Reverse Engineering Network APIs
Speaker: Dan Nagle

Demonstration Details

For: IEEE SoutheastCon 2022 in Mobile, NC

Time: 2 hours

Other Info: I will need a decent sized table and power source for all my gear. Ideally, I would like access to it about 15 min before I start because this is a complicated set up.

Abstract

A foundational component of communication between devices is the TCP/IP network stack. Web browsing, streaming video, secure control, and innumerable other applications are built upon this technology. This 3-part demonstration will use open source tools to focus on the data transfer components UDP and TCP while targeting an IoT device. Part 1 is reverse-engineering the network commands to better understand them and then mimic it (a common attack strategy). Network protocols will be discussed during this process. Armed with our new knowledge and skills, part 2 will take them a step further to discover and analyze malware present on the IoT device. Part 3 will cover fundamentals of network latency vs network throughput by forced network degradation. This presentation is light on slides and heavy on demos.

Outline

The presentation is divided in to 3 parts. The first part demonstrates reverse-engineering of an IoT device's communication protocols. The second part demonstrates a practical technique of security research. Packet Sender and Wireshark (2 popular free open source network tools) will be used heavily. The third part is covers some basic network tests.

Part 1: Reverse-Engineering an IoT device

A Raspberry Pi in a closed network will be running custom TCP and UDP services (for our example, a music player) with a black box client app used for control. The app provides discoverability (via UDP) and command and control (via TCP). There will be a discussion of why these protocols were chosen.

The device's commands will be captured and then replayed to verify the tool was successfully reverse-engineered. Once this is accomplished, the demo will lead to part 2.

Part 2: Discovering Malware on an IoT device

Inviting an IoT device to your home network is a risk. How risky? Fortunately, this demo is on a closed network. The techniques learned in Part 1 will be augmented by capturing and analyzing the malware communication happening with our IoT music player.

Part 3: Latency VS Throughput

Time permitting or post wrap-up for the extra curious, there will be demonstrations regarding latency and throughput by forced degradation of the network. Latency and throughput are the 2 most important metrics for network performance, and they are often confused. Hopefully, there will be no more confusion after these demos.

Wrap up: Q&A and Code Links

All original software demonstrated will be open source and available on the author's GitHub account. This includes the embedded IoT server apps.

About the Presenter

Dan Nagle has over 15 years of software development experience. He has written and published apps for desktop, mobile, servers, and embedded. He is the author and inventor of Packet Sender, an app used daily by security researchers, featured in manuals from major tech companies, and is taught in universities around the world. He is also the author of 2 network-related patents and a book published by CRC Press. His open source contributions have received international awards, and he has presented at many developer conferences about them.