SoK: Security Evaluation of Home-based IoT Deployments

Omar Alrawi, Chaz Lever,
Fabian Monrose, Manos Antonakakis

Alexa, unlock the front door.

Internet of Things

PARTNER CONTENT JASON BLOOMBERG, INTELLYX.

7 REASONS WHY THE INTERNET OF THINGS IS DOOMED

threatpost

SUBSCRIBE

Extinguishing the IoT Insecurity Dumpster Fire

T OF THINGS IS

threatpost

Extinguishing the IoT Insecurity Dumpster Fire

SUBSCRIBE

T OF THINGS IS

KnowTechie

IoT security is a nightmare, here's what you need to know

threatpost

Extinguishing the IoT Insecurity Dumpster Fire

SUBSCRIBE

T OF THINGS IS

KnowTechie

IoT security is a nightmare, here's what you need to know

threatpost

Extinguishing the IoT Insecurity Dumpster Fire

SUBSCRIBE

T OF THINGS IS

Kno

IoT sec e,
here's w now

threatpost

Extinguishing the IoT Insecurity Dumpster Fire

Kno

IoT sec re, here's w now

threatpost

Extinguishing the IoT Insecurity Dumpster Fi

SCRIBE

Kno

IoT sec

here's w


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

Prior Work

Prior Work

- Security Analysis of Emerging Smart Home Applications

Prior Work

- Security Analysis of Emerging Smart Home Applications
- DolphinAttack: Inaudible Voice Commands

Prior Work

- Security Analysis of Emerging Smart Home Applications
- DolphinAttack: Inaudible Voice Commands
- Soteria: Automated IoT Safety and Security Analysis

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

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

Wouldn’t be nice to know

- Cloud endpoints

Wouldn’t be nice to know

- Cloud endpoints
- Exposed services

Wouldn’t be nice to know

- Cloud endpoints
- Exposed services
- Mobile App

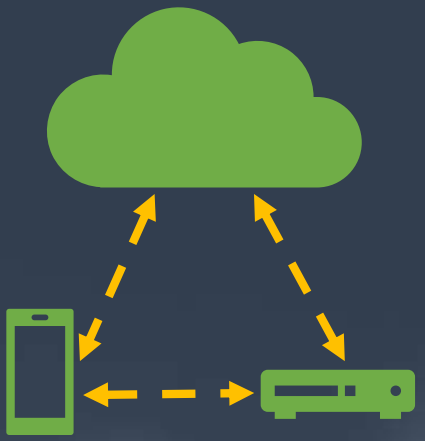
Wouldn’t be nice to know

- Cloud endpoints
- Exposed services
- Mobile App
- Network

Wouldn’t be nice to know

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

Overview of Prior Work



Studied Components	Mitigations	Unexplored Directions
Devices Cloud integration services Network (by association)	Patching bugs Vendor responsibility	Mobile app Cloud services Network discovery protocols User control and visibility

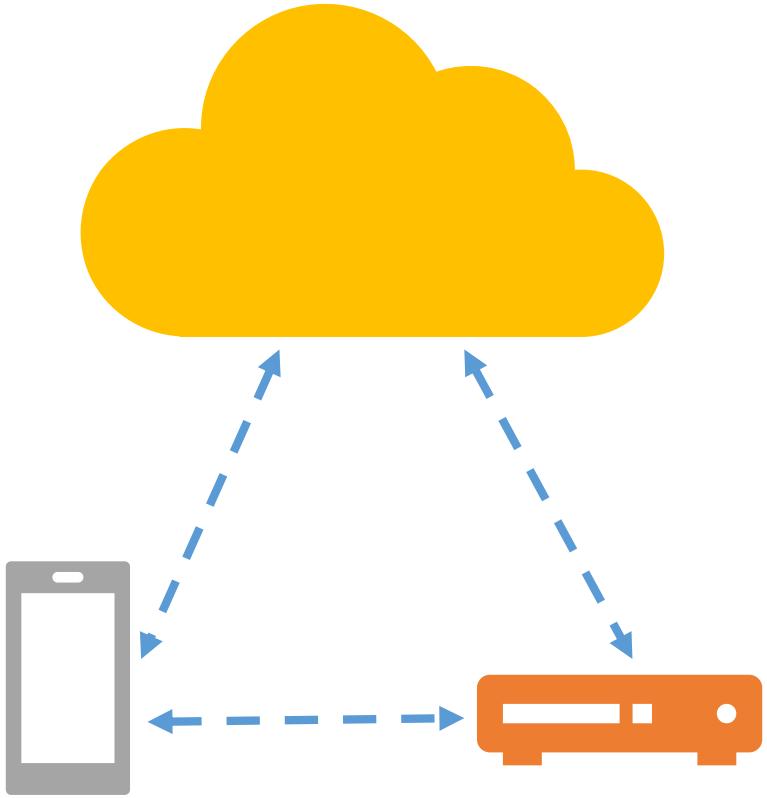
IoT Components

Device

Mobile App

Cloud Endpoints

Network



Evaluating Off The Shelf Devices

Evaluating Off The Shelf Devices

- Evaluation of IoT devices should be:
  - Objective
  - Transparent
  - Measurable
  - Reproducible

Evaluating Off The Shelf Devices

- Evaluation of IoT devices should be:
  - Objective
  - Transparent
  - Measurable
  - Reproducible
- Device Representation
  - Media devices vs appliances

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
No Signal

IoT Lab Evaluation Device

IoT Lab Evaluation Device

- Internet pairing

IoT Lab Evaluation Device

- Internet pairing
- Configuration

IoT Lab Evaluation Device

- Internet pairing
- Configuration
- Updateable

IoT Lab Evaluation Device

- Internet pairing
- Configuration
- Updateable
- Exposed services

IoT Lab Evaluation Device

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

IoT Lab Evaluation Device

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

IoT Lab Evaluation Cloud Backends

IoT Lab Evaluation Cloud Backends

- Types of cloud backends
  - 1st, 3rd, or hybrid

IoT Lab Evaluation Cloud Backends

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

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

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

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

IoT Lab Evaluation Mobile App

- Permissions
  - Requested unused

IoT Lab Evaluation Mobile App

- Permissions
  - Requested unused
- Programming errors
  - Incorrect use of crypto

IoT Lab Evaluation Mobile App

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

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: …**

IoT Lab Evaluation Network

IoT Lab Evaluation Network

- Protocols in use
  - Insecure Protocols
  - Custom Protocols

IoT Lab Evaluation Network

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

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

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

Scoring The Components

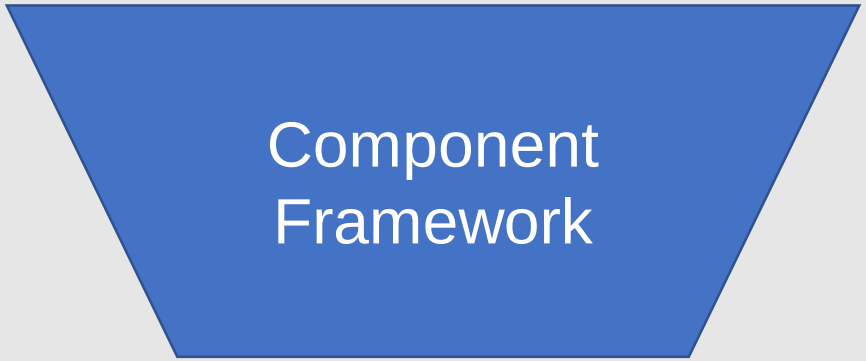
Scorecard system

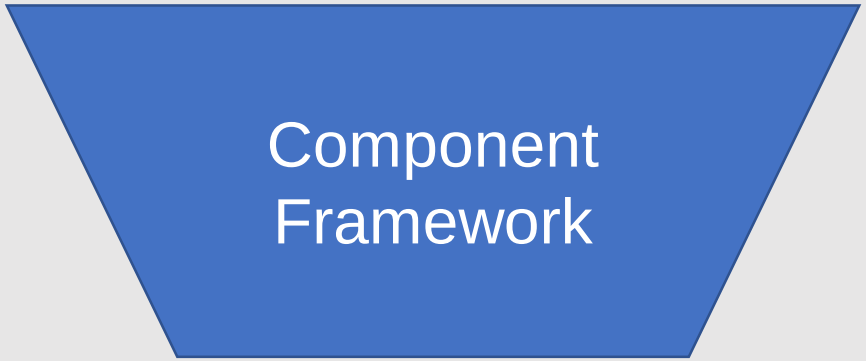
Rating components

Independent scoring

Modular

Documented


Component
Framework


Component
Framework

Component Framework

Device Grade
80.95% (B)

Component Framework

Device Grade
80.95% (B)

Component Framework

Device Grade
80.95% (B)

Component Framework

Device Grade
80.95% (B)

Mobile Grade
69.23% (D)

Component Framework

Device Grade
80.95% (B)

Mobile Grade
69.23% (D)

Component Framework

Device Grade
80.95% (B)

Mobile Grade
69.23% (D)

Component Framework

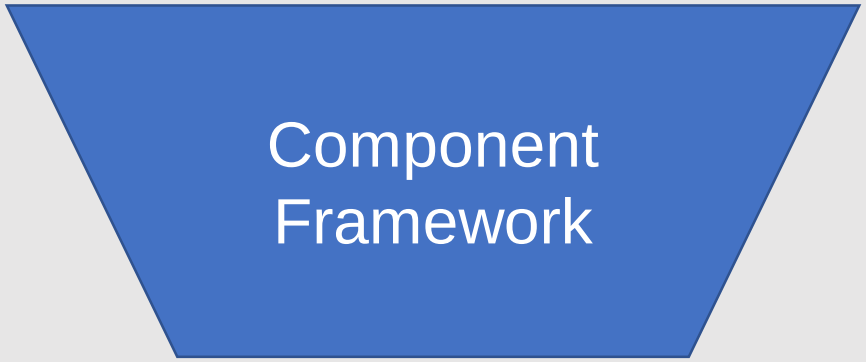
Device Grade	Mobile Grade	Network Grade
80.95% (B)	69.23% (D)	89.29% (B)

Component Framework

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

Component Framework

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



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

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

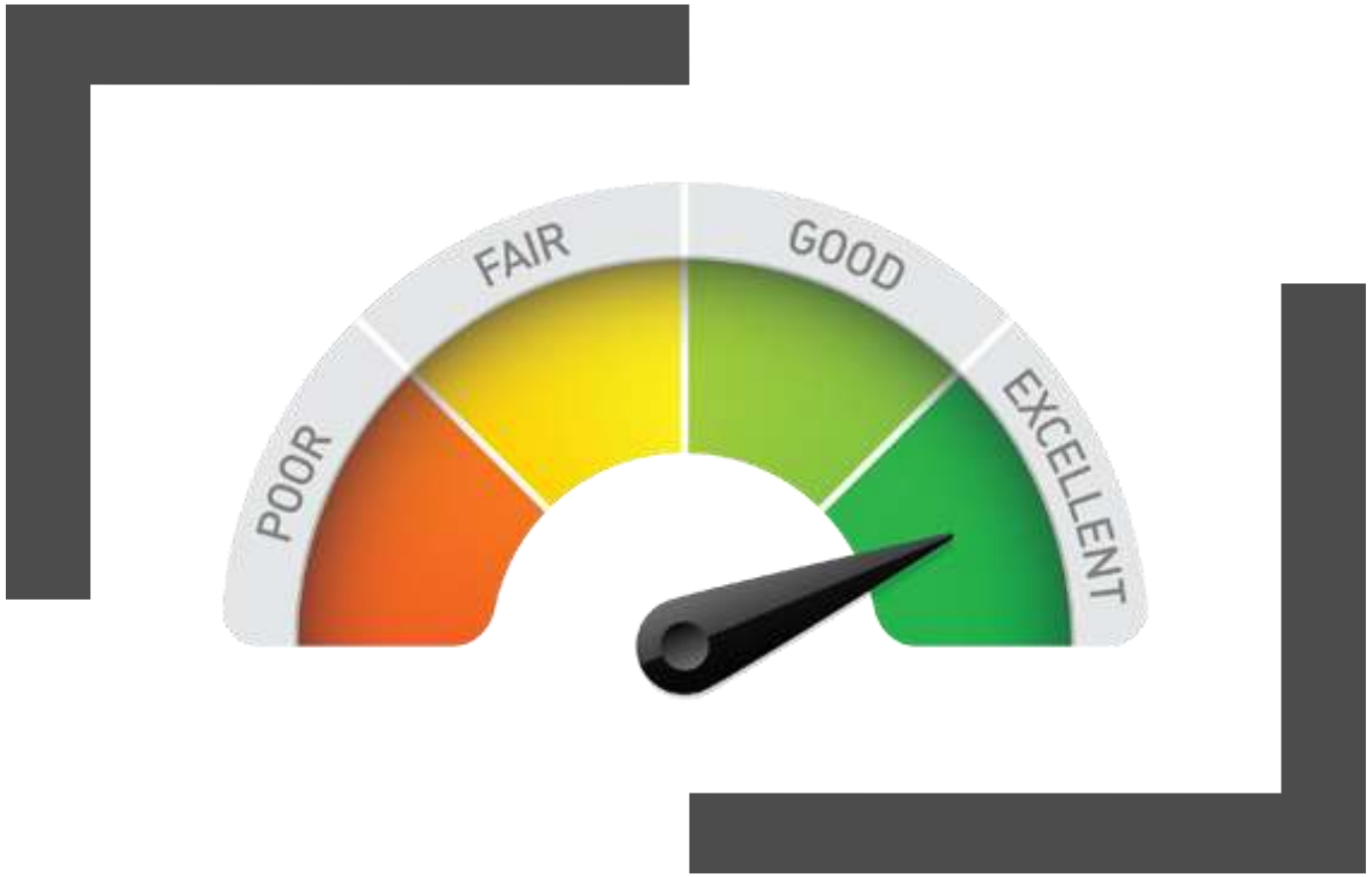
Device
Harmon Kardon Invoke

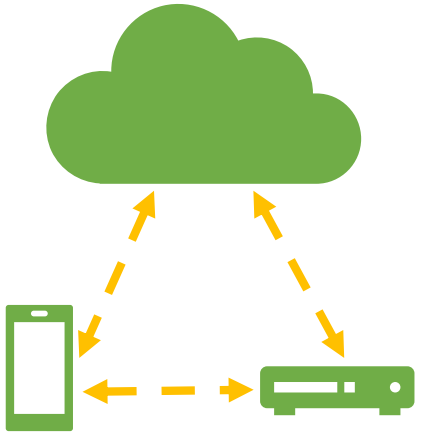
Device Grade	Mobile Grade	Cloud Grade	Network Grade
85.71% (B)	53.85% (F)	39.13% (F)	60.71% (D)
78.57% (C)	61.54% (D)	66.3% (D)	53.57% (F)
80.95% (B)	61.54% (D)	93.48% (A)	53.57% (F)

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)

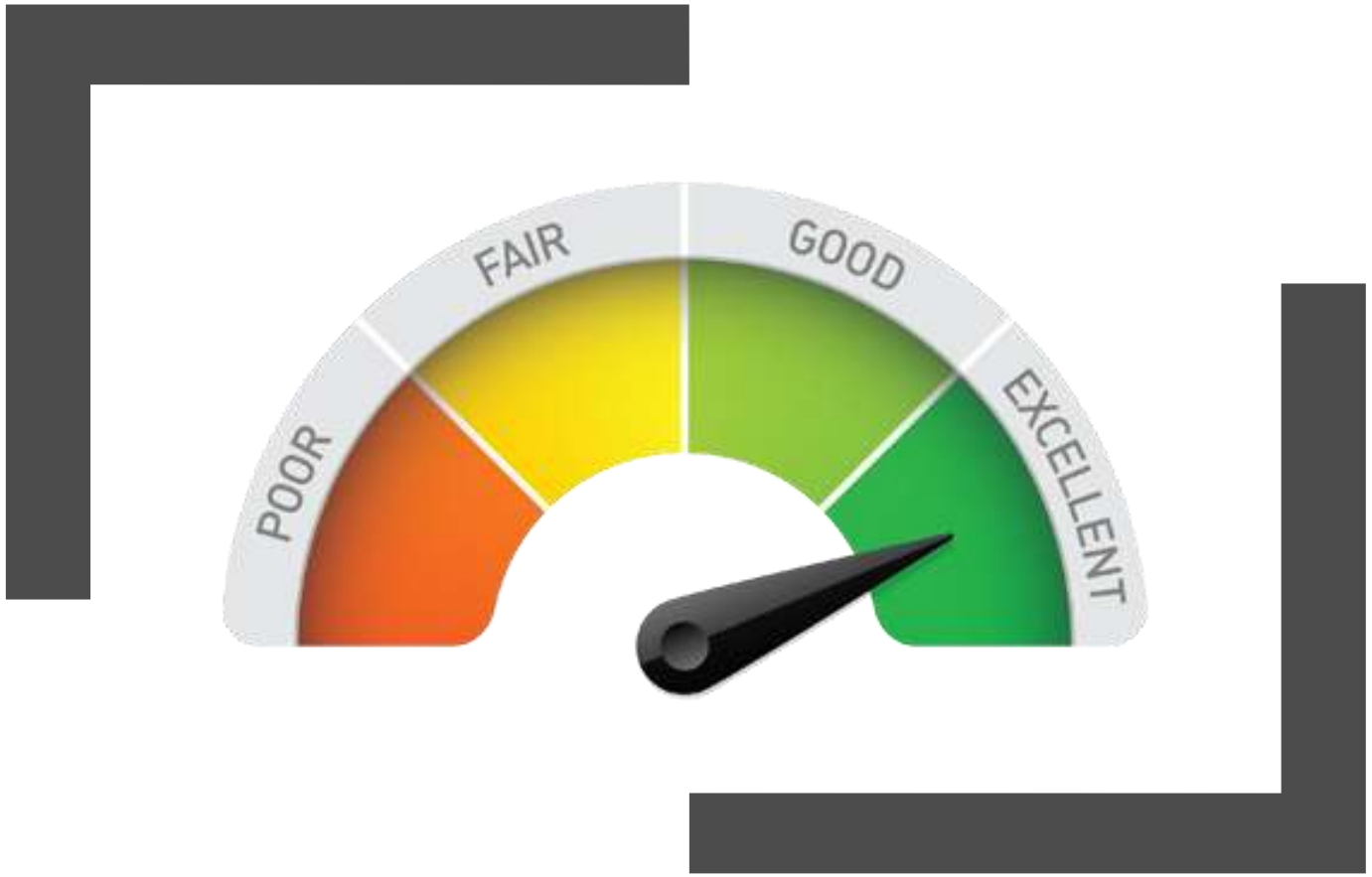
Device	Device Grade	Mobile Grade	Cloud Grade	Network Grade
Canary	92.86% (A)	100% (A)	83.7% (B)	100% (A)

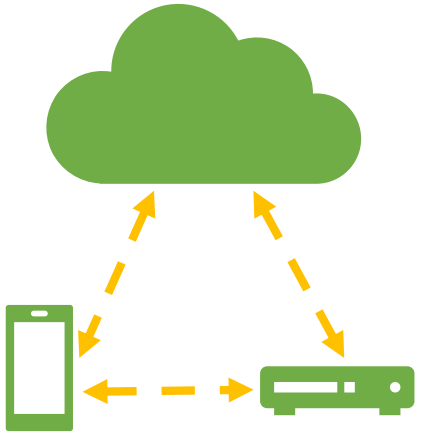
Evaluation Takeaways





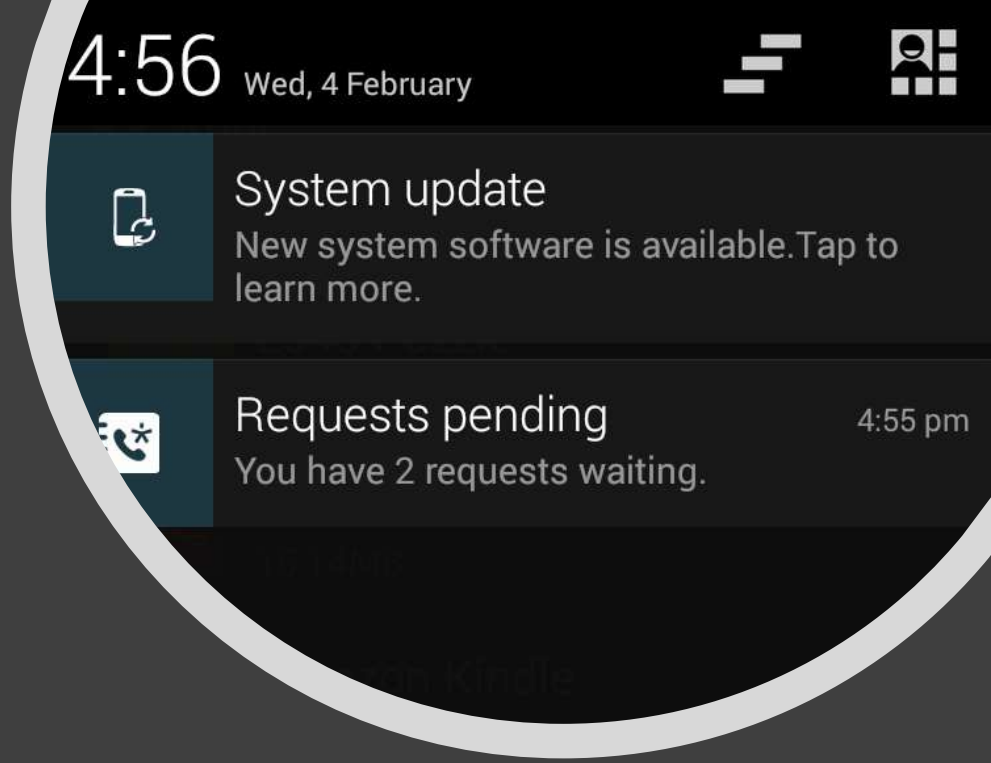
Evaluation Takeaways





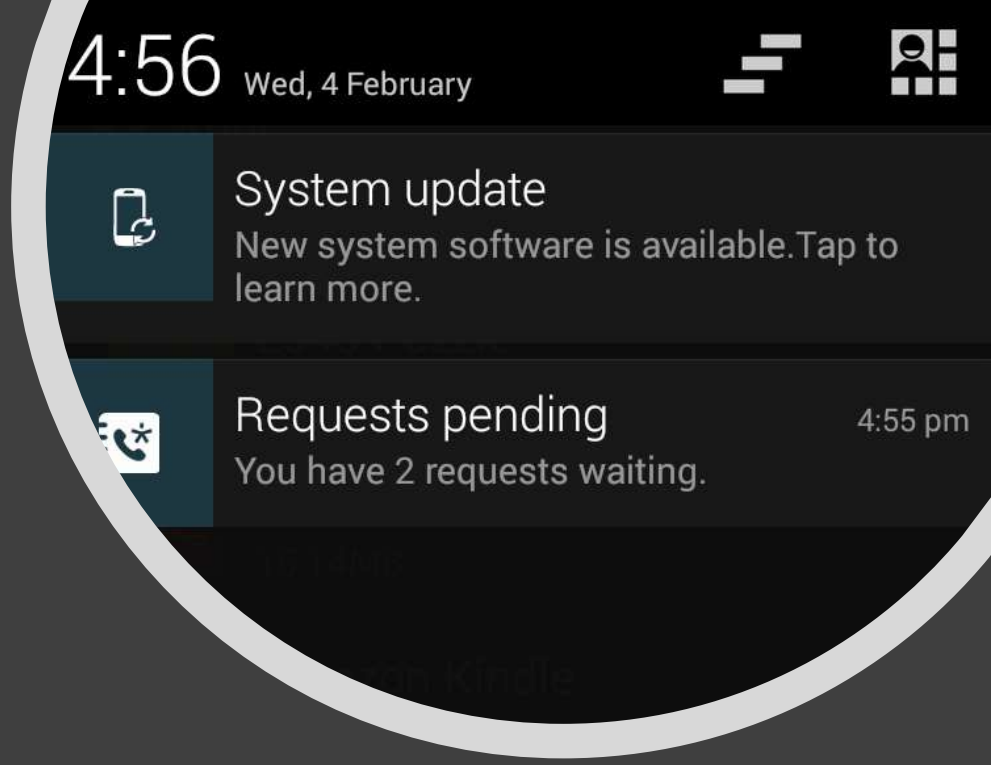
- Cloud managed
- Auto update
- Encrypted local traffic with authenticated services

What's Next?


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.

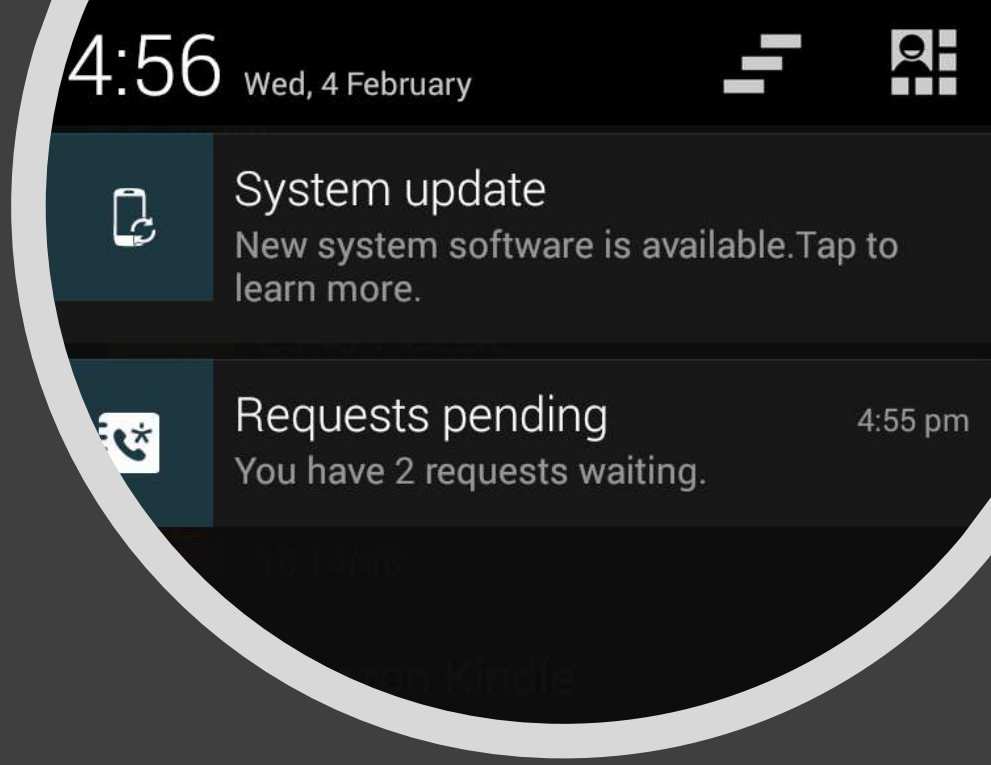
What's Next?

- Longitudinal analysis
  - Do updates improve the Things?



What's Next?

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



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*