2021 Guide to a Secure Smart Home

Zachary Martin – Computer Information Technology (CIT)

Eastern Illinois University

Abstract

Smart Phones, Tablets, Gaming systems, Thermostats, Doorbells, and Cameras are among many devices that can be connected to internet. In a 2019 article, Statista.com estimated there will be 75.44 billion devices connected to home networks by 2025. In 2017, a casino's database of high rollers was compromised through an unsecured wireless thermometer in a fish tank (Forbes.com). The threat to our home networks are real and exploitable. The purpose of this capstone project is to research and document the current state of security in the 2021 smart home. The project also researches existing technologies and recommends solutions for securing the 2021 smart home.

The impacts of this capstone project are far reaching. In 2019, 86.6% of homes in the United States had a computer and 77.3% were connected to the Internet (National Center for Education Statistics). The recommendations from this proposal have wide reaching implications for millions of citizens and will hopefully give those looking for suggestions on securing their smart homes a reliable resources.

Research Objectives

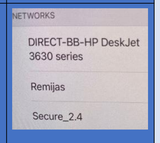
1. Research common home network security issues and vulnerabilities.
2. Demonstrate overlooked, but easily configured home wireless security settings.
3. Vulnerabilities and Exploits of commonly used Smart Home devices

Recommendations for Securing Wireless Home Networks

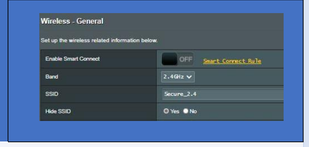
Securing Wireless Beacon

A wireless beacon is how wireless network are advertised as available for connections.
This is also a potential security concern.
Hiding/Securing a wireless beacon is one method of controlling what devices can access your network.

Beacons

Secure Beacon	Unsecure Beacon
	

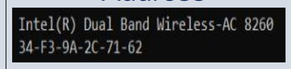
Access Point Configuration



Securing MAC Addresses

The Media Access Control Address (MAC) is hard coded into a device's Network Interface Card. By entering these MAC addresses into your Wireless Access Point manually a home user can control what devices can connect to their wireless networks.

Computer's MAC Address



Access Point MAC Configuration

Encryption Settings

Wireless Encryption options vary between Access Points and Wireless Standards. While many are available Advanced Encryption System or Counter-mode Cypher are recommended.

AES Encryption on an Access Point

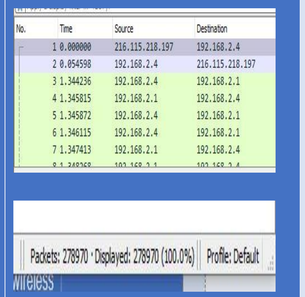
Experiment/Demonstrations

To demonstrate the security, or lack thereof, of smart home devices, two experiments were conducted with different technologies. Experiment 1 was using an Amazon Echo Dot. Experiment 2 was an unsecure FTP Honeypot Server.

Amazon Echo Dot

The Amazon Echo home devices have become commonplace in many homes for entertainment, shopping, scheduling, information and other daily activities.
It is rumored that these type of smart device are continually 'eavesdropping' on conversations and background activities such as TV viewing, web browsing, etc.
For six hours we ran Wireshark on the Echo Dot. We were not using the wireless network for any other activities.

Over six hours the Echo Dot sent roughly 218,000 data packets to the network. While it does not prove it is 'listening' it does prove that Echo devices are continually using the network.
Echo Dot IP Address: 192.168.2.4



No.	Time	Source	Destination
1	0.000000	216.115.218.197	192.168.2.4
2	0.054598	192.168.2.4	216.115.218.197
3	1.344236	192.168.2.4	192.168.2.1
4	1.345815	192.168.2.1	192.168.2.4
5	1.345872	192.168.2.4	192.168.2.1
6	1.346115	192.168.2.4	192.168.2.1
7	1.347413	192.168.2.1	192.168.2.4

FTP Honeypot Server

The goal for this experiment was to share a file on the live internet with no security. Due to the wireless security at my apartment I could not change security features thus my result were inconclusive.

Conclusions

In the summer of 2018, I took a class on wireless networking. During that class, the professor spoke of the wireless fish tank event at the Las Vegas Casino. I began to research vulnerabilities of wireless networks and it has become a professional interest of mine. The goal for my Capstone Project was to research and collect information about simple security mechanisms that the average home user can employ to secure their home networks. I also wanted to demonstrate the risks associated with the Internet of Things and the vulnerabilities associated with Smart Home Devices.

For anyone interested in learning more about the privacy associated with Smart Home devices please see the cnet.com article in my references and citations.

References/Citations

- Statista. (2021, January 22). *Internet of Things - number of connected devices worldwide 2015–2025*. https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/
- Mathews, L. (2017, July 27). *Criminals Hacked A Fish Tank To Steal Data From A Casino*. Forbes. https://www.forbes.com/sites/leemathews/2017/07/27/criminals-hacked-a-fish-tank-to-steal-data-from-a-casino/?sh=71df9d132b96
- *Number and percentage of households with computer and internet access, by state: 2015*. (2015). Number and Percentage of Households with Computer and Internet Access, by State: 2015. https://nces.ed.gov/programs/digest/d16/tables/dt16_702.60.asp
- Conner, K. (2020, March 26). *8 ways to protect your Amazon Echo privacy while working from home*. CNET. https://www.cnet.com/home/smart-home/8-ways-to-protect-your-amazon-echo-privacy-while-working-from-home/

Acknowledgements and Contact Information

I would like to thank Joliet Junior College's Cisco Networking Academy for the use of their Access Points and Equipment. I would also like to thank my Dad, Bill Martin for his support and advice on this project.

Contact Information:
Zachary Martin – CIT Class of 2021
zmmartin@eiu.edu

RESEARCH POSTER PRESENTATION TEMPLATE © 2019
www.PosterPresentations.com