International Journal of Advance Research in Science and Engineering
Vol. No.6, Special Issue (01), September 2017, BVCNSCS 2017
www.ijarse.com
IJARSE
ISSN 2319 - 8354

Security testing for IoT devices

Srinivasarao
Independent Security Researcher
Singapore

*Abstract***:** Internet of Things (IoT) is a new buzzword in the world of Internet. "The Internet of Things (IoT) is the network of physical objects or "things" embedded with electronics, software, sensors and connectivity to enable it to achieve greater value and service by exchanging data with the manufacturer, operator and/or other connected devices" is the definition of IoT as per Wikipedia. As the definition says these objects are interconnected and multiple communication technologies will be involved while building an IoT device. Enough attention was not paid to the security aspects of these devices. It is important to ensure that the IoT devices being built are safe enough to be used by a common man. This paper discusses common techniques to perform security testing of IoT devices to ensure that these devices are safe when connected to the Internet. Testing for security issues in the embedded device (Hardware), testing for security issues in the software used by the IoT device and testing for security issues in the communication protocols used by the device are the three major areas to focus while testing an IoT device. This paper focuses on these three major components providing in depth details about what to look at to ensure that your IoT device is far away from hackers.

Keywords: IoT; IoT Security; Internet of Things security Testing; Embedded system security; Hardware security

I. INTRODUCTION

Internet of Things had proven that anything on this planet could be connected to the Internet. A coffee machine, refrigerators, light bulbs, baby monitoring utilities and the list goes on. This evolution has changed the way we live and thanks to the organizations that have initiated this evolution. The number of IoT devices in 2020 is expected to cross 50 billions.

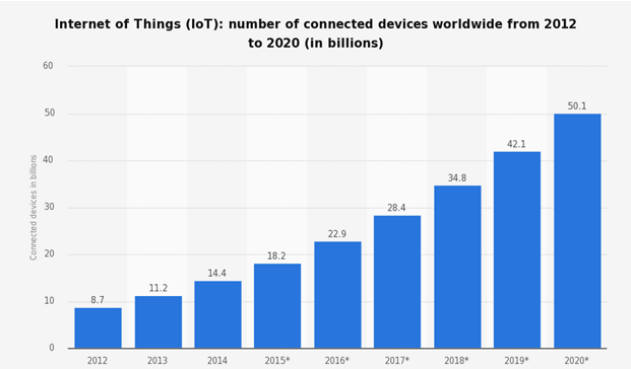

Figure 1. Evolution of IoT devices.

But, most of the manufacturers are not taking security of these IoT devices seriously while building them. Most of the manufacturers are in a rush to release their products into the market. They want their devices to have great features as quickly as possible. Since, IoT is not just a software component skillset also matters. The manufacturing companies should have both software and hardware security skill set if they want to ensure safety for their devices.

Testing hardware, software and communication channels is important to ensure the security of an IoT device. This paper provides some fundamental testing techniques that help manufacturers as well as security testers. Testing for security issues in the embedded device (Hardware), testing for security issues in the software used by the IoT device and testing for security issues in the communication protocols used by the device are the three major areas to focus while testing an IoT device.

II. THE IOT COMPONENTS

Hardware device, software and communication protocol are the three major components in IoT devices. Hardware device consists of the network gateway and the operating device, which does the processing in most of the IoT devices. Typical hardware security issues have to be tested on hardware device. Software component consists of any software that is involved in the architecture. Mobile application used to communicate with the hardware device, web application dashboard running on the device and the cloud component are the examples of the software components. Communication technology used in the device is another important element in any IoT device's architecture. Wi-Fi, Bluetooth Low Energy, Zigbee, ZWave and cellular are some examples of the communication technologies/protocols commonly used in IoT devices.

III. IDENTIFYING THE ATTACK SURFACE

Identifying the attack surface is the key in any security assessment. IoT is no exception. It is important to understand what are the attack vectors in the target IoT device's architecture. Before that, it is good to have a network diagram that shows various components of the IoT device and how the IoT device communicates with the Mobile app or any other device it interacts with. After identifying various components and communication technologies involved in the IoT device's architecture, we can start preparing the test cases to be executed against respective components. For example, if there is a web interface for configuring the IoT device, assess the web interface with various test cases such as SQL Injection, Remote Command Execution, Cross Site Scripting, Cross Site Request Forgery, No account lockout, weak passwords are allowed etc. The next section details various test cases to be executed against their respective components.

IV. SECURITY TESTING FOR INTERNET OF THINGS

This section shows some of the test cases to be executed against hardware, software as well as communication technologies.

A. Testing Hardware

Hardware testing or embedded device testing is usually done to identify the physical security holes such as exposed physical ports. This part usually includes opening the hardware device using screwdrivers in order to analyze and understand the components used in the embedded device. When a chip set is noticed, it is a good idea to get more information about it from the Internet or vendor documentation to get data sheets and understand detailed PIN outs of the chips. Most of the IoT devices use serial interfaces such as Universal Serial Bus (USB), Universal Asynchronous Receiver/Transmitter (UART), Serial Peripheral Interface bus (SPI), and Inter-Integrated Circuit (I2C) etc. for their communication with the device. Manufacturers often leave these interfaces open thus leaving the device's physical security at serious risk state. An attacker who finds these physical ports can further analyze the PINs and obtain a shell with root privileges on the device. This leads to full compromise of the hardware device. The easiest way to get a shell on the embedded device is to identify the Universal Asynchronous Receiver/Transmitter PIN. Once this PIN is identified, an attacker needs to identify the baud rate at which the device operates. Finally he can simply use a program like screen to obtain a shell on the embedded device. Testers should see if they could extract the firmware from the device using any of the exposed interfaces such as I2C or JTAG.

B. Testing software

Most of the today's IoT devices come with a mobile application. Since this mobile application is involved in the architecture, it needs to be tested for security issues. Some of the common test cases are looking for clear text transmission of sensitive data such as credentials, insecure data storage, hardcoded secrets in the code, un-obfuscated code, and weak authentication etc. Additionally, software testing should also cover testing of firmware that we extracted from the device or downloaded from Vendor's website. Depending on the file system type, we can mount the file system and explore the file system further. Running a tool like binwalk gives you information about different sections of firmware and it's file system type. Firmware often includes hardcoded secrets. This has to be properly tested. It is also possible to have backdoors in the firmware that comes with the device. It is a good idea to check for backdoors too.

Apart from firmware and mobile applications, we often see web dashboards to configure the respective IoT device. These dashboards often include serious web vulnerabilities. There have been many cases where remote code execution vulnerabilities are found on IoT devices through their web dashboards. All the web application security test cases have to be executed on these web dashboards.

C. Testing communication technologies

Though the definition of Internet of Things refers to the devices connected to the Internet, we often see devices that communicate over other protocols too. Bluetooth Low Energy, Zigbee, ZWave, 6LowPAN and cellular are some of the communication protocols being used in IoT devices. These protocols must be focused as well while testing the device. Clear text transmission of sensitive data is one of the most common things we see while assessing the security of IoT devices with these protocols. An attacker may find interesting information such as usernames, passwords in the traffic. Capturing the packets and replaying them using other tools is one of the common attack scenarios with these protocols. For example, if a device is built to work over Bluetooth Low Energy, it is common to have a mobile app to work with it. An attacker needs to capture the packets being transmitted from the mobile app and replay them using a custom script to gain control over the device. Interestingly, this replay attack works even when the data is encrypted. This is because; we are just capturing the legitimate traffic and replaying it.

V. TOOLS FOR TESTING IOT DEVICES

Some of the attack scenarios discussed in the previous sections of the paper need specialized tools. Security testing tools for Internet of Things devices are different from traditional tools we see with Web Application and Infrastructure penetration testing though they remain the same for Web application and infrastructure part of your IoT device. This section introduces some important tools that can be used in testing IoT devices.

A. MiTM Proxy

Mitmproxy is an application that allows intercepting HTTP and HTTPS communications between any HTTP(S) client and a web server.

B. Firmware Mod Kit

Firmware Mod Kit can be used to extract a firmware image, add our own code, and backdoor it and build a new version of the firmware. Firmware mod kit contains a set of tools both to extract, as well as build new firmware. For extraction, it also uses Binwalk as part of its extraction process.

C. Firmadyne

FIRMADYNE is used for performing emulation and dynamic analysis of Linux-based embedded firmware. It is automated and scalable.

D. Firmwalker

Firmwalker searches through the extracted or mounted firmware file system for things of interest such as:

- etc/shadow and etc/passwd
- list out the etc/ssl directory
- search for SSL related files such as .pem, .crt, etc.
- search for configuration files
- look for script files
- search for other .bin files
- look for keywords such as admin, password, remote, etc.
- search for common web servers used on IoT devices
- search for common binaries such as ssh, tftp, dropbear, etc.
- search for URLs, email addresses and IP addresses
- Experimental support for making calls to the Shodan API using the Shodan CLI

E. Flashrom

Flashrom helps to dump contents of a flash chip via the Serial Peripheral Interface(SPI).

F. ***Binwalk***

Binwalk is a tool used against firmware images. This is used for analyzing, reverse engineering, and extracting firmware images. This is fast and easy to use.

G. ***GDB***

GDB is a tool used to debug and analyze binaries.

H. ***Ubertooth***

Ubertooth is a popular wireless development platform, which is open source and suitable for experimenting Bluetooth. Ubertooth contains a BLE sniffer, which can be used to sniff some data from Basic Rate (BR) Bluetooth Classic connections.

VI. ACKNOWLEDGMENT

The authors gratefully acknowledge the contributions to the IoT Security community.

VII. REFERENCES

[1] OWASP IoT Testing guide.

[2] J Internet of Things: Converging Technology for Smart Environments and Integrated Ecosystems (River Publishers series in Information Science and Technology)(1 June 2013) Editors ovidiuVermesan& Peter Fries.3.

[3] Lei CHEN, Mitchell TSENG, Xiang LIAN. Development of foundation models for Internet of Things. Front. Comput. Sci. China 2010, 4(3): 376

[4] Ranade P, Londhe S. Smart Villages Through Information Technology

[5] Report on Connect 3 Platform & solution for smart village, by connect 3 Global Solutions Pvt. Ltd, 2015.