“Alexa, are you Skynet?”

Jessica Hyde
Director of Forensics – Magnet Forensics
Adjunct Professor – George Mason University

Brian Moran
Digital Strategy Consultant – BriMor Labs
Not sure I believe her....
A Brief List of Topics

• Introduction
• Amazon Echo Hardware
• Alexa
• kasa
• Security issues
• Scripts to parse data?
• 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 S5
  – BLU R1 HD

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

• Research on iOS phones & more Echo devices continues, because Amazon keeps making new ones!
App Versions Used For This Presentation

• Alexa (Android)
  – 1.24.2556.0

• Kasa (Android)
  – 1.9.1 Build 697

• **REMEMBER:** Data can slightly (or drastically!) change between app versions
How Did We Get Here?

- Adrian (@Cheeky4n6Monkey) tried very hard to win an Echo at SANS DFIRSummit in 2016 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
Obligatory Meme Capturing Research Mindset
Sources of Data

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

• Mobile Apps
  – Alexa
  – Kasa
Sources of Data

- Network
- Connected devices

OSDFCON - 2017
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 Brian’s 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 Dot ISP Pinout
Amazon Echo Dot

- 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 Show

- New June 2017
  - Thank you Amazon for the spare
- Disassembly
  - Well documented
  - 1 new in the box for pinout
  - 1 used for testing 3.5 months

https://www.ifixit.com/Teardown/Amazon+Echo+Show+Teardown/94625
Amazon Echo Show

• Components
  – 8GB NAND Embedded Flash Drive
    Sandisk SDIN9D92-8G

• Challenge
  – No Data Sheet
  – Future Pinout
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 mobile application

• View your Echo devices (Dot, Echo Tap, Echo Show, etc)

• Control what’s playing on an Echo device

• Message and call other Amazon Alexa application users
  – And Echo device owners
Alexa mobile application

- Conversations
  - Stephanie Randofferson
    - OSDFCon is coming up in a week!!
  - Juliet Seeker
    - Now you can instantly start a voice or video c…
  - Peacock Leprechaun
    - Hey hey hey PL
  - Brian Moran
    - Whoohoo
    - Now you can communicate with your friends and family.
    - Try saying:
      - “Alexa, send a message”
      - “Alexa, make a call”
      - “Alexa, play my messages”

- Home
  - How many episodes of Salvation are there?
    - Salvation has 13 episodes.
    - SEARCH BING FOR "HOW MANY EPISODES OF SALVATION ARE THERE"
  - What time is sunset today?
    - Sunset is at 6:52 p.m.
    - SEARCH BING FOR "WHAT TIME IS SUNSET TODAY"
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
Alexa mobile application

• But what if you only have a logical acquisition?
• Good news!! You can navigate to the path “com.amazon.avod.thirdpartyclient\db\map_data_storage.db”
• Search for the “amzn1.account” string to find the customer ID
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 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-kjxtaYjqetm_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:

  “https://alexa-mobile-service-na-preview.amazon.com/users/amzn1.comms.id.person.amzn1~amzn1.account.AEAM5TQ27DKFM7VJXYY3SFBDCAI
  Q/conversations/amzn1.comms.messaging.id.conversation~KEnAPYR-
kjxtaYjqqtm_lhU8OQ/messages?count=100&sort=asc”
Alexa Calling & Messaging

```json
{"conversationId":"amzn1.comms.messaging.id.conversation~KEnAPYR-kjxtaYjvqetm_lhU8OQ","messages":
["conversationId":"amzn1.comms.messaging.id.conversation~KEnAPYR-kjxtaYjvqetm_lhU8OQ","messageId":1,"sequenceId":1,"time":"2017-05-11T18:38:52.654Z","sender":"amzn1.comms.id.person.amzn1~amzn1.account.AEAM5TQ27DKFM7VJXYY3SFBDCAIQ","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-kjxtaYjvqetm_lhU8OQ","messageId":2,"sequenceId":2,"time":"2017-05-11T18:39:19.024Z","sender":"amzn1.comms.id.person.amzn1~amzn1.account.AEAM5TQ27DKFM7VJXYY3SFBDCAIQ","type":"message/text","payload":{"text":"Hello"}},
{"conversationId":"amzn1.comms.messaging.id.conversation~KEnAPYR-kjxtaYjvqetm_lhU8OQ","messageId":3,"sequenceId":3,"time":"2017-05-19T03:59:32.315Z","sender":"amzn1.comms.id.person.amzn1~amzn1.account.AEAM5TQ27DKFM7VJXYY3SFBDCAIQ","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
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
  – A0O6WSCOZPW80
    • Device Account ID

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

```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 Activities
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” 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)
• Just like Amazon, new devices keep coming
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 Autopsy 4.4.1
kasa mobile application (cont.)

Well that is a convenient name!

Data viewed in Autopsy 4.4.1
iot.1.db

- Contains at least 8 tables, with straightforward naming conventions

- For example, “accounts” contains account information

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

Data viewed in SQLiteSpy 1.9.6
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!
**iot.1.db – “devices”**

Data viewed in SQLiteSpy 1.9.6
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_v2”

• Contains account ID, created time, last sync time, and geographic coordinates of where the user account is
iot.1.db – “locations_v2”

• 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”
Addressing kasa Security Concerns

• TP-Link was responsive and had an application update out by June 23rd (DFIRSummit presentation date)
  – 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

• 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.)

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

3:32 PM - 11 May 2017

@brianjmoran

Tweet your reply

Derek Abdine @dabdine · May 11
Replying to @brianjmoran
@brianjmoran they've given a heads-up to the relevant team. can you send details to security@amazon.com?
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.)

• 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 Wi-Fi profiles from your account
  – Watch your Echo while you do this. Blinking lights!

• 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
  – Hard to fix something when, it works the way that it should, but can also be used for malicious purposes

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

• The Amazon security team has been fantastic to work with!
Plugins. For Autopsy. To Parse Data

*Because this is OSDFCon after all!!*

- Thanks to the hard work of Mark McKinnon, we were able to make a plugin called “Amazon Echosystem Parser” available for Autopsy.

- Download from:
  https://github.com/markmckinnon/Autopsy-Plugins/tree/master/Amazon_Echosystem_Parser
Plugins. For Autopsy. To Parse Data (cont.)

- Currently parses Alexa and Kasa related databases
  - Presents data under “Extracted Content”
The Road Ahead

• Add iOS device testing
• Enhance scripts, plugins, and applications to parse the SQLite and JSON data
• 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 ...
YET
Questions?

Contact Us!

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

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