT devices. Delays from adopting enhanced security measures can prevent a timely push to market, further compounding profit-per-device issues.

"With the increased adoption of IoT, attackers have also focused their efforts on IoT platforms. Techniques and tool capabilities have become exponentially more sophisticated, and they are often used for 1good to unlock additional features and capabilities. However, less-ethical attackers have gained the same sophistication with their toolsets, giving them the upper hand in exploiting the technology we rely on for critical tasks. The IoT adoption rate, in combination with the sophistication of attackers, paints a grave picture for the future of IoT and the networks IoT devices are connected to unless we begin now to improve the security of all facets of the IoT ecosystem.

"We are very excited to deliver interactive, hands-on labs and a suite of hardware and software tools to equip IoT analysts and developers with practical skills, methodologies, and thought processes that they can bring back to their organizations and apply on day one. The skills you will build in this class will be valuable for today's IoT technology and serve as a foundation for tomorrow's advancements, regardless of your vertical, application, or data."

–Larry Pesce, James Leyte-Vidal, and Steven Walbroehl

Section Descriptions

SECTION 1: Introduction to IoT Network Traffic and Web Services

This course section introduces the overall problem with IoT security and examines how testing can address the problem in largely generic terms, given the multitude of IoT implementations. The first technical concepts include network recon and attacks as well as key web application issues often found with IoT devices, such as authentication bypass, RFI, and command injection. Additionally, we will examine API requests from mobile apps to back-end services and the devices themselves, then use the tools testers need to inspect and exploit network and web-based IoT.

TOPICS: Course Introduction; Course Methodology for Testing IoT: Modified IoTA; Tooling for IoTA: Introducing Hardware Tools; Network Discovery and Recon; Active Network Discovery; Network Exploitation for IoT; Web Services in IoT; Web and API Recon and Discovery; Tools for Web Services; Web Service Attack Types and Exploitation

SECTION 3: Exploiting Wireless IoT: WiFi, BLE, Zigbee, LoRA, and SDR

This course section focuses on the more popular and developing, documented, and standardized wireless technologies often found in IoT technology. The concepts introduced include capturing traffic, gaining access to networks and encrypted data, and interacting with and compromising IoT devices and their functions. The section will introduce the concepts to analyze and exploit non-standard and proprietary RF communications often found in IoT devices.

TOPICS: Wi-Fi; Bluetooth Low Energy; Zigbee; LoRA; SDR

SECTION 2: Exploiting IoT Hardware Interfaces and Analyzing Firmware

This section will introduce key concepts to perform recon against various hardware devices for destructive and semi-destructive testing for hardware, as well as hardware identification, communication, and exploitation using various hardware tools. We will also examine ways to recover device operating systems (firmware) and analyze them to recover stored secrets and various implementation flaws.

TOPICS: Background and Importance of IoT Hardware; Opening the Device; Examining and Identifying Components; Discovering and Identifying Ports; A Soldering Primer; Sniffing, Interaction, and Exploitation of Hardware Ports: Serial, SPI, JTAG; Recovering Firmware; Firmware Analysis; Pillaging the Firmware

Who Should Attend

This course is designed for professionals seeking the comprehensive technical skills needed to understand, analyze, attack, and defend the entire spectrum of the IoT ecosystem. The course will enable attack-focused and defense-focused security practitioners, as well as those designing and implementing embedded, IoT, and IIoT solutions across many verticals (automotive, healthcare, consumer electronics, industrial instrumentation, smart home, etc.), to gain a deep understanding of the attack surfaces of IoT devices and appropriate defenses. The course is suited for:

- Penetration testers
- Embedded system developers
- Security analysts
- Security architects
- Product security engineers
- IoT product developers
- Anyone releasing an IoT device to market