Arizona State University
Center for Cybersecurity and Digital Forensics
781 Terrace Road, 4th Floor
Tempe, AZ 85281

iSmart Guard

Validation Project

Start: October 3, 2017
End: October 26, 2017

Objective

Determine the effectiveness of iSmart Guard against the external or internal hacking of WiFi enabled devices such as computers, laptops, and Internet-Of-Things. After 2 weeks, of use, all devices are analyzed to determine which connections are genuine, and therefore, “whitelisted” as authorized. All other connections are then blocked.

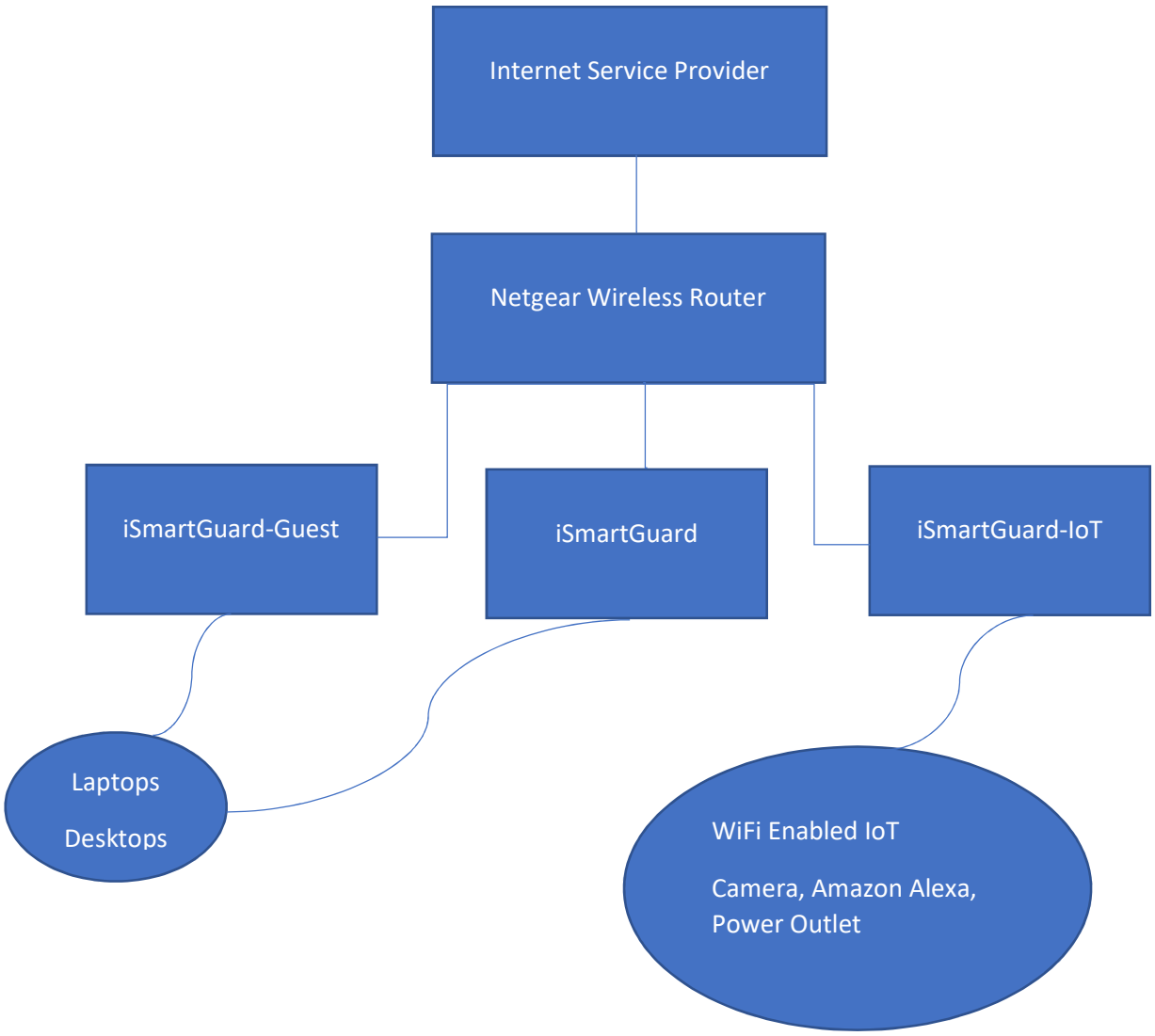
Environment

A suitable facility with public access.

Requirements

iSmart Guard requires an unrestricted Internet access via its Cat5 connection.

Exemplary Environment



Controlled WiFi Enabled Devices
SSID: iSmartGuard-IoT

These devices operate on a password protected iSmart Guard that is not shared with anyone.

__X___ IoT Device

Make: D-Link WiFi Camera

Model: DCS-5030L

Type: _____

__X__ IoT Device

Make: Amazon

Model: Echo

Type: _Personal Assistant

___X_ IoT Device

Make: August

Model: August-Connect

Type: ___Lock

___X__ IoT Device

Make: TP-Link

Model: Smart WiFi-Plug

Type: __Outlet

Data Collection

Week 1, iSmart Guard will monitor inbound and outbound data for:

SSID: iSmartGuard-IoT

iSmartGuard will not be use during week 1 to block any outbound or inbound connections as to simulate other WiFi router that are vulnerable to attacks from external and internal.

Week 2, iSmart Guard is powered on with all inbound connections closed off and outbound connections are only allowed to destination servers for which the devices are destined to. Administrator will have the ability to white list specific IP Addresses that are allowed to receive data from iSmartGuard.

For SSID iSmartGuard-IoT, IoT devices will only send data to their manufacturer and not third-party companies for which the manufacturers are affiliated. This will demonstrates that IoT devices are sending data to various sites for which consumers are not aware of, but have agreed to the terms and privacy policy of the IoT providers.

Report

After the 2-Week Pilot, a report is generated to demonstrate the effectiveness of iSmart Guard from external and internal attacks. All outbound IP Addresses are associated to the device description and MAC Addresses. For each device, please complete the following.

Device Description: **Amazon Echo** _____

MAC Address: _**80:58:f8:84:28:0b**_____

Inbound Connections
# of Attempts **0**_____ # of Successful Attempts **0**_____

* Blocked Outbound Connections
# of IP Addresses Blocked _47_____ # of IP Addresses Broke Through **0**_____

If the # of IP Addresses Broke Through is zero, it shows iSmart Guard provided 100% protection from hacking.

Outbound Connections
# of IP Addresses **198**_____

1st Highest ISP Requests **Google**_____ # of IP Addresses _**78**_____
2nd Highest ISP Requests **Amazon.com Inc.**_____ # of IP Addresses _**39**_____

Device Description **TP-Link**

MAC Address **b4:7c:9c:30:c1:22**

Inbound Connections
# of Attempts **0** # of Successful Attempts **0**

* Blocked Outbound Connections
# of IP Addresses Blocked **62** # of IP Addresses Broke Through **0**

If the # of IP Addresses Broke Through is zero, it shows iSmart Guard provided 100% protection from hacking.

Outbound Connections
# of IP Addresses **96**

1st Highest ISP Requests **Linode LLC** # of IP Addresses **18**
2nd Highest ISP Requests **Amazon.com Inc.** # of IP Addresses **9**

Device Description **August-Connect**

MAC Address **28:24:ff:cc:2f:b5**

Inbound Connections
# of Attempts **0** # of Successful Attempts **0**

* Blocked Outbound Connections
# of IP Addresses Blocked **0** # of IP Addresses Broke Through **0**

If the # of IP Addresses Broke Through is zero, it shows iSmart Guard provided 100% protection from hacking.

Outbound Connections
# of IP Addresses **1**

1st Highest ISP Requests **Multicast** # of IP Addresses **1**
2nd Highest ISP Requests _____ # of IP Addresses _____

Device Description **D-Link WiFi Camera**

MAC Address **b2:c5:54:3d:13:1c**

Inbound Connections
# of Attempts **0** # of Successful Attempts **0**

* Blocked Outbound Connections
# of IP Addresses Blocked **0** # of IP Addresses Broke Through **0**

If the # of IP Addresses Broke Through is zero, it shows iSmart Guard provided 100% protection from hacking.

Outbound Connections
# of IP Addresses **5**

1st Highest ISP Requests **Multicast** # of IP Addresses **4**
2nd Highest ISP Requests **Limited Broadcast** # of IP Addresses **1**

Conclusion

Based on the IoT tested, the Amazon Echo and the TP-Link made more connections to external IP Addresses.

TP-Link Power Outlet made more connections than usual for a smart power outlet. This Smart WiFi broadcast data to many locations, but mainly Linode LLC and Amazon.com Inc. All other IP Addresses were blocked by iSmart Guard and no connections were ever made to those other IP Addresses.

Amazon Echo made 198 connections because it utilizes external information to present to the user. Amazon Echo utilizes Google for its real-time data and therefore, allow Google to collect as much information about the user. The information collected also was shared with third party advertisement companies, such as Facebook. Once iSmart Guard blocked the third party companies, data stop flowing to those advertisement companies and only to Google and Amazon.

iSmart Guard was 100% efficient in allowing only authorized connections and in blocking all unauthorized ones.

Certification

Based on the information collected by iSmart Guard, attached hereto with this report, I certified that the information presented in this document is accurate and to the best of my knowledge based on the spreadsheet of data collected.

Assistant Research Professor, Arizona State university
Title

_____
Ziming Zhao

2017/10/30
Date