IoT Device Vulnerabilities and Security

Kayshaunna Williams
Jackson State University
shaunna.williams1@gmail.com

Kelvin Ly, Orlando Arias
University Of Central Florida
rangertime@knights.ucf.edu,
oarias@knights.ucf.edu

Yier Jin, Shaojie Zhang
University Of Central Florida
yier.jin@eecs.ucf.edu,
shzhang@cs.ucf.edu

Abstract

The world now is heavily dependent on wireless devices for most of its efficient functioning. These technological advances have their fair share of misfortunes when compared to their benefits. Most of these misfortunes arise in their vulnerability to exploitation. Considering that most are directly connected to the Internet, Internet of Things (IoT) devices have surfaces that are vulnerable to attack by anyone in the world. Many of these attacks originate from the challenges that are present in IoT devices such as less storage space and processing power.

While exploring IoT security this summer, we will be exploiting the D-Link Water Sensor via different techniques such as network scanning and reverse engineering, in hopes of educating users about the risks involving many of their everyday smart devices.

Water Sensor

This smart device connects via Wi-Fi, and is comprised of two main parts: The D-Link sensor, and its detachable alarm cable. Upon initial setup, the user is required to make a Wi-Fi connection via their smart phone to the network of the water sensor. It was then well aware that the device was operating as an access point. Using WireShark, the entire local network was then scanned and the device, along with its IP address was discovered. Its IP address was then scanned using NMap, and an unsecured server was discovered running on the device. Using different techniques such as DNS spoofing and reverse engineering, the plan was then to exploit that server in hopes of finding vulnerabilities within the device.

Acknowledgments: The support for this work was provided by the National Science Foundation REU program under Award No. 1560302. Any opinions, findings, and conclusions and recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

Network Probe of Device

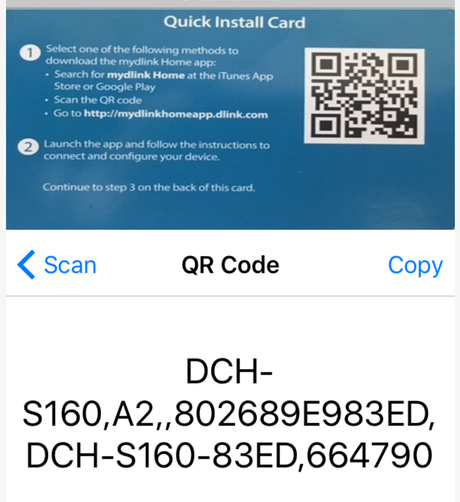
Wireshark is a free and open source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development. Wireshark was used to discover packets sent by the water sensor.

Nmap is a security scanner, used to discover hosts and services on a computer network. It sends specially crafted packets to the target host(s) and then analyzes the responses. Nmap was used to scan the IP address of the water sensor.

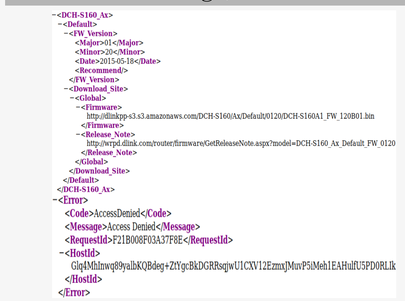
Lighttpd is an open-source web server optimized for speed-critical environments while remaining standards-compliant, secure and flexible. Network traffic from the water sensor was redirected to this personally configured webserver.

Dnsmasq is a Domain Name System (DNS) forwarder. It is lightweight and provides network infrastructure for small networks. Dnsmasq was used to redirect network traffic from the water sensor to the configured lighttpd server.

Data Found Using Personal QR Scanner



Firmware Image/ Release Notes



- Link to both firmware image and release notes lead to access denied error messages. Decryption of the HostID was also attempted. It unfortunately resulted in unreadable characters. These road blocks ultimately lead us in a different dirction and prompted the use of DNS spoofing.

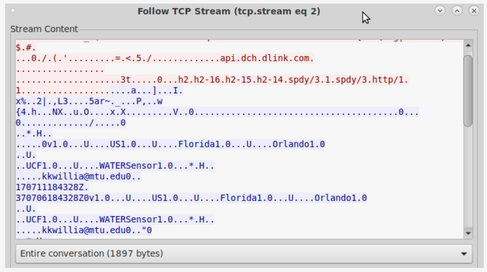
NMap Results

```
# nmap 192.168.0.60

Starting Nmap 7.50 ( https://nmap.org ) at 2017-07-06 13:16 EDT
Nmap scan report for 192.168.0.60
Host is up (0.036s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 80:26:89:E9:83:ED (D-Link International)

Nmap done: 1 IP address (1 host up) scanned in 13.84 seconds
```

Content Found on Server

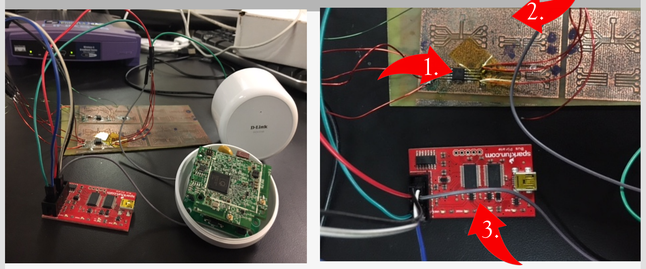
```
[http://192.168.0.60/version.txt]

Firmware External Version: V1.22
Firmware Internal Version: V1.22b03
Date: Wed, 27 Jan 2016
Checksum: 0x8652E35E
2.4GHz regulation domain: NA
1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11
Firmware Query: http://wrpd.dlink.com/router/firmware/query.aspx?model=DCH-S160_Ax_Default_FW_0122_802689E983ED
LAN MAC: 80:26:89:E9:83:ED
Kernel: 2.6.31, B0015, Date=Tue, 1 Dec, 2015
Apps: 1.1, B0138, Date=Mon, 25 Jan, 2016
WLAN Driver: AR9531, 10.2-00082-4, B0012, Date=Fri, 15 Jan, 2016
2.4GHz WLAN MAC 0: 80:26:89:E9:83:ED
2.4GHz SSID: DCH-S160-83ED
Factory Default: 1
DCH_ID: dc57995424d8840e99dd7fec7f22f806
```

Water Sensor Network Redirection

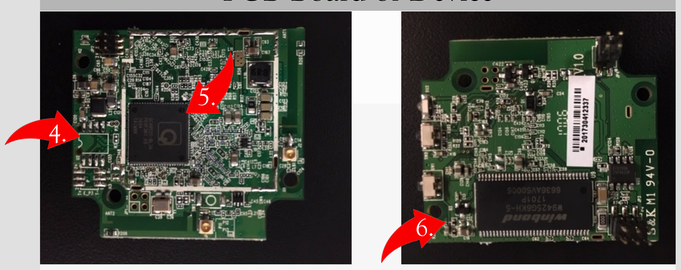


Physical Probe of Device

Device Configuration



PCB Board of Device



1. Breakout Board
2. Soldered Flash Chip
3. Bus Pirate

4. **Flash Memory Chip:** Figure one shows location of Flash Chip (M25-C136E). The chip was de-soldered from the PCB board and soldered onto a breakout board. It was then connected to a bus pirate for data dump.

5. **CPU:** This device is equipped with the QCA9531 System-on-a-Chip (SoC) for advanced WLAN platforms. This chip encompasses a feature-rich IEEE 802.11n 2x2 2.4 GHz System.

6. **Processor:** Figure three displays the W9425G6KH-5 Processor. W9425G6KH is ideal for main memory in high performance applications.

Firmware Conversion