IoT Fundamentals: IoT Security 1.1
Scope and Sequence

Last updated October 21, 2019

Introduction

The advent of the Internet of Things (IoT) has created many new opportunities for connecting people, places, and things. It has also brought with it an ever-expanding attack surface for threat actors to exploit. Today's organizations are challenged with securely implementing many new devices into the existing information technology (IT) infrastructure. The *IoT Security 1.1* course arms students with crucial knowledge they need to intelligently discuss and evaluate, at a basic level, the IoT security environment for a given business context.

Target Audience

IoT Security 1.1 is designed for Cisco Networking Academy® students seeking foundational knowledge in security analysis; specifically, vulnerability and risk assessment of IoT systems. Target students include individuals enrolled in high school technology programs, technology degree programs at institutions of higher education, and IT professionals who want to learn more about IoT security.

Prerequisites

An *IoT Security 1.1* student should have completed the following courses or their equivalents:

- Cybersecurity Essentials
- Networking Essentials
- Connecting Things

In addition to the prerequisite courses, *IoT Security 1.1* students should have the following skills and knowledge:

- PC and Internet navigation skills
- Basic Windows and Linux system concepts (e.g. Cisco Networking Academy's Linux Unhatched course)
- Basic Networking concepts
- Binary and Hexadecimal understanding
- Awareness of basic programming concepts

Curriculum Description

The course has many features to help students understand these concepts:

- Rich multimedia content, including interactive activities, videos, games, and quizzes, addresses a variety of learning styles and help stimulate learning and increase knowledge retention
- Virtual environments simulate real-world cybersecurity threat scenarios and create opportunities for ethical hacking, vulnerability assessment, risk assessment, and mitigation techniques.
- Hands-on labs help students develop critical thinking and complex problem-solving skills.
- Innovative assessments provide immediate feedback to support the evaluation of knowledge and acquired skills.

- Technical concepts are explained using language that works well for learners at all levels and embedded interactive activities break up reading of the content and help reinforce understanding.
- The curriculum encourages students to consider additional IT education, but also emphasizes applied skills and hands-on experience.
- Cisco Packet Tracer activities are designed for use with Packet Tracer 7.1.1 or later.

Curriculum Objectives

Upon completion of the *IoT Security 1.1* course, students will be able to complete the following tasks:

- Evaluate IoT security risks in an industry sector.
- Use industry-standard models to explain security requirements in IoT systems.
- Perform threat modeling activities to evaluate physical device security vulnerabilities in IoT systems.
- Perform threat modeling activities to evaluate communication security vulnerabilities in IoT systems.
- Perform threat modeling activities to evaluate application security vulnerabilities in IoT systems.
- Use threat modeling and risk management frameworks to recommend threat mitigation measures.
- Explain the impact of emerging technologies on IoT Security.

Equipment, Software, and Virtual Machine Requirements

The *IoT Security 1.1* course has the following equipment, software, and virtual machine requirements

Hardware Equipment Requirements

The Cisco Prototyping Lab consists of the Prototyping Lab Application (PL-App) software that is provided for free to the Academy students and the Prototyping Lab Kit that Academies will need to purchase. Instructors may substitute the recommended list of sensors and controllers with other similar devices based on the price and availability in their region, and would then need to customize the lab and activities accordingly.

The Prototyping Lab Application runs on Microsoft Windows and Mac OS and supports labs on the Raspberry Pi 3 in the Prototyping Lab Kit. Cisco Packet Tracer activities are designed for use with Packet Tracer 7.1 or later. Each team of 2-4 students needs one Prototyping Lab Kit as follows:

- Raspberry Pi 3 device, Model B or B+, with PL-App
- MicroSD card, 8GB minimum
- Breadboard
- Two 330K Ohm resistors
- Two LEDs, one red and one green
- Jumper wires
- Smartphone with recent operating system (Requires iOS 9.0 or higher, or Android devices running 4.1 or higher.)
- Bluetooth devices (e.g., PC, Smartphone, Smartband, Bluetooth LED Control, etc.)
- adafruit - USB to TTL serial cable - debug/console cable for Raspberry Pi or compatible cable
- Network switch
- Ethernet cable

Software Requirements

The following software is required to complete the labs in the course:

- Oracle VirtualBox
- Kali Linux virtual machine (VM) customized for the course (see Table 1)
- Metasploitable VM customized for the course (see Table 1)
- PL-App image
- PL-App launcher

- IFTTT app for Android or iOS
- Packet Tracer version 7.1 or later

Virtual Machine Requirements

This course uses two VMs. The lab or student PC should meet the following requirements:

- Host computer with at least 4GB of RAM and 15GB of free disk space
- Internet connection
- Two virtual machines listed in the table below:

Table 1. Virtual Machine Requirements

Virtual Machine	RAM	Disk Space	Username	Password
Kali	1 GB	10 GB	root	toor
Metasploitable	512 KB	8 GB	msfadmin	msfadmin

For the best learning experience, we recommend a typical class size of 12 to 15 students and a ratio of one Lab PC per student. At most, two students can share one Lab PC for the hands-on labs. Some lab activities require the student Lab PCs to be connected to a local network.

Course Outline

Table 2. IoT Security 1.1 Course Outline

Chapter/Section	Goals/Objectives
Chapter 1. The IoT Under Attack	**Evaluate IoT security risks in an industry sector.**
1.1 IoT Security Challenges	Explain the need for IoT security in several IoT environments.
1.2 IoT Security Use Cases	Evaluate potential risks in various IoT use cases.
Chapter 2. IoT Systems and Architectures	**Use industry-standard models to explain security requirements in IoT systems.**
2.1 Models of IoT Systems	Use industry standard models to explain IoT systems.
2.2 A Model for IoT Security	Evaluate IoT security using a simple model.
2.3 IoT Threat Modeling	Create an IoT threat model.
Chapter 3. IoT Device Layer Attack Surface	**Perform threat modeling activities to evaluate physical device security vulnerabilities in IoT systems.**
3.1 Overview of IoT Devices	Explain the operation of IoT device hardware and firmware.
3.2 Vulnerabilities and Attacks at the Hardware Layer	Perform threat modeling activities to evaluate IoT device hardware and firmware.
3.3 Threat Mitigation of the Physical Device	Recommend measures to mitigate threats to IoT devices.
Chapter 4. IoT Communication Layer Attack Surface	**Perform threat modeling activities to evaluate communication security vulnerabilities in IoT systems.**
4.1 The IoT Communication Layer	Determine vulnerabilities of the IoT communication layer.
4.2 TCP/IP Vulnerabilities in IoT Networks	Determine vulnerabilities in TCP/IP that impact IoT systems.

4.3 Mitigating IoT Communication Threats	Explain measures to mitigate threats at the IoT network layer.
Chapter 5. IoT Application Layer Attack Surface	**Perform threat modeling activities to evaluate application security vulnerabilities in IoT systems.**
5.1 IoT Applications	Perform vulnerability assessment activities with IoT applications and protocols.
5.2 Mitigation	Recommend measures to mitigate threats to IoT applications.
Chapter 6. Vulnerability and Risk Assessment in an IoT System	**Use threat modeling and risk management frameworks to recommend threat mitigation measures.**
6.1 Vulnerability Assessment and Penetration Testing of IoT Systems	Explain how vulnerabilities are assessed in IoT Systems.
6.2 Risk Assessment	Evaluate security in an IoT system risk using assessment.
6.3 Innovations in IoT Security	Explain innovations in IoT Security
Capstone Activity	**Apply skills learned in the previous chapters in a challenging hands-on capstone activity.**
IoT Security Game	**In teams play a fun and engaging CTF game, that mimics a real world-like scenario of an end to end IoT system. Apply White Hat Hacker skills to conduct a vulnerability assessment and provide mitigation recommendations, collect points and win.**