Omar Alrawi

Security Evaluation of Home-based IoT Deployments

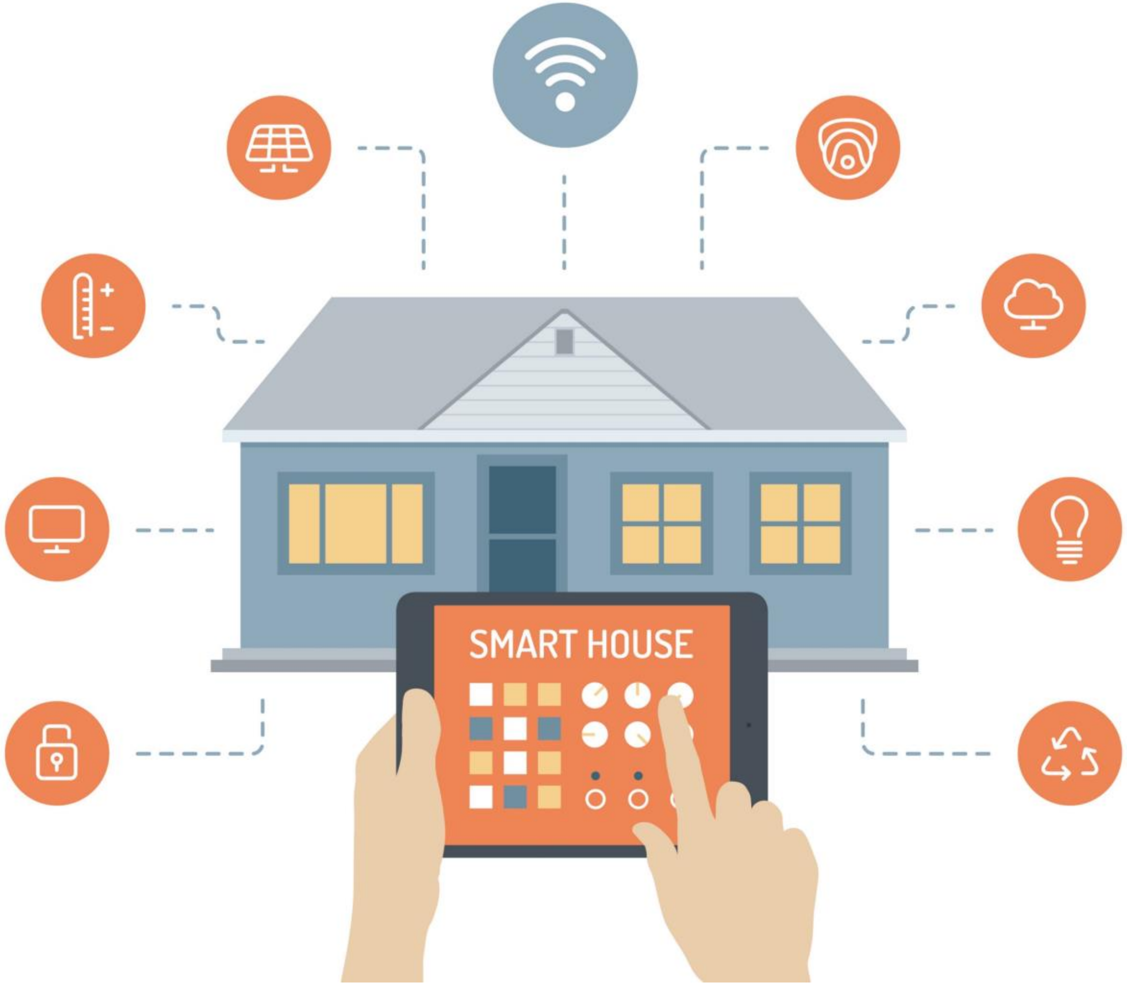
Georgia Tech

CREATING THE NEXT

About Us

- Astrolavos Research Lab at Georgia Tech
- We specialize in Network Security Measurements
- Work is presented on behalf of my team
  - **Omar Alrawi – PhD Student (me)**
  - Chaz Lever – Research Scientist
  - Manos Antonakakis – PI and my advisor
  - Fabian Monrose – Collaborator PI from UNC Chapel Hill

This work looks at commodity smart home IoT deployments



Presentation Outline

Motivation

- **Why is the evaluation of IoT deployment important?**

Past Research

- **Components of an IoT deployment**
- **Attacks, mitigations, and stakeholders**

Methods

- **How we go about objectively evaluating heterogeneous devices**

Findings

- **What we found applying our methodology to 45 devices.**

Moving Forward

- **https://YourThings.info portal and publicly available evaluation data**
- **Collaboration/partnership with industry**

Motivation

Market demand for home IoT devices is sky rocketing

Some vendors lack expertise

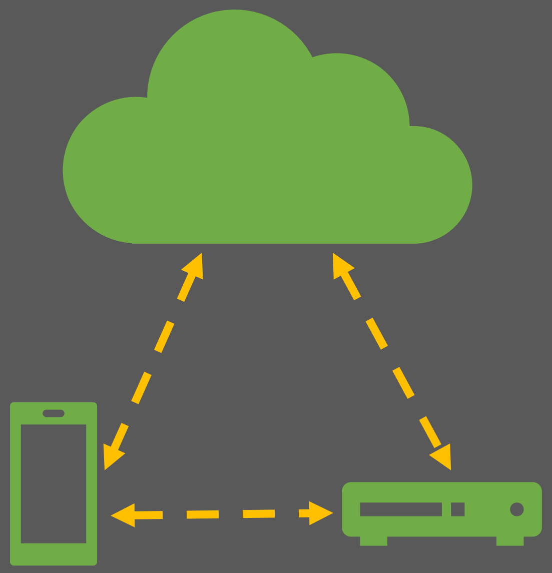
Building secure IoT is hard (distributed systems)

Attack surface is large
(several componenets)

Example of attacks: DynDNS

IoT Components

- Device
- Mobile App
- Cloud Endpoints
- Network



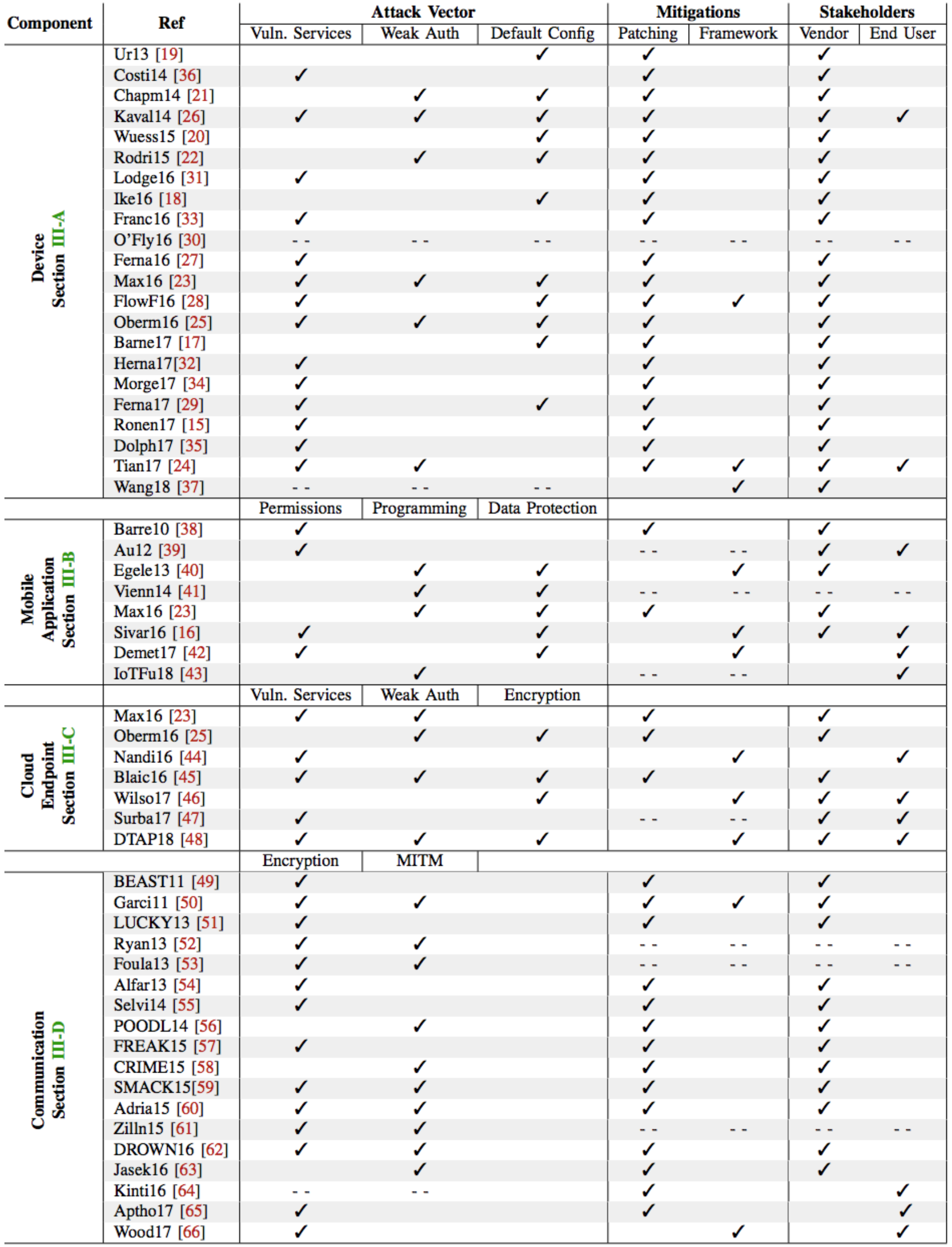
Past and Current Research

Past Research

- Divided research based on
  - Device, Cloud, Mobile App, and Network
- Cross compare against
  - Attacks, Mitigations, and Stakeholders
- Answering the following:
  - What is the focus of the community?
  - What attack surfaces are studied?
  - What defenses are proposed?
  - Who is responsible for fixes?

Research Directions

- Focus in **Device** and **Network** security
- Attacks are **Device** oriented, very few in **Mobile App** and **Cloud**
- Defenses propose **Patching** and few propose **Frameworks**
- Responsible party is the **Vendor** in most cases



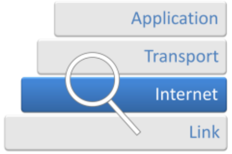
Component	Ref	Attack Vector			Mitigations		Stakeholders	
		Vuln. Services	Weak Auth	Default Config	Patching	Framework	Vendor	End User
Device Section III-A	Ur13 [19]			✓	✓		✓	
	Costi14 [36]	✓			✓		✓	
	Chapm14 [21]		✓	✓	✓		✓	
	Kaval14 [26]	✓	✓	✓	✓		✓	✓
	Wuess15 [20]			✓	✓		✓	
	Rodri15 [22]		✓	✓	✓		✓	
	Lodge16 [31]	✓			✓		✓	
	Ike16 [18]			✓	✓		✓	
	Franc16 [33]	✓			✓		✓	
	O'Fly16 [30]	- -	- -	- -	- -	- -	- -	- -
	Ferna16 [27]	✓			✓		✓	
	Max16 [23]	✓	✓	✓	✓		✓	
	FlowF16 [28]	✓		✓	✓	✓	✓	
	Oberm16 [25]	✓	✓	✓	✓		✓	
	Barne17 [17]			✓	✓		✓	
	Herna17[32]	✓			✓		✓	
	Morge17 [34]	✓			✓		✓	
	Ferna17 [29]	✓		✓	✓		✓	
	Ronen17 [15]	✓			✓		✓	
	Dolph17 [35]	✓			✓		✓	
	Tian17 [24]	✓	✓		✓	✓	✓	✓
	Wang18 [37]	- -	- -	- -		✓	✓	
		Permissions	Programming	Data Protection				
Mobile Application Section III-B	Barre10 [38]	✓			✓		✓	
	Au12 [39]	✓			- -	- -	✓	✓
	Egele13 [40]		✓	✓		✓	✓	
	Vienn14 [41]		✓	✓	- -	- -	- -	- -
	Max16 [23]		✓	✓	✓		✓	
	Sivar16 [16]	✓		✓		✓	✓	✓
	Demet17 [42]	✓		✓		✓		✓
	IoTFu18 [43]		✓		- -	- -		✓
		Vuln. Services	Weak Auth	Encryption				
Cloud Endpoint Section III-C	Max16 [23]	✓	✓		✓		✓	
	Oberm16 [25]		✓	✓	✓		✓	
	Nandi16 [44]	✓				✓		✓
	Blaic16 [45]	✓	✓	✓	✓		✓	
	Wilso17 [46]			✓		✓	✓	✓
	Surba17 [47]	✓			- -	- -	✓	✓
	DTAP18 [48]	✓	✓	✓		✓	✓	✓
		Encryption	MITM					
Communication Section III-D	BEAST11 [49]	✓			✓		✓	
	Garci11 [50]	✓	✓		✓	✓	✓	
	LUCKY13 [51]	✓			✓		✓	
	Ryan13 [52]	✓	✓		- -	- -	- -	- -
	Foula13 [53]	✓	✓		- -	- -	- -	- -
	Alfar13 [54]	✓			✓		✓	
	Selvi14 [55]	✓			✓		✓	
	POODL14 [56]		✓		✓		✓	
	FREAK15 [57]	✓			✓		✓	
	CRIME15 [58]		✓		✓		✓	
	SMACK15[59]	✓	✓		✓		✓	
	Adria15 [60]	✓	✓		✓		✓	
	Zilln15 [61]	✓	✓		- -	- -	- -	- -
	DROWN16 [62]	✓	✓		✓		✓	
	Jasek16 [63]		✓		✓		✓	
	Kinti16 [64]	- -	- -		✓			✓
	Aptho17 [65]	✓			✓			✓
	Wood17 [66]	✓				✓		✓

Example of Device Research

- Echo exposed hardware debug pins
- SmartTV unauthenticated services leads to Ransomware
- Vendor backdoors (Arris)
- Static master key in firmware (LIFX)
- Side-channel and vulnerable firmware – going nuclear (Hue)

Examples of Network Research

- Devices use IP to talk over the Internet
  - UPnP
  - Privacy issues (DNS)
  - TLS/SSL bugs
- Devices use low-energy protocols for nearby communication
  - Insecure rejoin (ZigBee)
  - ZWave master key
  - Bluetooth



SSL

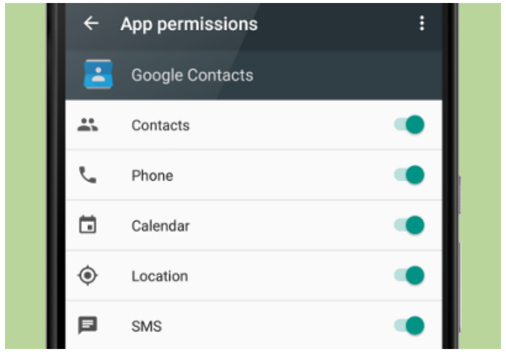
zigbee

Examples of Cloud Research

- Vulnerable cloud endpoints
- Integration services
- Cloud endpoint vulnerabilities
  - Expose PII
  - Control devices
  - Escalate privilege

Examples of Mobile Research

- Common permissions problem
- Incorrect use of cryptographic protocols
- Hardcoded keys
- Malicious apps
- IoT device fuzzing using mobile apps



App permissions

Google Contacts

Contacts

Phone

Calendar

Location

SMS

Overview of Past Research

Studied Componenets

Devices
Cloud integration services
Network (by association)

Mitigations

Patching bugs
Vendor responsibility

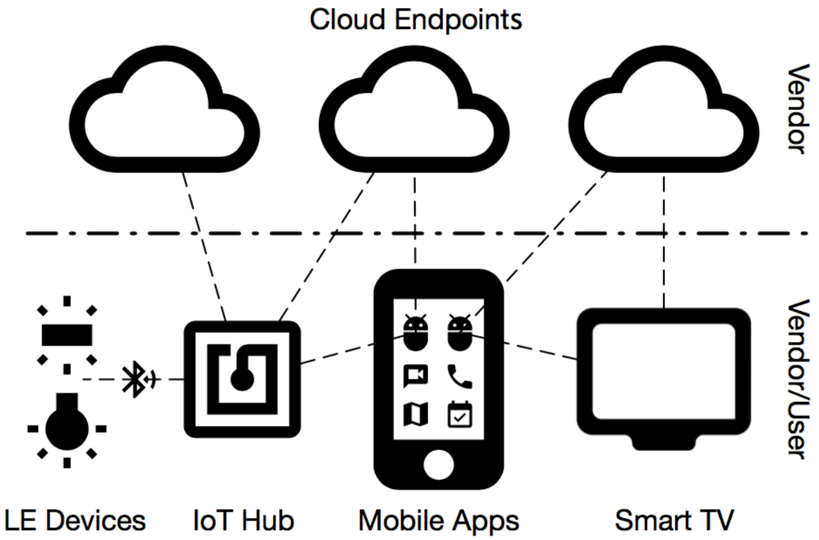
Unexplored Directions

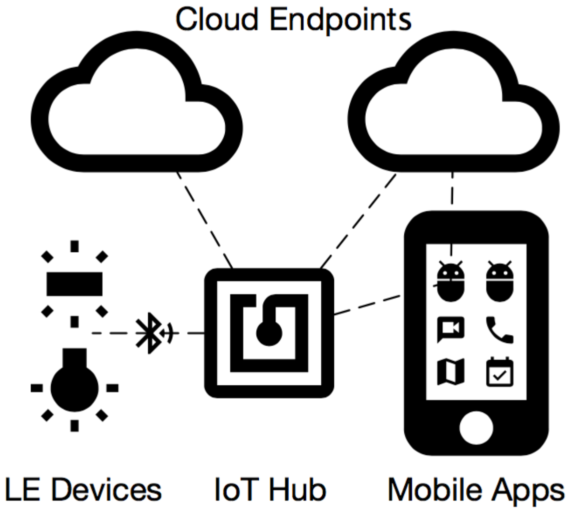
Mobile app
Cloud services
Network discovery protocols
User control and visibility

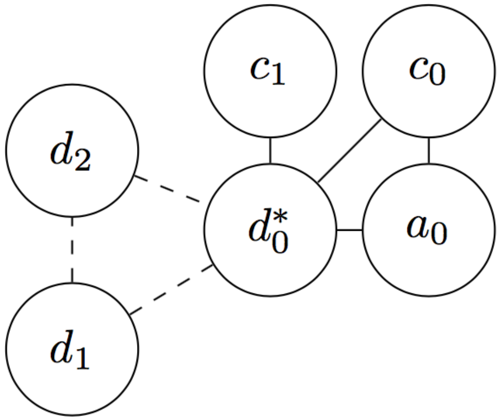
Reality Check: Research vs Market

- Evaluate IoT devices with a practical approach
  - Objective
  - Transparent
  - Measurable
  - Reproducible
- Device Representation
  - Media devices vs appliances
- Easy to understand
  - Consumer oriented

Methods: Deployment Evaluation







Our Approach

- Get a comprehensive view of deployments
- Account for all components
- Module design to accommodate for heterogeneity

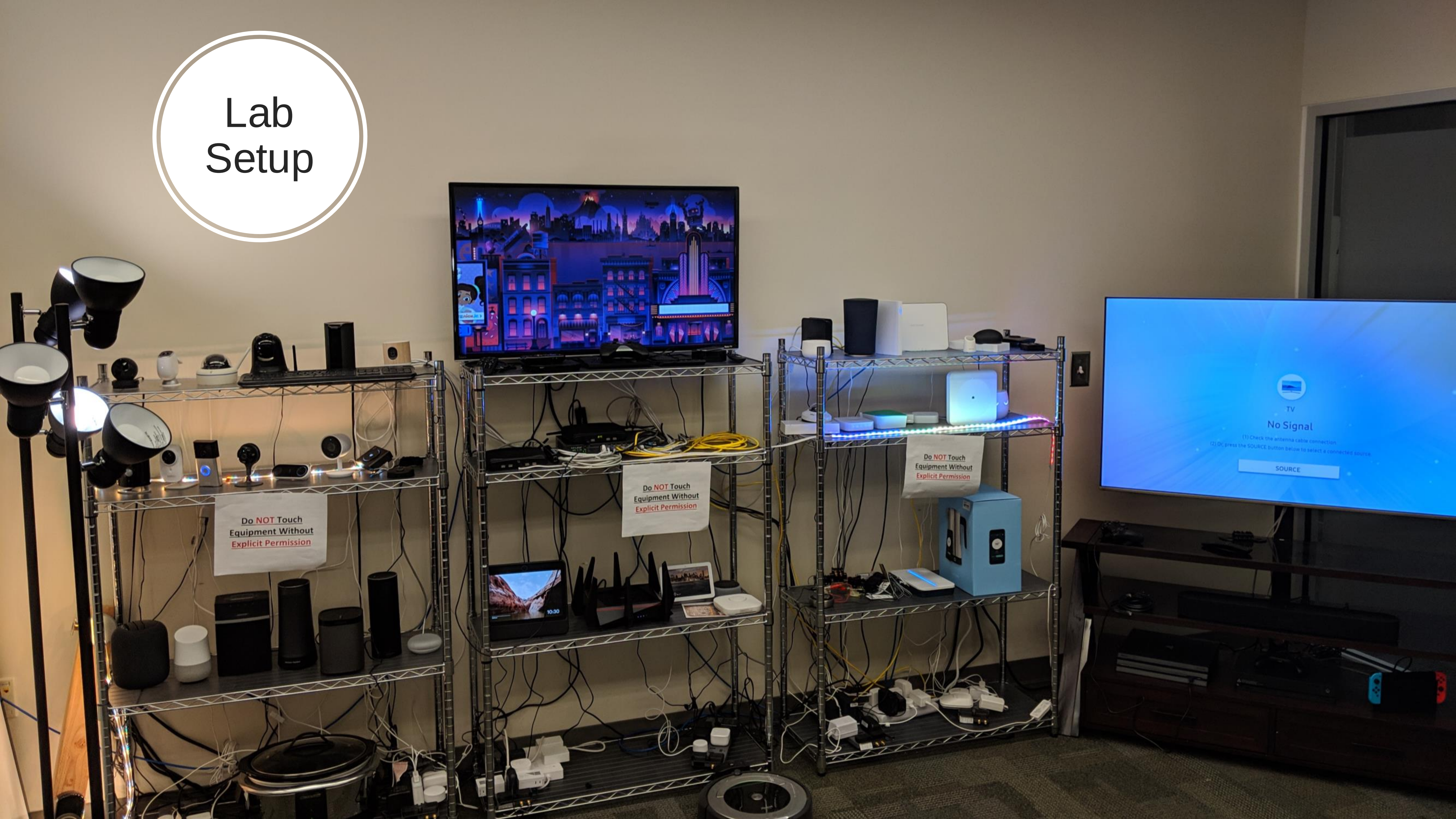
Overview of Approach

- Device
  - Internet pairing, configuration, updateable, exposed services
- Mobile app
  - permissions, crypto errors, hardcoded keys/secrets
- Cloud endpoints
  - types and counts, TLS/SSL, vulnerable software, insecure protocols
- Network
  - Device from/to cloud
  - Device from/to mobile app
  - Mobile app from/to cloud

Lab Setup

- The lab has over 65+ devices
  - Media devices, cameras, appliances, home security, home assistant, light bulbs, hubs, TVs, game consoles
- Network: single /24 private IPs with Linux (Debian) gateway
- ASUS AC5300 as a Wireless AP
- 48 Port Switch
- Ports are mirrored
- Device configuration
  - Minimal, keep default settings
  - Turn off auto-update, if possible
- iPad Mini and Samsung Tablet with companion mobile apps

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
SOURCE

Tools

- Device
  - Network service scan
  - Nessus scanner
- Mobile App
  - Static and dynamic analysis for iOS and Android apps
  - Kryptowire (Thank You!) kryptowire
- Cloud endpoints
  - Extract and label DNS traffic
  - Network service scan
  - Nessus scanner
- Network
  - Protocol analysis
  - Man-in-the-middle attack on TLS/SSL
  - SSLSplit, ntop-ng, iptables

Findings

Findings

- Devices
  - Insecure exposed services
  - Weak/no authentication on services
- Network communication
  - Encrypted over the Internet, TLS/SSL vulnerabilities
  - Most LAN communication lack encryption
- Cloud endpoints
  - Exposed services (some vulnerable)
  - Misconfigured
- Mobile apps
  - Over provisioned with permissions
  - Cases of incorrect use of crypto
  - Hard coded API/secret keys

Case Study: Device

MiCasa Verde VeraLite

- Bridge hub with ZWave
  - Door/window/motions sensors, door locks
- Cloud/device pairing
  - pre-printed pin (MAC address)
- Manual updates
  - notifies users of available updates
- Exposed services
  - DNS, UPnP, web, and SSH
- Default configurations out of the box
- UPnP services RCE vulnerability
  - CVE-2012-5958-65
- Dropbear SSH RCE vulnerability
  - CVE-2013-4863

Case Study: Network - Sonos Play 1

- Firmware version 8.3 (prior to 10)
- Wireless speaker
- UPnP on LAN
- Custom protocol over the Internet, port 3401
- Unencrypted communication between components
- Susceptible to man-in-the-middle
  - Passive snooping
  - Active interception

Case Study: Cloud - Belkin Netcam

- Cloud controlled indoor camera
- Motion detection
- Cloud endpoint allows SSLv2,v3
  - Vulnerable to downgrade attack
- Web app exposes running processes on server
- Open basic auth over HTTP
- JBoss vulnerable to unauthenticated RCE

Case Study: Mobile App - Koogeek

- Android v1.2.2
- WiFi lightbulb
- Mobile app controls lights
    - State (on/off), color, timer, and dimmer
- Hardcoded crypto keys
- API key and secret key for cloud services
- Requests excess permissions
    - More than 10 requested app permissions that are not used

Simple Setup
Connect to a 2.4 GHz Wi-Fi network. No hub or bridge required.
ogeek
E26
se
Done
BRIGHTNESS
SATURATION

Moving Forward

Putting it Together – YourThings.info

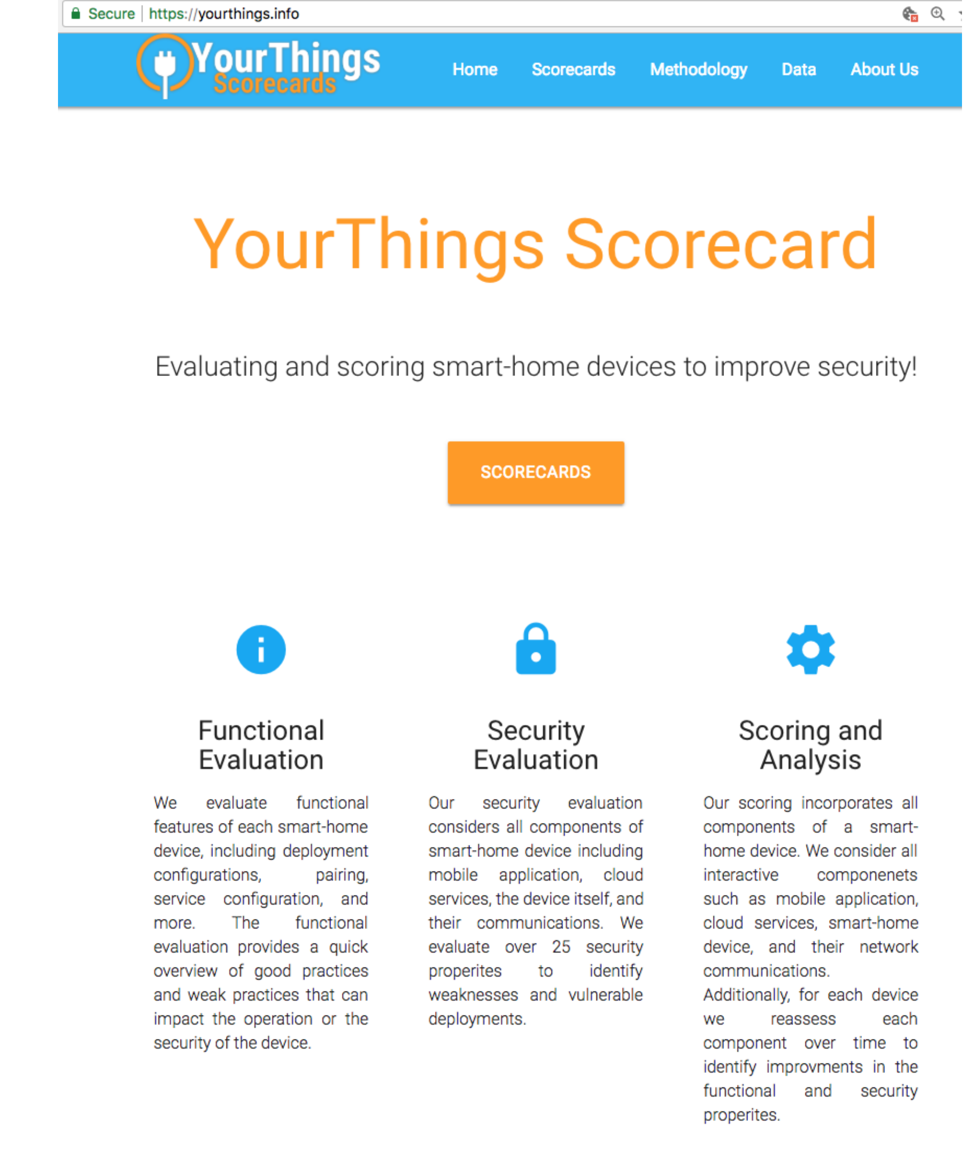
Created a scorecard system

Rating for components

Independent scoring

Modular and customizable

Documented



YourThings Scorecard

Evaluating and scoring smart-home devices to improve security!

Functional Evaluation

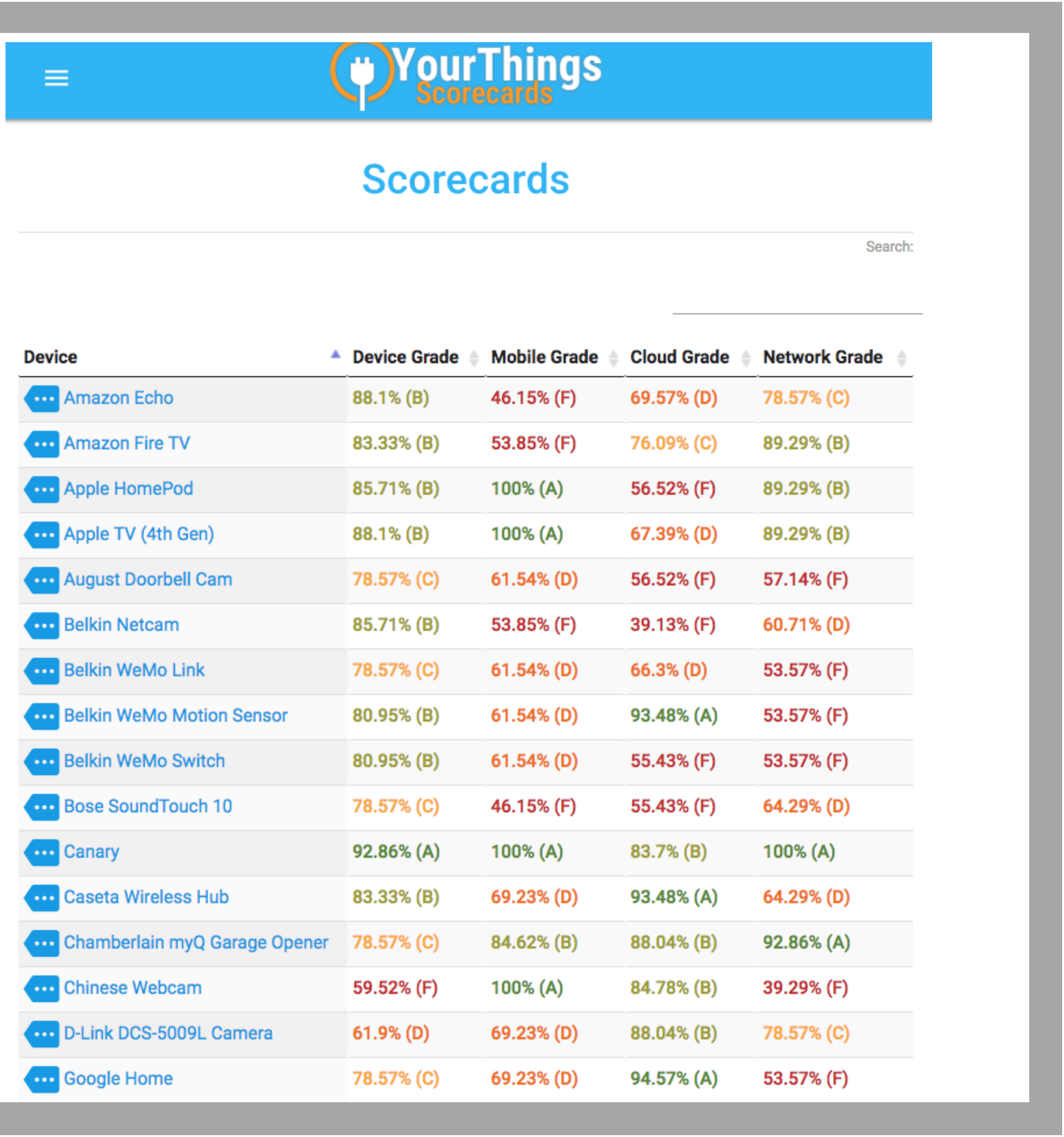
We evaluate functional features of each smart-home device, including deployment configurations, pairing, service configuration, and more. The functional evaluation provides a quick overview of good practices and weak practices that can impact the operation or the security of the device.

Security Evaluation

Our security evaluation considers all components of smart-home device including mobile application, cloud services, the device itself, and their communications. We evaluate over 25 security properites to identify weaknesses and vulnerable deployments.

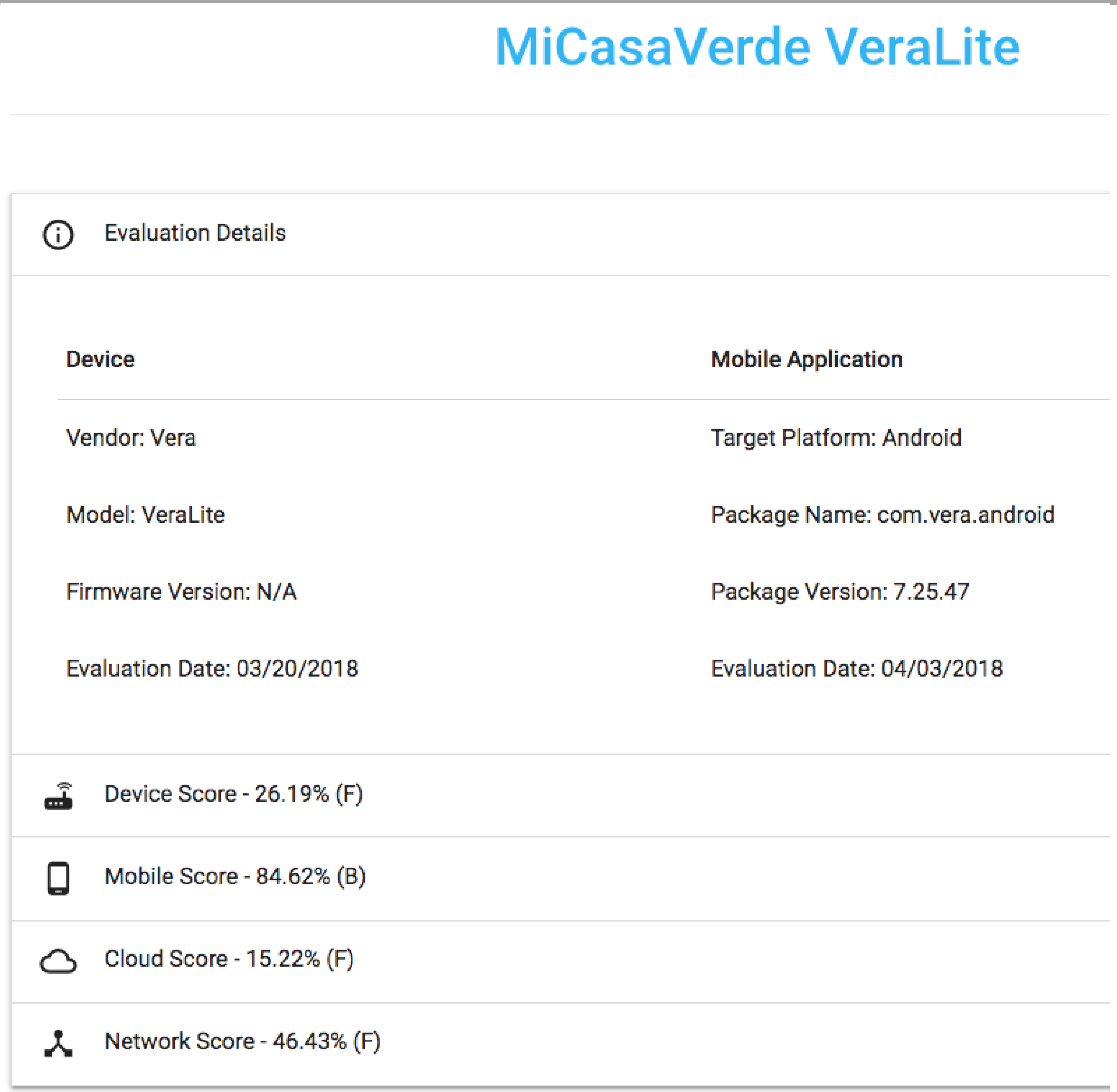
Scoring and Analysis

Our scoring incorporates all components of a smart-home device. We consider all interactive componenets such as mobile application, cloud services, smart-home device, and their network communications. Additionally, for each device we reassess each component over time to identify improvments in the functional and security properites.



Scorecards

Device	Device Grade	Mobile Grade	Cloud Grade	Network Grade
Amazon Echo	88.1% (B)	46.15% (F)	69.57% (D)	78.57% (C)
Amazon Fire TV	83.33% (B)	53.85% (F)	76.09% (C)	89.29% (B)
Apple HomePod	85.71% (B)	100% (A)	56.52% (F)	89.29% (B)
Apple TV (4th Gen)	88.1% (B)	100% (A)	67.39% (D)	89.29% (B)
August Doorbell Cam	78.57% (C)	61.54% (D)	56.52% (F)	57.14% (F)
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)
Belkin WeMo Switch	80.95% (B)	61.54% (D)	55.43% (F)	53.57% (F)
Bose SoundTouch 10	78.57% (C)	46.15% (F)	55.43% (F)	64.29% (D)
Canary	92.86% (A)	100% (A)	83.7% (B)	100% (A)
Caseta Wireless Hub	83.33% (B)	69.23% (D)	93.48% (A)	64.29% (D)
Chamberlain myQ Garage Opener	78.57% (C)	84.62% (B)	88.04% (B)	92.86% (A)
Chinese Webcam	59.52% (F)	100% (A)	84.78% (B)	39.29% (F)
D-Link DCS-5009L Camera	61.9% (D)	69.23% (D)	88.04% (B)	78.57% (C)
Google Home	78.57% (C)	69.23% (D)	94.57% (A)	53.57% (F)



MiCasaVerde VeraLite

Evaluation Details

Device	Mobile Application
Vendor: Vera	Target Platform: Android
Model: VeraLite	Package Name: com.vera.android
Firmware Version: N/A	Package Version: 7.25.47
Evaluation Date: 03/20/2018	Evaluation Date: 04/03/2018

Device Score - 26.19% (F)

Mobile Score - 84.62% (B)

Cloud Score - 15.22% (F)

Network Score - 46.43% (F)

Moving Forward – YourThings.info

- Evaluation data is public
- Packet capture includes
  - Device activity
  - Scans (request/response)
  - Mobile App interactions
  - Network attacks (MiTM)
- List of devices with IP mapping
- Raw scores in CSV format
- Evaluation single snapshot
- Network traffic collection continuous

Moving Forward - Collaboration/Partnership

- 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*