“Alexa, are you Skynet?”
Not sure I believe her....
A Brief List of Topics

• Introduction
• Amazon Echo Hardware
• Alexa
• kasa
• Scripts to parse data?
• Security issues
• Questions/comments/etc.?
Jessica’s Introductory Introduction

• Hello, my name is Jessica Hyde
  – Hi Jessica!

• 6+ years Marines - Active Duty
  – 13ish years mobile exploitation/engineering/DFIR experience

• FUN FACT: I don’t run often, but I do run for Data Gen
I RUN FOR Data Gen
Brian’s Introductory Introduction

• Hello, my name is Brian Moran
  – Hi Brian!

• 13+ years Air Force Active Duty
  – 14ish years mobile exploitation/DFIR experience

• FUN FACT: Was unable to get smooth jazz by Davey C on my test Amazon account
THE VERY
BEST OF
DAVEY
C
Devices Used For This Presentation

• Android phones
  – Galaxy Note 2
  – Galaxy S5
  – BLU R1 HD

• Amazon Echo devices
  – Echo Dot (Gen 1)
  – Echo Dots (Gen 2)
  – Echo (Gen 1)

• Research on iOS phones & more Echo devices coming soon!!
How Did We Get Here?

• Adrian (@Cheeky4n6Monkey) tried very hard to win an Echo last year for chip off
  – Spurred some initial thoughts
• A smart bulb, controlled by Alexa, was the perfect fix for impending doom in my home
  – To turn off a lamp, had to stand on the couch, right in front of stairwell
• Wanted to generate data (and use) smart home devices for an extended period of time
  – Not just one week of test data

“TURN OFF THE LIGHT BEFORE COMING TO BED” SHE SAID
“IT WILL BE FINE” SHE SAID
Amazon Echo Devices

- Stuff about the Echo family
- What it does
- Etc, etc.
Sources of Data

• Hardware
  – Amazon Echo
  – Amazon Echo Dot
Sources of Data

• Mobile Apps
  – Alexa
  – Kasa
Sources of Data

- Network
- Connected devices
Amazon Echo Devices

• How do you get to data on the device?
• Destructive vs. Non Destructive
• Ports
  – USB – root-able?
  – JTAG - no ports
  – ISP – eMMC – yes!
• What is the quickest way to see what is stored?
  – Chip-off followed by ISP
Amazon Echo

- Original Echo
- Disassembly
  - Well documented
- Device from WV
  - From an actual case
  - Compared to test device (from Teel Tech Canada)
Amazon Echo

- Research
- Components
  - SanDisk SDIN7DP2-4G
    - 4GB iNAND Ultra Flash Memory
    - Documented

https://www.ifixit.com/Teardown/Amazon+Echo+Teardown/33953
Amazon Echo

- ISP Pin out
  - VCC
  - VCCq
  - CMD
  - CLK
  - DAT0
Echo ISP Pinout
Amazon Echo

- Research pin out
- ISP using Z3X Easy JTAG Box
Amazon Echo Dot

- Echo Dot
- Disassembly
  - No Documentation
- Devices from Brians’ smart home
  - One from test network
  - One from real use – 1 year
  - Compared to new OOB device
Amazon Echo Dot

• Components
  – Different eMMC on each board
    • Micron 6PA98 JWB30
    • SEC 625
      B213
      KMF J2005A S4DCVA9VC

• Challenge
  – No Data Sheet
  – Assume eMMC

Amazon Echo Dot

- Chip-off
  - New out-of-box
  - Used IR station
    - Thanks Teel Tech Canada
- Clean and Read chip
- Determine pinout by researching SD standard for BGA pattern
Amazon Echo

- ISP Pin out
  - VCC
  - VCCq
  - CMD
  - CLK
  - DAT0
Echo ISP Pinout
Amazon Echo

- Image 4GB eMMC using RIFF2
- Huzzah – Non-destructive ISP method
- Apply ISP method to Brian’s device (used 1 year)

https://www.riffbox.org/
Amazon Echo Flash Dump
Amazon Echo Flash Memory

- What data can we find?
  - WiFi Connections
    - device_information_logs
  - Registration Information
    - data\local\token\registrationinfo.txt
Alexa

• “Alexa” is virtual assistant on Amazon Echo devices
• Amazon Alexa is also the name of the application you can install on your mobile device
• You can do many, many things with the application
  – In many different ways
Alexa mobile application

- View your Echo devices (Dot, Echo Tap, Echo Show, etc)
- Control what’s playing on an Echo device
- (NEW, May 2017) Message and call other Amazon Alexa application users
  – And Echo device owners
Alexa mobile application

Conversations

Brian Moran
Hi from the new Dot... or is it?
10:22 PM

Stacey Randolph
And testing from the BLU, with no number yet
5:25 PM

Peacock Leprechaun
Hello

Thursday

Now you can communicate with your friends and family who have Echo devices or the Alexa app.

Try saying:
“Alexa, send a message”
“Alexa, make a call”
“Alexa, play my messages”

To-do List

Hope The IOT Uprising Happens...

Shopping List

Make Peacock Leprechaun Great...

Welcome!
Alexa mobile application

• Very little information is stored within the application itself, there have been numerous posts on the data that is stored, so we won’t go over that

• Most of the data is pulled from URLs (more on that soon!)
Alexa mobile application

• There is a file named “comms.db” stored in the Alexa application folder under the path
  – “data\com.amazon.dee.app\databases”

• One could wager this contains messages/messaging information
  – The data is encrypted, have not figured out the encryption/decryption yet

• Kudos to Amazon! (But we did find a work around!!)
Alexa mobile application

• One database file worth noting for later use is “map_data_storage_v2.db”, stored under the path “data\com.amazon.dee.app\databases”

• It was possible, in previous versions, to pull out authentication data & use that to access information. This is no longer the case as the data is now encrypted
  – This is why it is important to stay on top of new releases!

• The main thing we want from here is the Amazon account ID string
Alexa mobile application

<table>
<thead>
<tr>
<th>id</th>
<th>account_data_directed_id</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>amzn1.account.AEAM5TQ27DKFM7VJXYY3SFBDAI0Q</td>
</tr>
</tbody>
</table>
Alexa mobile application

• We be using this string shortly
  – “amzn1.account.AEAM5TQ27DKFM7VJXY3SFBDCAIQ”
Alexa web application

• Browse to the URL
  “http://alexa.amazon.com/”
  – Should be required to sign in to your Amazon account

• Even more options than the mobile app
  – But no messaging!
Alexa web application
Alexa applications (behind the GUI)

• Remember we said most of the data is pulled from URLs
  – One we will use a LOT is variations of “https://pitangui.amazon.com/api”

• In fact, if your investigation involves Amazon Echo/Alexa, most of your good information will come from here
  – HINT: One keyword should be “pitangui.amazon.com/api”

• You will need the email address & password for the Amazon account in question
Alexa Calling & Messaging

- Remember the string from before?
  - amzn1.account.AEAM5TQ27DKFM7VJXYY3SFBDCAIQ

- We will add it to the URL "https://alexa-mobile-service-na-preview.amazon.com/users/amzn1.comms.id.person.amzn1~"

https://alexa-mobile-service-na-preview.amazon.com/users/amzn1.comms.id.person.amzn1~amzn1.account.AEAM5TQ27DKFM7VJXYY3SFBDCAIQ
Alexa Calling & Messaging

• To view the Alexa Contacts, use this full URL
Alexa Calling & Messaging
Alexa Calling & Messaging

• To view the Alexa Conversations, use this full URL

Alexa Calling & Messaging
Alexa Calling & Messaging

• We will need the conversation ID to get the messages for each conversation
  – “amzn1.comms.messaging.id.conversation~KEnAPYR-kjxtaYjvqetm_lhU8OQ”

• We will add that to the URL “https://alexa-mobile-service-na-preview.amazon.com/users/amzn1.comms.id.person.amzn1~amzn1.account.AEAM5TQ27DKFM7VJXYY3SFBDCAIQ/conversations/”

• And append “messages?count=100&sort=asc” to the end of the URL
Alexa Calling & Messaging

• So to view the messages, this is our URL:

Alexa Calling & Messaging

```
{
  "conversationId": "amzn1.comms.messaging.id.conversation~KEnAPYR-kjxtaYjvqtem_lhU8Q0", "messages": [
    {
      "conversationId": "amzn1.comms.messaging.id.conversation~KEnAPYR-kjxtaYjvqtem_lhU8Q0", "messageId": 1, "sequenceId": 1, "time": "2017-05-11T18:38:52.654Z", "sender": "amzn1.comms.id.person.amzn1~amzn1.account.AEAM5TQ27DKFM7VJXYY3SFB DCAIQ", "type": "message/text", "payload": { "text": "Now you can call and message your friends and family that have Echo devices. To set up additional members of your family, download and install the app on their phone." }
    },
    {
      "conversationId": "amzn1.comms.messaging.id.conversation~KEnAPYR-kjxtaYjvqtem_lhU8Q0", "messageId": 2, "sequenceId": 2, "time": "2017-05-11T18:39:02.024Z", "sender": "amzn1.comms.id.person.amzn1~amzn1.account.AEAM5TQ27DKFM7VJXYY3SFB DCAIQ", "type": "message/text", "payload": { "text": "Hello" }
    },
    {
      "conversationId": "amzn1.comms.messaging.id.conversation~KEnAPYR-kjxtaYjvqtem_lhU8Q0", "messageId": 3, "sequenceId": 3, "time": "2017-05-19T03:59:32.315Z", "sender": "amzn1.comms.id.person.amzn1~amzn1.account.AEAM5TQ27DKFM7VJXYY3SFB DCAIQ", "type": "message/text", "payload": { "text": "Hi" }
    }
  ]
}
```
Alexa Calling & Messaging

• Important things to note:

  – The URL query only allows for 100 messages
  – You must be signed in as the user (username and password)
  – This may change in the future. Or by the time we give this presentation!
Alexa Devices

• Browse to https://pitangui.amazon.com/api/devices/device?

• This lists all the Alexa enabled devices associated with the account (in JSON format)
Alexa Devices

```json
{
  "devices": [{
    "accountName": "Peacock's Echo Dot",
    "appDeviceList": [],
    "capabilities": [
      "PAIR_BT_SOURCE",
      "KINDLE_BOOKS",
      "EARCONS",
      "REMINDERS",
      "PAIR_REMOTE",
      "REQUIRE_OOBE_FOR_SETUP",
      "AUDIOPLAYER",
      "FAR_FIELD_WAKE_WORD",
      "SUPPORTSCONNECTEDHOME",
      "PAIR_BT_SINK",
      "DREAM_TRAINING",
      "CUSTOM_ALARM_TONE",
      "LEMUR_ALPHA",
      "UPDATE_WIFI",
      "FLASH_BRIEFING",
      "I_HEART_RADIO",
      "POPTART",
      "AUDIBLE",
      "SUPPORTS_SOFTWARE_VERSION",
      "TUNE_IN",
      "TIMERS_AND_ALARMS",
      "SOUND_SETTINGS",
      "VOICE_TRAINING",
      "PERSISTENT_CONNECTION",
      "SET_LOCALE",
      "SUPPORTS_CONNECTED_HOME_ALL",
      "PANDORA",
      "AMAZON_MUSIC",
      "SLEEP",
      "ACTIVE_AFTER_FRO",
      "DEREGISTERDEVICE",
      "CHANGE_NAME",
      "SALMON"
    ],
    "charging": null,
    "clusterMembers": [],
    "deviceAccountId": "AO06W5SC0ZPW80",
    "deviceOwnerCustomerId": "A260ZWE7XUMK9M",
    "deviceType": "A355BH2HU6VAYF",
    "essid": "PeacockNet",
    "language": null,
    "macAddress": "40B4CD10B295",
    "online": true,
    "parentClusters": [],
    "postalCode": null,
    "registrationId": null,
    "remainingBatteryLevel": null,
    "serialNumber": "G090L90970950GPN",
    "softwareVersion": "575215620"
  }]
}
```
Alexa Devices
Alexa Devices

• We now have the following items:
  – A3S5BH2HU6VAYF
    • Model type of Echo Dot
  – G090L90970950GPN
    • Serial Number of Echo Dot
  – A260ZWE7XUMK9M
    • Customer ID
  – 575215620
    • Software version
  – AOO6WSCOZPW80
    • Device Account ID

• Searching for these may lead to more URLs to pull data from!
Alexa Cards

• Browse to https://pitangui.amazon.com/api/cards?

• This lists the “cards” associated with the account
  – You can see these on the website as well
    • But much more pretty than JSON
Alexa Cards
Alexa Wifi

• Browse to
  “https://pitangui.amazon.com/api/wifi/configs?”

• This lists wireless network information that the user chooses to save to the Amazon cloud (on by default)
  – Including SSID & plain-text password
Alexa Wifi

JavaScript code snippet:

```json
{ "values": [{
    "deviceSerialNumber": null,
    "deviceType": null,
    "preSharedKey": "pw4peacocknet",
    "securityMethod": "WPA_PSK",
    "ssid": "PeacockNet"}
}]
```
Alexa Smart Home Devices

• Browse to “https://pitangui.amazon.com/api/phoenix?”

• This lists all the Smart Home devices, and groups, that the user has associated with the Alexa account
Alexa Smart Home Devices
Alexa Activities

• Browse to “https://pitangui.amazon.com/api/activities?size=100&offset=-1”

• This the last 50 activities that was performed by Alexa
  – Regardless of device that it originated from
    • Currently last 50 are returned, but URL lists size as 100 just in case Amazon changes that amount!
Alexa URLs

• There are many more known (and probably unknown) URLs to pull data from as well

• Smart keyword searching is DEFINITELY your friend
kasa mobile application

• “kasa” is the mobile application for TP-Link smart devices
  – Smart Plug (HS100/110)
  – Smart Plug Mini (HS105)
  – Smart Switch (HS200)
  – Smart Bulbs (LB100/110/120/130)
  – Range Extender (RE350K)
  • As of May 8, 2017
kasa mobile application (cont.)
kasa mobile application (cont.)

- \"data\com.tplink.kasa_android\" is the path to kasa folder on device
- Folder of primary interest is “databases”
- This folder contains (surprise) SQLite databases
kasa mobile application (cont.)

Data viewed in X-Ways 19.2
kasa mobile application (cont.)

• “databases” folder contains at least four database files
• Take a guess which one contains all of the kasa user data??
kasa mobile application (cont.)

Well that is a convenient name!

Data viewed in X-Ways 19.2
• Contains at least 8 tables, with straightforward naming conventions.

• For example, "accounts" contains account information

– Notice anything particularly useful?
iot.1.db – “accounts”

<table>
<thead>
<tr>
<th>createdOn</th>
<th>email</th>
<th>firstN...</th>
<th>id</th>
<th>lastN...</th>
<th>password</th>
<th>refe...</th>
<th>token</th>
</tr>
</thead>
<tbody>
<tr>
<td>1494813551654</td>
<td><a href="mailto:peacockleprechaun@gmail.com">peacockleprechaun@gmail.com</a></td>
<td>9E8...</td>
<td></td>
<td></td>
<td>pw4plamazon</td>
<td></td>
<td>e5e500ed-42808</td>
</tr>
</tbody>
</table>
iot.1.db – “accounts”

• Yup! That is the password*, in plain-text!

Data viewed in SQLiteSpy 1.9.6

* Please note, this is no longer my password. No legitimate passwords were harmed in the making of this presentation
iot.1.db – “devices”

• Following that line of thinking, I bet “devices” contains a list of all the TP-Link devices associated with the account!
### Data viewed in SQLiteSpy 1.9.6

<table>
<thead>
<tr>
<th>addr...</th>
<th>appServerUrl</th>
<th>cate...</th>
<th>cloud...</th>
<th>createdOn</th>
<th>deviceAddress</th>
<th>deviceAlias</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><a href="https://use1-wap.tplinkcloud.com">https://use1-wap.tplinkcloud.com</a></td>
<td></td>
<td></td>
<td>1494271325826</td>
<td>50:C7:BF:</td>
<td>Upstairs Plant Outlet</td>
</tr>
<tr>
<td></td>
<td><a href="https://use1-wap.tplinkcloud.com">https://use1-wap.tplinkcloud.com</a></td>
<td></td>
<td></td>
<td>1494271325781</td>
<td>50:C7:BF:</td>
<td>Downstairs Couch Light</td>
</tr>
<tr>
<td></td>
<td><a href="https://use1-wap.tplinkcloud.com">https://use1-wap.tplinkcloud.com</a></td>
<td></td>
<td></td>
<td>1494271325780</td>
<td>50:C7:BF:</td>
<td>Downstairs Plant Light</td>
</tr>
<tr>
<td></td>
<td><a href="https://use1-wap.tplinkcloud.com">https://use1-wap.tplinkcloud.com</a></td>
<td></td>
<td></td>
<td>1494271325761</td>
<td>50:C7:BF:</td>
<td>Living Room Green Lamp Light</td>
</tr>
<tr>
<td></td>
<td><a href="https://use1-wap.tplinkcloud.com">https://use1-wap.tplinkcloud.com</a></td>
<td></td>
<td></td>
<td>1494271325734</td>
<td>50:C7:BF:</td>
<td>Kitchen Sink One</td>
</tr>
<tr>
<td></td>
<td><a href="https://use1-wap.tplinkcloud.com">https://use1-wap.tplinkcloud.com</a></td>
<td></td>
<td></td>
<td>1494271325707</td>
<td>50:C7:BF:</td>
<td>Kitchen Sink Two</td>
</tr>
<tr>
<td></td>
<td><a href="https://use1-wap.tplinkcloud.com">https://use1-wap.tplinkcloud.com</a></td>
<td></td>
<td></td>
<td>1494271325684</td>
<td>50:C7:BF:</td>
<td>Panda Lamp Light</td>
</tr>
<tr>
<td></td>
<td><a href="https://use1-wap.tplinkcloud.com">https://use1-wap.tplinkcloud.com</a></td>
<td></td>
<td></td>
<td>1494271325607</td>
<td>50:C7:BF:</td>
<td>Couch Lamp Light</td>
</tr>
<tr>
<td></td>
<td><a href="https://use1-wap.tplinkcloud.com">https://use1-wap.tplinkcloud.com</a></td>
<td></td>
<td></td>
<td>1494271325634</td>
<td>50:C7:BF:</td>
<td>Dino Light Bulb</td>
</tr>
<tr>
<td></td>
<td><a href="https://use1-wap.tplinkcloud.com">https://use1-wap.tplinkcloud.com</a></td>
<td></td>
<td></td>
<td>1494271325662</td>
<td>50:C7:BF:</td>
<td>Downstairs Black Lamp Light</td>
</tr>
<tr>
<td></td>
<td><a href="https://use1-wap.tplinkcloud.com">https://use1-wap.tplinkcloud.com</a></td>
<td></td>
<td></td>
<td>1494271325662</td>
<td>50:C7:BF:</td>
<td>Bedroom Plant Bulb</td>
</tr>
</tbody>
</table>

### SANS DFIR Summit - 2017
## Data viewed in SQLiteSpy 1.9.6

### Table: `iot.1.db` – “devices”

<table>
<thead>
<tr>
<th>deviceName</th>
<th>deviceId</th>
<th>deviceM</th>
<th>deviceClass</th>
<th>deviceAddress</th>
<th>createdDate</th>
<th>createdTime</th>
<th>cloudId</th>
<th>cloudTime</th>
<th>deviceId</th>
<th>deviceClass</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upstairs Plant Outlet</td>
<td>800679A0</td>
<td>04D</td>
<td>switch</td>
<td>149471325826</td>
<td>1449</td>
<td>18:31:39</td>
<td>149471325826</td>
<td>1449</td>
<td>18:31:39</td>
<td>800679A0</td>
</tr>
<tr>
<td>Downstairs Couch Light</td>
<td>80082686</td>
<td>3D0</td>
<td>switch</td>
<td>149471325781</td>
<td>1449</td>
<td>18:31:39</td>
<td>149471325781</td>
<td>1449</td>
<td>18:31:39</td>
<td>80082686</td>
</tr>
<tr>
<td>Downstairs Fireplace Plant Light</td>
<td>80099520</td>
<td>33D</td>
<td>switch</td>
<td>149471325761</td>
<td>1449</td>
<td>18:31:39</td>
<td>149471325761</td>
<td>1449</td>
<td>18:31:39</td>
<td>80099520</td>
</tr>
</tbody>
</table>

---

### Additional Details

- Data was viewed using SQLiteSpy 1.9.6, a tool for exploring SQLite databases.
- The database `iot.1.db` contains records for various devices, including switches and light bulbs.
- Each record includes fields such as `deviceName`, `deviceId`, `deviceM`, `deviceClass`, and `deviceAddress`.
- The timestamps associated with device creation and updates are also recorded.
iot.1.db – “devices”

- Created date, device MAC address, user created alias, device type, unique device ID, model, given name, current device state, hardware ID, IP address, cloud bound (remotely controllable), signal strength, etc.

- SOO MANY DETAILS!!
iot.1.db – “locations”

- Contains account ID, created time, last sync time, and geographic coordinates of where the user account is
iot.1.db – “locations”

<table>
<thead>
<tr>
<th>accountId</th>
<th>bindToCloud</th>
<th>createdOn</th>
<th>id</th>
<th>lastSyncTime</th>
<th>latitude</th>
<th>locationAlias</th>
<th>longitude</th>
<th>timezone</th>
<th>updatedOn</th>
</tr>
</thead>
<tbody>
<tr>
<td>838D049</td>
<td></td>
<td></td>
<td></td>
<td>1483065913541</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>id</th>
<th>lastSyncTime</th>
<th>latitude</th>
</tr>
</thead>
<tbody>
<tr>
<td>58A6D</td>
<td>1489440270859</td>
<td>39.1189215095865</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>locationAlias</th>
<th>longitude</th>
<th>timezone</th>
<th>updatedOn</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>-76.6179607641965</td>
<td>America/Cancun</td>
<td>1493147488659</td>
</tr>
</tbody>
</table>

Data viewed in SQLiteSpy 1.9.6
iot.1.db – “locations”

• A quick Google map search shows the location to be pretty accurate.
  – Not 100% accurate, but pretty darn close!
A quick Google map search shows the location to be pretty accurate. Not 100% accurate, but pretty darn close!

iot.1.db – “locations”
Scripts to parse data?

• We are working on it! Pinky Swear!

• Why not today?
  – Want to wait for the Echo Show to come out
    • Data may change. And probably have more data

• ....biggest reason, we found a lot of security issues within kasa & Alexa
kasa Security Concerns (initially)

• Account credentials (email & password) saved in plain-text

This means any person, anywhere in the world, can log into the kasa application with the credentials, & remotely control configured devices

– Thanks to Stacey (@4n6woman) for testing this!!
kasa Security Concerns (cont.)

• You don’t have to be logged in to an account to control TP Link devices
  – You just have to be on the same wireless network
  – The app finds devices and lets you add them, as long as they are on the same wireless network as the mobile device
Addressing kasa Security Concerns

• Update: TP-Link will have an update to the application by June 23rd (the date of this presentation)
  – No longer storing credentials in plain-text
  – Must now sign in to kasa to control devices (both locally and remotely)
    • This means Timmy at the family reunion can no longer control the smart home just because he downloaded kasa app
      – Sorry Timmy!
Addressing kasa Security Concerns (cont.)

• TP-Link has (will have been) outstanding in working with us to ensure these issues are fixed
  – Should be addressed in kasa update before June 23\textsuperscript{rd} (this presentation date)
• TP-Link has continually stressed that they are actively working on identifying any/all issues and balancing the fine line between user security & usability

• Honestly wish that more companies took such an active approach to working with researchers to identify, mitigate, and implement solutions to security concerns
  – Many, many thanks to TP-Link!!
Alexa Security Concerns

- Initially, we found almost nothing with security issues of Alexa

- Alexa Calling & Messaging changed all of that

- Thanks to Twitter, we were able to get in directly touch with security folks at Amazon in about an hour
Alexa Security Concerns (cont.)

• Initially, no way to block Alexa contacts
  – Ironic, because the underlying code does account for blocking contacts
  – Must contact Amazon to delete contacts

• Easy Fix: Don’t keep the contact information of people you don’t want to talk to in your phone
Alexa Security Concerns (cont.)

Simple request, right? I was shocked by the response.
Alexa Security Concerns (cont.)

• Not being able to block contacts was about 0.001% of the problem

• The discovery happened on Thursday afternoon, right after the Alexa app was released with the new Calling & Messaging feature
  – And about 12 hours before the contact blocking story made its round
  – Also the WannaCry ransomware helped shift focus elsewhere (fortunately. Or unfortunately)
  – Again, within an hour, we were talking to the right folks at Amazon
Alexa Security Concerns (cont.)

Do I know anyone, specifically dealing with Alexa Calling & Messaging, at Amazon? I need to talk to them right now.

RETWEETS | LIKES
---|---
8 | 3

3:32 PM - 11 May 2017

Tweet your reply

@brianjmoran they've given a heads-up to the relevant team. can you send details to security@amazon.com?
Alexa Security Concerns (cont.)

• The issues were discovered, ironically, because the app did not work properly on my Galaxy Note 2 test device
  – If the app had worked, probably would not have stumbled on this

• As it turns out, the Alexa application is set to automatically pull data, from a variety of sources, as quickly as possible
  – Ease of use, convenience, as little user interaction as possible
    • All are really good reasons from a regular user standpoint!
Alexa Security Concerns (cont.)

• The first sign in, by a user on a mobile device, requires a PIN sent, via SMS, to verify that user.
• That is the only time that it was needed.

• If you have access to the Amazon credentials, you can sign into any device that has the app installed.
Alexa Security Concerns (cont.)

• This means that you could
  – Make Alexa Calls as another person
  – Receive Alexa Calls being sent to another person
  – Send Alexa Messages as another person
  – Receive Alexa Messages being sent to another person
  – Have Alexa contacts synced to your device

• All without the original user ever knowing!
Alexa Security Concerns (cont.)
Alexa Security Concerns (cont.)

• My two test phones rang and Stacey’s rang in Chicago, all while signed into the Peacock Leprechaun account
  – Echo devices will also ring as well

• When the call is answered, a brief message flashes on the screen saying it was answered on another device
Alexa Security Concerns (cont.)

• All of my contacts replicated across the Peacock Leprechaun account, regardless of what device it was signed in on

• Even enabling two factor authentication did not change that, once the user logged in on the device, they were in the account
Alexa Security Concerns (cont.)

• The wifi/configs? URL query could also give someone who has your Amazon account credentials the SSID & plain-text password for your wireless network(s)
  – As long as they are saved to Amazon (on by default)
Addressing Alexa Security Concerns

• You can call Amazon to remove wifi profiles from your account
  – Watch your Echo while you do this
• Or you can do it through the browser...

You can delete your saved Wi-Fi information from the Manage Your Content and Devices page.

In your web browser:
1. Go to www.amazon.com/mycd
2. Click the Settings tab.
3. Under Saved Wi-Fi Passwords, click Delete.

The next time you connect to a new Wi-Fi network, make sure you deselect "Save password to Amazon."

Thanks for using Alexa.
Addressing Alexa Security Concerns (cont.)

• Amazon security team working on fixes
  – ETA early June
    • Should be before this presentation!

• Amazon was very happy that we identified issues & shared this with them

• The Amazon security team has been fantastic to work with!
The Road Ahead

• Add iOS device testing
• Create scripts to parse the SQLite and JSON data
• Get some robust testing done with Echo Show
• Continue to help ensure applications are working in as secure a manner as possible
Summary

• Alexa data is stored primarily in the cloud
  – Very little is available offline
• The kasa/TP-Link application stores a ton of useful data in plain-text
  – But not as much thanks to our research!
• Account credentials are all that is needed to control smart home devices from anywhere
• Connected applications (Alexa’s “skills”) however likely contain a good amount of data
• Amazon’s security team is really on top of things!
• TP-Link also takes smart home security very seriously!

• Alexa is not quite Skynet …
Questions?

Contact Us!

Jessica Hyde
Twitter: @B1N2H3X
Email: Jessica.hyde@magnetforensics.com

Brian Moran
Twitter: @brianjmoran
Email: brian@brimorlabs.com