Network analysis for the Internet of things

Michael Amabile
Mentored by Mike Bowen

Introduction

In the tempest of emerging computer technologies that has been raging in the past decades, one aspect of this field that has been lacking is the monitoring of home networks for potential threats (Cisco, 2015). This project's purpose was to address this gap in data security by developing a device that can read and analyze communications between devices and identify potential threats within the Internet of Things (IoT) for home networks. The device, termed *NetID*, was wired via Ethernet directly to a router, which allowed it to monitor all communications between systems on the network. NetID is a program made up of Linux shell scripts, powered by the Ubuntu 16.04 operating system, and running on a lightweight computer system, the ODROID-XU4™. NetID's capabilities augment what is typically provided by home routers, and would increase home security in the digital world by informing users of otherwise hidden network activity.

Materials and Methods

A lightweight but capable computer system, the ODROID-XU4™, was used as the host machine for NetID. A second network interface was added via a USB-to-Ethernet dongle, the Linksys™ USB3GIG v1, enabling the device to serve as an inline network data collector. Using a combination of standard UNIX tools and available software components, an application was created to collect network traffic, import it into a database, and present collected information, which is illustrated in Figure 1.

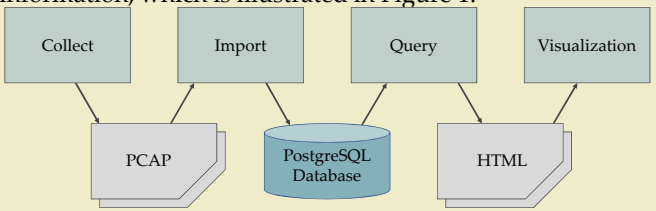

Figure 1: An illustration of NetID's software architecture. The top row features the functions the device performs, with the bottom row featuring the intermediate storage methods, including the Packet Capture (PCAP) and Hypertext Markup Language (HTML) file formats and a PostgreSQL database.

Materials and Methods (cont.)

NetID was integrated into a test network with a controlled number of other representative systems, including laptops, mobile devices and IoT components (Fig. 2). A series of tests were executed to determine the NetID's ability to detect new data flows, the reporting delay for detection of data flows, as well as the characterization of the data flows observed from several common IoT components.

Figure 2: NetID and some supporting hardware. From left to right: ❶ an Apple iPhone 6™, ❷ a Honeywell RedLink™ Internet gateway, ❸ an ODROID-XU4™ platform (hosting the NetID software), and ❹ a Linksys™ WAP610N 802.11n Access Point. The ODROID™ has two gigabit Ethernet connections, one onboard and the other via a ❺ Linksys™ USB3gIg USB-to-Ethernet dongle, enabling it to be in-line with the network's Internet connection, similar to a user's home router.

Results

A defined set of tests were executed where a total of 7 devices were configured to join the test network under controlled conditions. During each of the tests, the NetID system was able to detect all of the devices as they began communicating with external systems. For testing, device-on times varied from a minimum of 90 seconds to just over 3 minutes. The minimum delay is a function of the internal timers employed within NetID's software.

Figure 3 illustrates the NetID user interface after one of the test runs. A summary of the total traffic statistics and detected devices are shown to the left. The right-hand pane illustrates a breakdown of traffic from one of the devices.

Results (cont.)

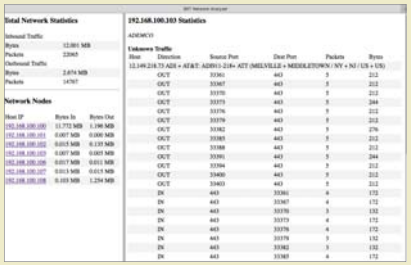

Figure 3: The NetID web-based display, including statistics for all flows in and out of the network (upper left), detail for each locally-detected devices (lower left), as well as individual data flow statistics for one of the selected devices (right-hand side). Each element includes total packets and total bytes.

Each of the devices detected had a different "signature" data flow. The Honeywell device shown in Figure 3 exhibited a periodic status update to three external servers, while a Samsung SmartThings™ hub maintained longer-running connections. As each device was operated, a number of new flows were identified by the NetID system.

Conclusion

The goal of this project was to develop a device that tracks communications between internet connected devices on a home network and alerts users to anomalous data flows. The project successfully demonstrated employment of the NetID system on a test network, as well as the measurement of several fundamental metrics related to the system's operation and IoT device behavior observed by the system.

Given the complexity of the problem space, a number of enhancements to the NetID system are possible. The current system supports the ability to "learn" data flows deemed acceptable via manual execution of a script; this could be automated and tuned to detect common device signatures. Additionally, the reporting capability could be enhanced by sending alerts via text or e-mail, and portraying devices in a more human-readable format.

References

Cisco Corporation. (2015). *IoT Threat Environment*. Retrieved from http://theinternetofthings.report/Resources/Whitepapers/4c7c4eca-6167-45c3-aac8-bff6031cadc9_IoT%20Threat%20Environment.pdf