An Analysis of Amazon Echo’s Network Behavior

Jan Janak
with T. Tseng, A. Isaacs, H. Schulzrinne

Dept. of Computer Science
Columbia University

IEEE Globecom2021, Madrid, Spain, December 10, 2021
Talk Outline

1. Introduction
2. Methodology & Experimental Setup
3. Network Behavior & Protocols
4. Discussion
5. Summary and Q&A
Introduction

- More than 20 million Amazon Echo units sold since 2015
- Deployed in home, school classrooms, some hotels
- What do we know about its network behavior?
  - How secure is the Wi-Fi pairing process?
  - How secure is the connection to Amazon Cloud?
  - Are the calls made from an Amazon Echo encrypted?
Methodology

1. Put a man-in-the-middle (MITM) TLS proxy between Echo and internet
2. Make the Echo accept the proxy’s CA certificate
3. Record, decrypt, analyze communication between Echo and Amazon cloud
4. Analyze Wi-Fi pairing on rooted Android device
Hardware Setup

- 1st gen. Amazon Echo with exposed pins
- External SD card with Amazon Echo OS image
- Laptop with USB-UART converter
- Laboratory power supply
Out of the Box Experience (OOBE)

Protocol executed between Echo, smartphone/web app, and Amazon cloud

1. Provision Wi-Fi network name and password into the Echo
2. Associate the device with an Amazon user account
3. Performed after factory reset or when Wi-Fi is unusable

*Pairing takes place over open temporary Wi-Fi network created by Echo*
OOBE Key Features

● Echo supports Wi-Fi AP and client roles at the same time
● Echo provides internet connectivity to smartphone during pairing
  ○ Necessary to associate Echo with user’s Amazon user account
● Wi-Fi credential provisioning:
  ○ Password encrypted (AES-256 in CBC mode) with random secret
  ○ Random secret encrypted with Echo’s public key (from self-signed X.509 certificate)
  ○ Vulnerable to MITM
● Amazon user account registration:
  ○ Link code: five alphanumeric characters obtained from Amazon cloud
  ○ Based on a secret string set during manufacturing
  ○ Associated with user account via HTTP cookie (must be logged in to Amazon in browser)
OOBE Overview of Operation

System architecture diagram

OOBE message flow diagram
Alexa Voice Service (AVS)

- Speech recognition, natural language understanding, text to speech
- Public API provided by Amazon cloud (available to third-party developers)
- Echo maintains a persistent SPDY connection to AVS
- **NegotiationCommand** authenticates the device
- Authenticated with a secret key obtained during device pairing
- Rest similar to public AVS
Alexa Drop-in Calling

- Place calls to Alexa-enabled devices, phone numbers, or Skype
- Voice activated:
  - “Alexa drop in on …”
  - “Alexa call …”
  - “Alexa answer”
- Two modalities: regular call, intercom
- Amazon Echo answers intercom calls automatically
Alexa Call Flow Diagram

- Based on the Session Initiation Protocol (RFC 3261)
- Audio encoded with Opus codec
- Encrypted with sRTP (AES-256)
- UA remotely managed by Alexa
- Calls individually authorized by Alexa cloud service
Alexa Drop-in Calling System Architecture

- Calls are end-to-end encrypted
- Amazon cloud has access to the key
- Calls within single LAN (home) remain local
- Calls between LANs (homes) relayed through Amazon cloud
Discussion

- Our MITM approach is only effective with 1st generation Amazon Echo
- However, the described protocols are compatible with newer devices
- OOBE vulnerable to eavesdropping and MITM
  - Hijacking of de-registered Echo prevented by pre-registration during purchase
- Calls are end-to-end encrypted authorized in all scenarios
  - Per-INVITE authorization prevents intercom misuse
  - Passive eavesdropping won’t reveal audio
  - Amazon cloud can force calls through a relay and decrypt audio

The 1st generation Amazon Echo is a well designed device with respect to network behavior
Summary

1. Made 1st generation Amazon Echo vulnerable to MITM attacks

2. Launched a MITM attack, recorded, decrypted, and analyzed:
   a. Out-of-box-experience (OOBE) Wi-Fi pairing protocol
   b. Alexa Voice Service (AVS) protocol
   c. Alexa Drop-in Calling protocols

3. Found OOBE vulnerable to eavesdropping

4. Found drop-in calling end-to-end encrypted and secure

Contact: janakj@cs.columbia.edu