Spring 5-3-2020

Effects of the IoT on Network Security

Zachary Virgo
zachary.virgo@valpo.edu

Effects of the IoT on Network Security

Zachary Virgo

Introduction

- The Internet of Things (IoT) is a group of network connected devices used for anything from controlling lights in a room to cooking and cleaning
- IoT devices are made by a large variety of manufacturers with a variety of uses and interfaces
- There is no set of laws of regulation in the Unites States setting guidelines for how to create these devices, including their security

How Big of an Impact Does the IoT Have?

- Estimated to have 75 billion connected units by 2025
- Can be found in homes across the world, but also factories, power plants, in the military and government facilities.
- Not just smart speakers and vacuums, but automated machines that put together cars, measuring devices, and drones.
- Collect personal data on users and on tasks they do.
- Data is at risk due to lack of security.

Purpose

- To show how suspectable to attack various IoT devices are in real world conditions without expensive, specialized equipment
- Analyze current legislation for IoT security and see if it is effective in helping manufacturers prevent attacks

Method

- Device types were chosen based on how popular they are
- Attacks were based on what a reasonable person could do without expensive specialized equipment and limited knowledge
- Attacks were researched and chosen based on past success
- 12 Volunteers were found with various IoT devices in their homes and these attacks were carried out with permission
- House 0 is a control, a home with no IoT devices, House 11 has at least one of each type but all devices have had firmware and patches updated to the latest version.

Device Types

- Amazon Alexa
- Google Home
- Smart Bulbs
- Smart Cars
- Smart Watches/Fitness Trackers
- Video Doorbell/Security Systems
- Baby Monitor
- Automated Vacuum
- Smart Locks

Amazon Alexa Methods

- Voice Squatting – An app (Skill) is created that leave the recording function open after the Skill is turned on. This is done by having the device attempt to say unpronounceable words (in this case H0R7!!). The Skill often has a name that sounds like a word often spoken, like Liight or Viirus, so it could be activated randomly through casual conversation near the device. Once run, it prompts the user to say their Amazon password, and records it.
- Yelling Through a Window- If an attacker can see a device through an open window, they can make it respond to commands. If the user has audio ordering turned on, and has not activated two factor authentication on the device, items can be purchased without the user's approval.

Amazon Alexa Data

- Skill was denied publishing from Amazon, but in testing inside volunteer homes did work.
- This was a widely reported vulnerability, that it appears Amazon has gotten better at detecting.
- Speaking to the device through an open windows does work, but if the built in two factor authentication has been enabled, it would require confirmation on the Amazon app.

Google Home Method

- Voice Squatting – Works similarly to the Alexa, except it is an Action instead of a Skill, and uses Python for coding.
- This one has an option to leave recording option for a certain amount of time built into the code, leaving it open for 100 seconds allows for recording of ambient discussion, and you can prompt the user for a password.
- Was never approved or disapproved of by Google, possible quality control or possibly just backlogged.
- Window Yelling – This method did work, but unless it has been set up previously voice enabled shopping isn't an option on the Home. Setting it up involves enabling two-factor authentication. Contact and Calendar information is accessable.

Smart Bulb Methods

- Large variety of products each that bring their own issues and vulnerabilities
- LIFX bulbs, found in store at many US retailers save network passwords in plaintext on the board inside the bulb, have to break the bulb to get to it.
- Many bulb systems can hook up to a hub, the most popular version of this is the ZigBee hub, which comes in various styles and is even built into some Amazon Echo devices. The processing stack can be exploited by software found online called ZigDiggity and around $40 of parts with a Raspberry Pi 3 B+

Smart Bulb Data

- LIFX bulbs were replaced, broken open and hooked up to a break board and files were transferred to Kali Linux, where the passwords were found in the file in plaintext as ASCII, which was then encoded to cleartext with an ASCII translator
- Two homes had non ZigBee smart hubs with bulbs hooked up to them and the bulbs could not be identified via radio transmission.
- Houses 2, 6, and 9 had bulbs with official ZigBee hubs that came packaged with bulbs, bulbs were identified via radio transmission and taken control of, allowing for full access to bulb control through console commands. A payload could them be added to the data stream and if the owner disconnected and reconnected the bulb with the payload, it could spread something malicious across the network.
- Houses 8 and 11 had Amazon Echo devices with ZigBee hubs built in, these could not be accessed in the same way. This could mean Amazon has increased security on these devices, or simply that the Echo devices auto update and others do not.

Smart Car Systems

- Vary in complexity depending on brand and model of vehicle.
- Can be hacked by accessing the Controller Area Network bus in all cars built since 1996, examining the traffic between the CAN and the car’s onboard computer, and then making false packets to send to make the cardo what you like.
- Requires very specific equipment with a high cost, and time to study each manufacture's specific system. Also, attempting this voids the warranty on the vehicle, so trying was decided against
- Vehicles with app control like FordPass which allows for locking and unlocking of the vehicle can be taken over with only a few minutes of physical access to the vehicle, but without a cloned FOB key, you can’t go more then a few feet away from the vehicle’s location.

Smart Watches/Fitness Trackers Method

- Many models can simply be stolen, if unlocked, thief will have access to data the device is connected to.
- Smart watch devices of models owned by volunteers (Apple Watch, Fit Bit Versa 2, Fossil Sport Watch) were tested with this method.
- A popular technique for phones, an evil twin attack was set up using a fake WiFi network set up using software on Kali Linix.

Smart Watches/Fitness Trackers Data

- Many newer devices have a feature that auto locks when removed from the wrist, a 4 digit pin must be entered to unlock, with limited attempts before the device had to be unlocked via an app on your phone or tablet. This prevents brute force attacks. This also prevent the “Steal” method from working on all the but the Fossil Sport, but the device only had access to apps such as Calendar and email.
- Some devices allow for this feature to be turned off, but it is required to have kind of payment app on the device (Google Pay, Apple Pay, ect.)
- Evil Twin attacks were found to be useable, as a fake, no password required network was set up for volunteers to connect to via their smart watches, none of them detected a problem with the network. Traffic was able to be monitored on this network.

Video Doorbells/Security Systems Method

- IP camera systems have one large weakness: weak passwords. While this plagues many IoT devices, these are often security system or monitoring inside homes.
- Using ID’s and Passwords gathered through other attack methods for devices, or default IDs and passwords, were attempted for logging into the system for these devices.
- Researchers also tried to shut the devices off temporarily using a DDoS attack after a scan to see camera IPs.

Video Doorbells/Security Systems Data

- Four of the houses, 2, 4, 7 and 9, were using either the default password for the devices or were using the same password they used for their network log in with the network name as the username.
- This gave complete access to the cameras, including being able to save recorded video.
- DDoS attacks disabled the cameras for roughly 4-5 minutes, which is the time it took them to boot up after being taken offline. If someone were trying to break in, this could give them a window.

Baby Monitor Method

- Similar to IP cameras and with similar vulnerabilities.
- Somewhat famous for lack of security features when pointed at sleeping babies.
- Default/Reused usernames and DDoS attacks were used
- Devices were also searched for on the popular open web search site Shodan which finds unsecured devices open to the internet.

Baby Monitor Data

- House 7 used the same user name and password as it did for its other IP camera system and its network.
- House 10 had left the system default username and password in place.
- Both devices were suspectable to DDoS attack and took nearly 10 minutes to reboot.
- House 10’s device was findable on Shodan, and with the default username and password, was accessable.

Automated Vacuum

- Most brands have vulnerabilities only accessible via physical access
- Some, typically cheaper, brands have remote vulnerabilities through techniques such as manipulating the MAC address of the device, or unsecured encryption.
- All volunteer homes with vacuums had iRobot Roomba devices, which, due to bad press, has increased security on recent models. While the device takes maps of your home and has a camera, current models have AES 256-bit encryption. At this time there are no known remote vulnerabilities for use with this brand of device.

Smart Locks Method

- Varied by brand, and type of lock
- Locks often have bad physical builds, even if the technology is sound
- Bluetooth Sniffing with a Raspberry Pi 4 and reelyActive software allows for packet collection over Bluetooth which can be analyzed in WireShark to potentially find password data before it is encoded.

Smart Locks Data

- 5 houses had locks of various types, 6 had a door lock deadbolt, and 5, 8, 10, 11 had padlocks.
- Only locks on house 6 and 11 were not able to be accessed via Bluetooth sniffing. 5, 8, and 10 had unencrypted information transferring between devices which included password data for the network.
- Of note, locks on houses 6 and 11 were purchased within the last year.
- Luggage locks, no matter how expensive, always have a master key for TSA agents at airports to be able to unlock. These have been leaked and can easily be 3D printed.

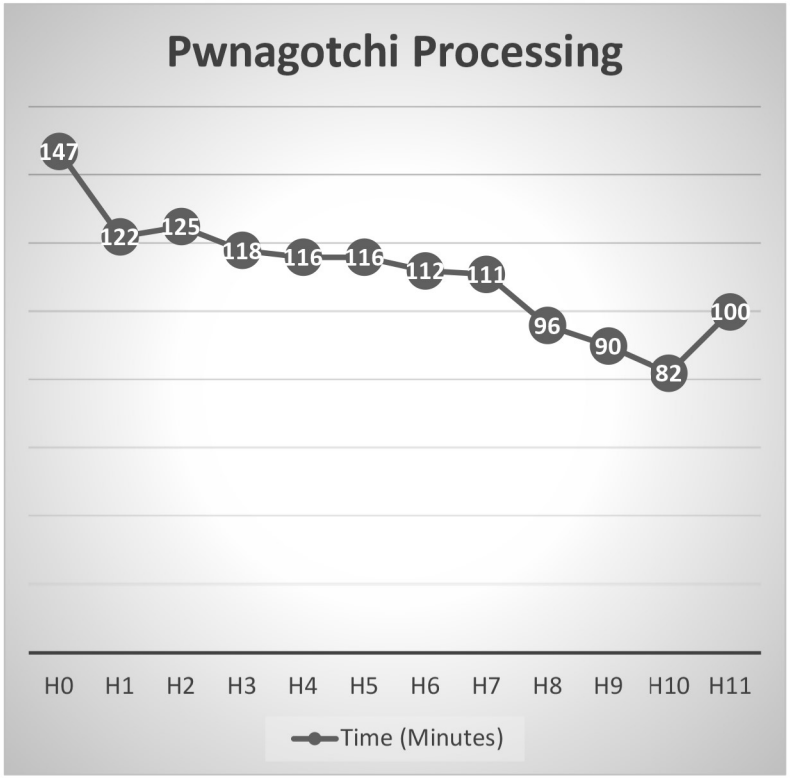
Pwnagotchi Attack Method

- A machine learning, WPA key stealing device built out a Raspberry Pi W and some opensource software.
- Given enough time on a detectable network, it reads the traffic between devices in order to try and find the hashed WPA network key, and save that to a file which can be run through a program such as Hashcat to be deciphered into cleartext.
- The idea is that more devices on the network talking constantly (as IoT devise are wont to do) will make the amount of time this attack takes shorter while giving it more accuracy due to low security standards on IoT devices.

Pwnagotchi Attack Data

House Number	Correct WPA2 Cracked
H0	Yes
H1	Yes
H2	Yes
H3	Yes
H4	Yes
H5	No
H6	Yes
H7	Yes
H8	Yes
H9	No
H10	Yes
H11	No

House Number	Amount of Time (in Minutes)
H0	147
H1	122
H2	125
H3	118
H4	116
H5	116
H6	112
H7	111
H8	96
H9	90
H10	82
H11	100



Pwnagotchi Attack Data Cnt.

- As the data shows, for most of the homes, the more devices on the network, the faster the device cracked the key, with the exception of House 11, which had the most devices, but also the most up to date devices and security.
- All networks had their WPA key cracked except 5, 9, and 11.

IoT Legislation

- No Federal legislation exists to govern the IoT or its security in the United States at current time.
- The National Institute of Standards and Technology (NIST) has released a set of guidelines for companies to follow, but it is not mandatory.
- Legislation was suggested in March 2019 for devices and companies sold to the US Federal Government which would put the NIST in charge of legislation for IoT devices, but it has not been voted on, this would not cover consumers.

IoT Legislation Cont.

- California and Oregon have passed laws in 2019 that set restrictions on IoT security and how collected data is handled.
- Unfortunately California's uses broad wording like requiring "reasonable security feature or features" or "Security appropriate to the nature of the function of the device."
- Oregon's law has more straightforward stating "a requirement that a user generate a new means of authentication before gaining access to the connected device for the first time."

Conclusions

- Security for IoT devices is as diverse as the devices themselves
- Some are very secure, others are almost completely open to the intent out of the box
- If manufacturers won't come together, legislation needs to be passed to require certain features be includes, or even automatically turned on, with these devices.
- This includes two-factor authentication, implementing strong usernames and passwords and proper encryption of data.

Considerations for Future Research

- The real world environment is chaotic with many variable like modem and router choices, age, and built in security. Results should be tested in a lab under controlled conditions for authenticity.
- This study tried to find easy to use methods that it doesn't take much time or money to be able to do, but further study in more intrusive but specialized methods should be done.
- Legislation from other countries should be compared to what is proposed in the USA to see if either can be improved.