Team IoTSec
Sprint 1

By Sara Fagin,
Nuwapa Promchotichai (Prim)
https://github.com/sfagin89/EC601-TeamIoTSec

Product Mission

To improve IoT Security by investigating current vulnerabilities through the development of Security testing tools targeting IoT Security.

MVP

Design an affordable hardware/software package, accessible via Mobile Application, that helps with IoT network security testing in one of the following ways:

- Packet Sniffing
- Port Scanning
- Vulnerability Scanning
- Password Cracking

MVP User Stories

As a professional Security Tester, I want an affordable security tool

As a professional Security Tester, I want a tool that can be easily accessed from a mobile device

As a professional Security Tester, I want a UI that shows useful information on network security

As a professional Security Tester, I want a tool that is unobtrusive.

Why IoT Security Matters

- There is an increasing dependence on IoT devices in various industries, automotive and healthcare in particular[2][3]
- IoT devices are particularly vulnerable to remote hacking attacks due to their internet-supported connectivity
- Common targets to recruit for cryptocurrency mining, DDOS attacks or stealing data from other devices on that network.
- Kaspersky reported around 1.51 billion breaches of IoT devices from January to June of 2021, more than doubling that same period in 2020 (639 million)[1]

Current Challenges with IoT Security

- Insecure Interfaces
- Lack of regular patches and/or weak update mechanisms
- Weak password protection
- Unencrypted data
- Insufficient logging mechanisms

Technologies to evaluate

Hardware Pen Testing Tools

WiFi Pineapple

Can be utilized in wireless man-in-the-middle attacks by creating rogue Access Points

Rubber Ducky

Payload Injector that replicates an HID device to bypass Firewall and Antivirus Software

Bash Bunny

Quicker to create payloads due to its simple scripting language

Technologies to evaluate

Hardware Pen Testing Tools

Ubertooth One

Open-source 2.4GHz wireless application framework that can be used to work with Bluetooth

Proxmark3 Kit

The preferred tool for reading and copying RF Tags

HackRF

Allows you to build your own wireless protocol and test it against a target device

Killerbee

Let you write your own exploit using SCAPY

User-friendly toolset written around Python

Thank you!

Q & A

Sources

[1] https://www.iotworldtoday.com/2021/09/17/iot-cyberattacks-escalate-in-2021-according-to-kaspersky/

[2] https://www.wipro.com/business-process/what-can-iot-do-for-healthcare-/

[3] https://ordr.net/article/iot-healthcare-examples/

[4] https://internetofthingsagenda.techtarget.com/definition/IoT-security-Internet-of-Things-security

[5] https://www.thesecmaster.com/top-15-powerful-hardware-pen-testing-tools-for-successful-pen-testing/