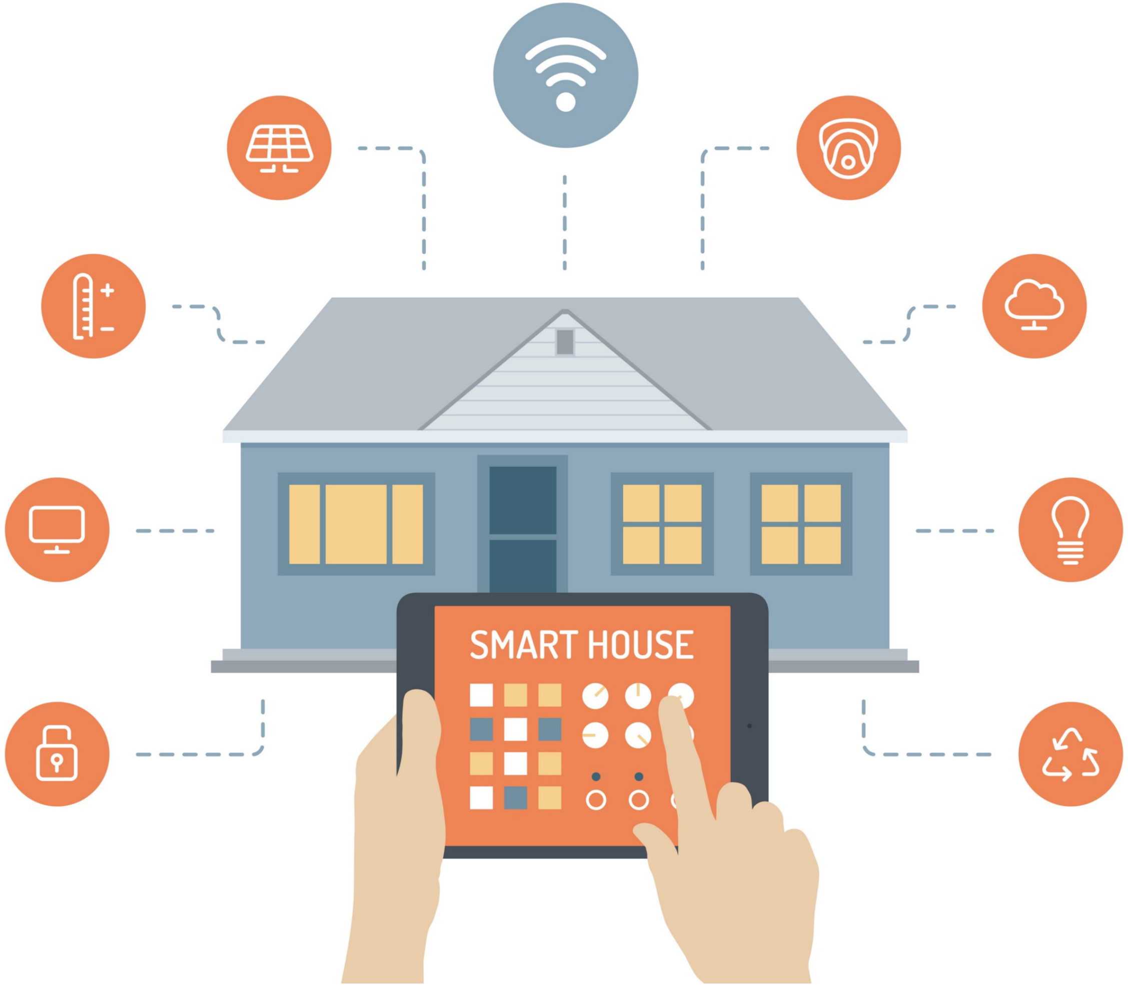
SoK: Security Evaluation of Home-based IoT Deployments

Omar Alrawi, Chaz Lever,
Fabian Monrose, Manos Antonakakis



Alexa, unlock the front door.

threatpost

Extinguishing the IoT Insecurity Dumpster Fi

Kno

IoT sec
here's w

OH CVE-2016-7407?
I SHOULD UPGRADE
DROPBEAR SSH SERVER
imgflip.com

Prior Work

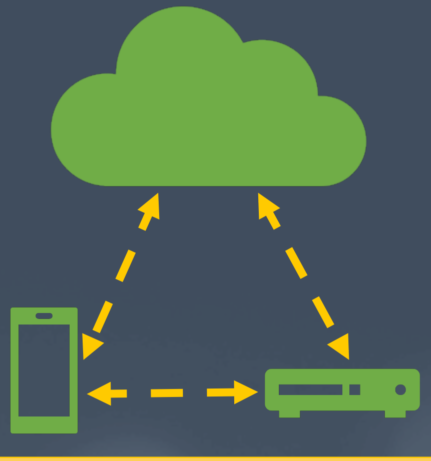
- Security Analysis of Emerging Smart Home Applications
- DolphinAttack: Inaudible Voice Commands
- Soteria: Automated IoT Safety and Security Analysis
- Skill Squatting Attacks on Amazon Alexa
- Rethinking Access Control and Authentication for the Home Internet of Things

Wouldn’t be nice to know

- Cloud endpoints
- Exposed services
- Mobile App
- Network
- Consumer report evaluation?

CR Consumer Reports

Overview of Prior Work



Studied Components

Devices

Cloud integration services

Network (by association)

Mitigations

Patching bugs

Vendor responsibility

Unexplored Directions

Mobile app

Cloud services

Network discovery protocols

User control and visibility

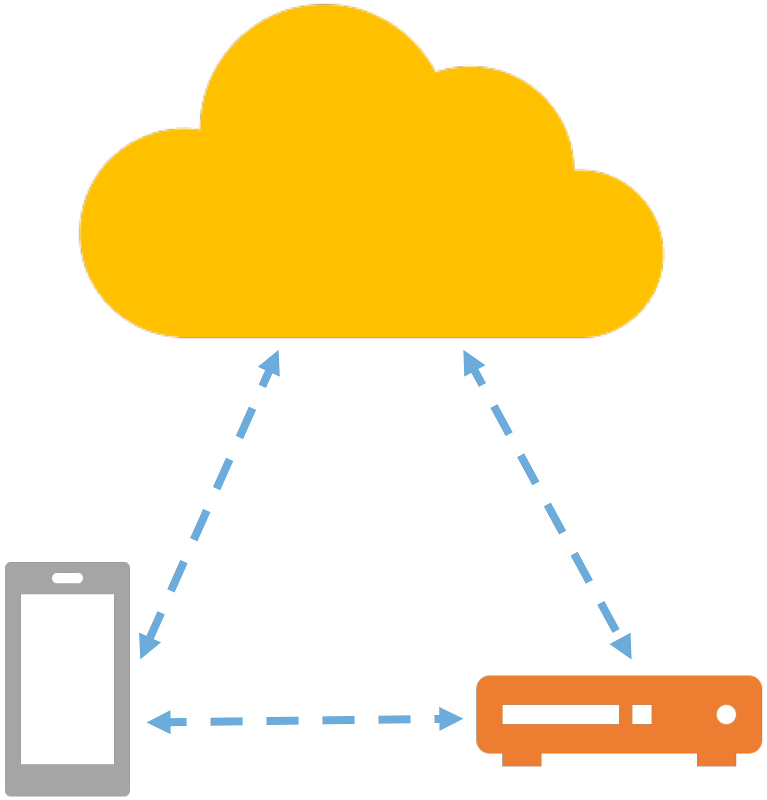
IoT Components

Device

Mobile App

Cloud Endpoints

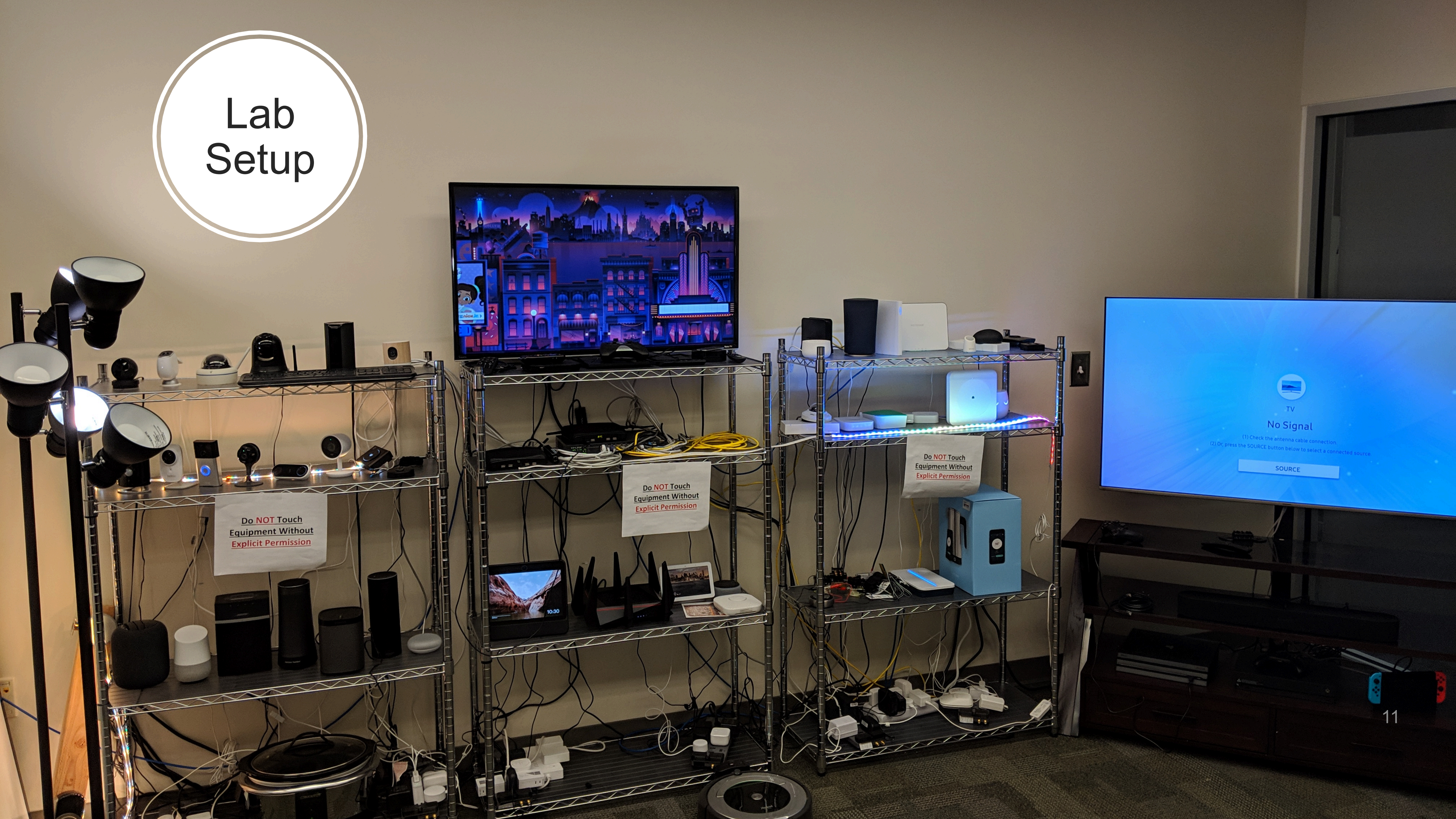
Network



Evaluating Off The Shelf Devices

- Evaluation of IoT devices should be:
  - Objective
  - Transparent
  - Measurable
  - Reproducible
- Device Representation
  - Media devices vs appliances
- Easy to understand
  - Consumer oriented

Lab Setup


Do NOT Touch Equipment Without Explicit Permission
Do NOT Touch Equipment Without Explicit Permission
Do NOT Touch Equipment Without Explicit Permission
TV
No Signal
(1) Check the antenna cable connection.
(2) Or, press the SOURCE button below to select a connected source.
SOURCE
10:30

IoT Lab Evaluation Device

- Internet pairing
- Configuration
- Updateable
- Exposed services
  - Vulnerable Services

UPnP services RCE vulnerability
CVE-2012-5958-65
Dropbear SSH RCE vulnerability
CVE-2013-4863

IoT Lab Evaluation Cloud Backends

- Types of cloud backends
  - 1st, 3rd, or hybrid
- TLS/SSL
  - Self-signed
  - Name mismatch
  - Vulnerable TLS/SSL version
- Insecure protocols
- Vulnerable software
  - Services

- **12 different backends, 1st Party**
- **Supports SSL v2/v3**
- **CVE-2013-4810 – RCE JBoss Server**

IoT Lab Evaluation Mobile App

- Permissions
  - Requested unused
- Programming errors
  - Incorrect use of crypto
- Hardcoded secrets
  - API keys for cloud services

- **Hardcoded Crypto key**
  - **uLi4/f4+Pb39.T19**
- **UMENG_MESSAGE_SECRET: …**

Simple Setup

Connect to a 2.4 GHz Wi-Fi network. No hub or bridge required.

IoT Lab Evaluation Network

- Protocols in use
  - Insecure Protocols
  - Custom Protocols
- Encryption between
  - Device to Cloud
  - Device to Mobile App
  - Mobile App to Cloud
- MITM Attack on
  - Device to Cloud
  - Device to Mobile App
  - Mobile App to Cloud

- **Partial Encryption Across the Internet**
- **No Encryption on the LAN**

Scoring The Components

Scorecard system

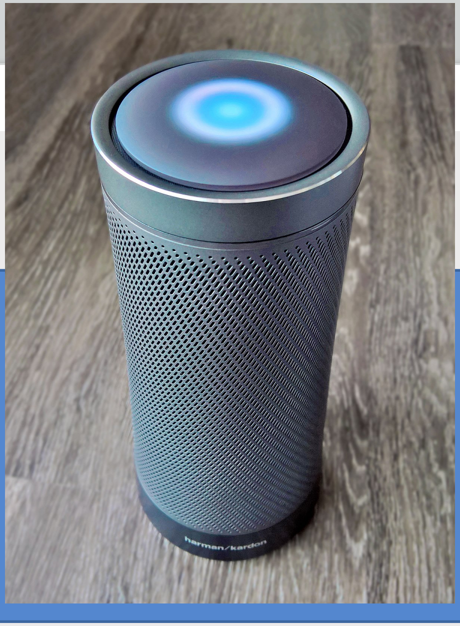
Rating components

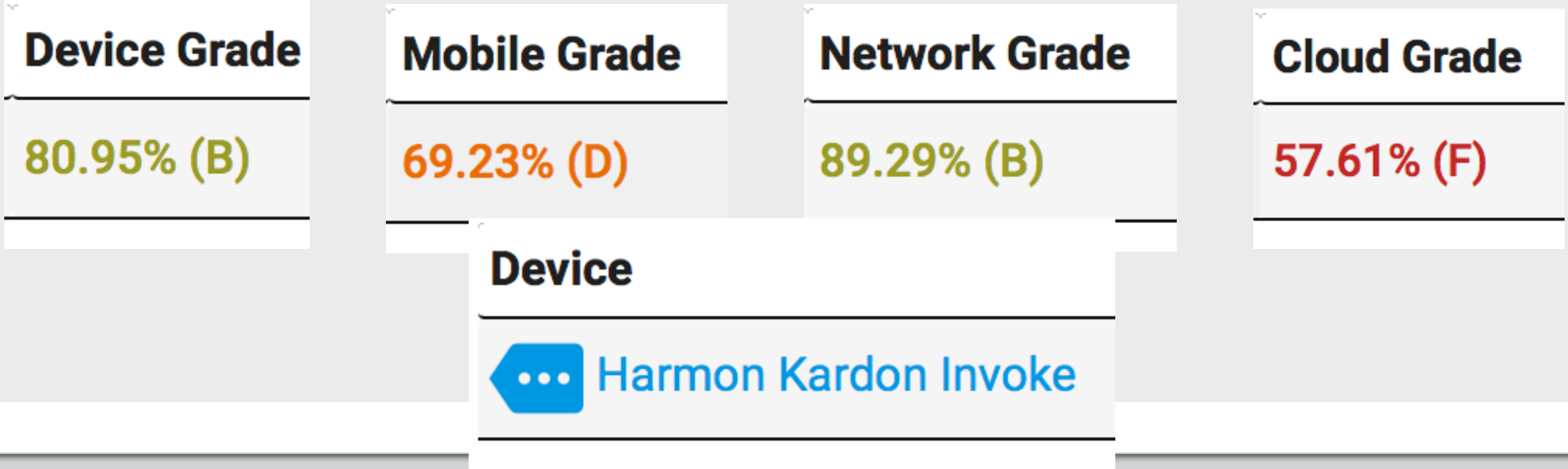
Independent scoring

Modular

Documented

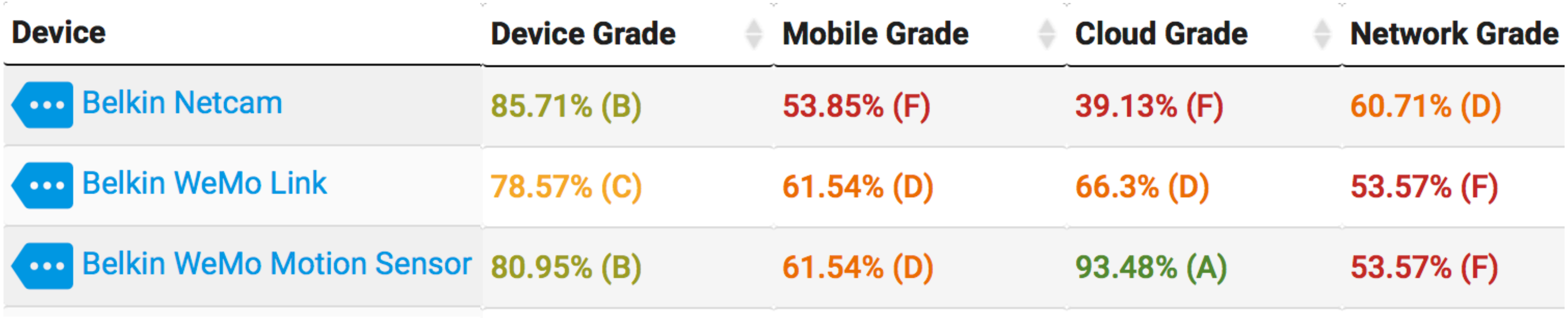
☑ Excellent
□ Very good
□ Good
□ Average
□ Poor



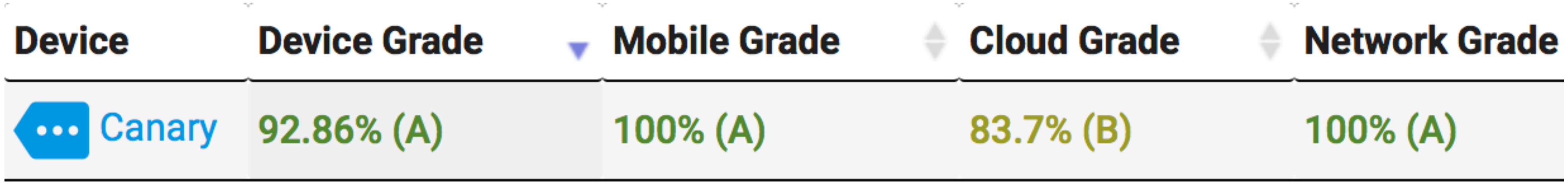


Device Grade	Mobile Grade	Network Grade	Cloud Grade
80.95% (B)	69.23% (D)	89.29% (B)	57.61% (F)

Device
••• Harmon Kardon Invoke

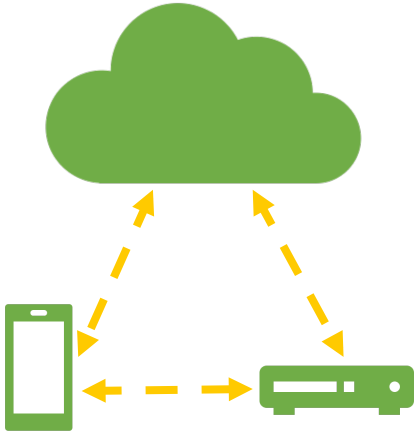


Device	Device Grade	Mobile Grade	Cloud Grade	Network Grade
Belkin Netcam	85.71% (B)	53.85% (F)	39.13% (F)	60.71% (D)
Belkin WeMo Link	78.57% (C)	61.54% (D)	66.3% (D)	53.57% (F)
Belkin WeMo Motion Sensor	80.95% (B)	61.54% (D)	93.48% (A)	53.57% (F)



Device	Device Grade	Mobile Grade	Cloud Grade	Network Grade
Canary	92.86% (A)	100% (A)	83.7% (B)	100% (A)

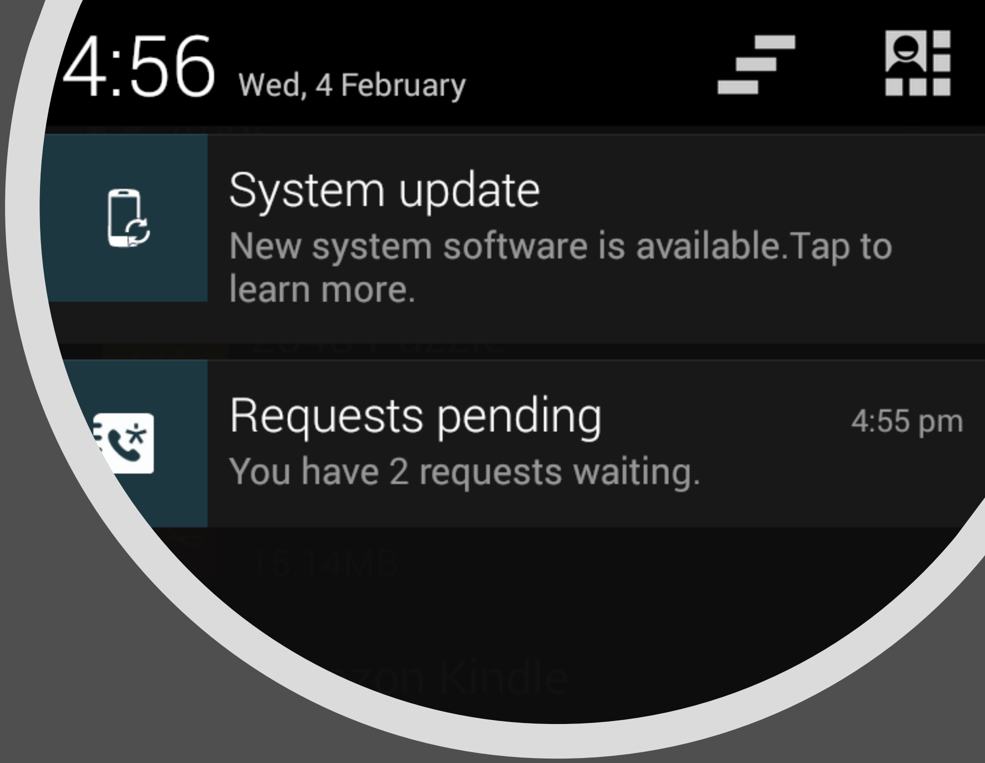
Evaluation Takeaways



- Cloud managed
- Auto update
- Encrypted local traffic with authenticated services

What's Next?

- Longitudinal analysis
  - Do updates improve the Things?
- Accurate representation
  - Inducing device activities



4:56 Wed, 4 February

System update

New system software is available.Tap to learn more.

Requests pending 4:55 pm

You have 2 requests waiting.

How Can You Access/Contribute?

- Evaluation data is public
- Feel free to reach out:
  - Request specific device evaluation
  - Sponsor devices for evaluation
  - Additional questions
- Download our data
  - https://YourThings.info
- Contact email:
  - *contact@YourThings.info*