RSAConference2018
San Francisco | April 16–20 | Moscone Center


SESSION ID: MBS-T10

# IOT TRUST BY DESIGN - LESSONS LEARNED IN WEARABLES AND SMART HOME PRODUCTS

MODERATOR: **Jeff Wilbur**
Director, Online Trust Alliance initiative, Internet Society
@jeffwilbur01

PANELISTS: **Marc Bown**
Senior Director, Security
Fitbit
@marcbown

**John Cook**
Sr Director, Product Management
Symantec
@disruptprodsguy

# Poll the Audience

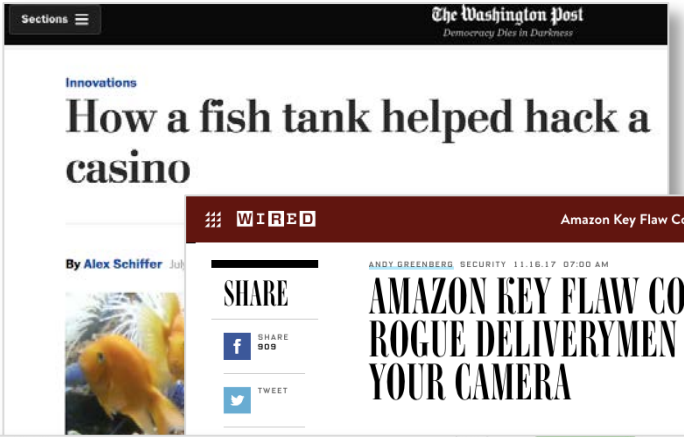


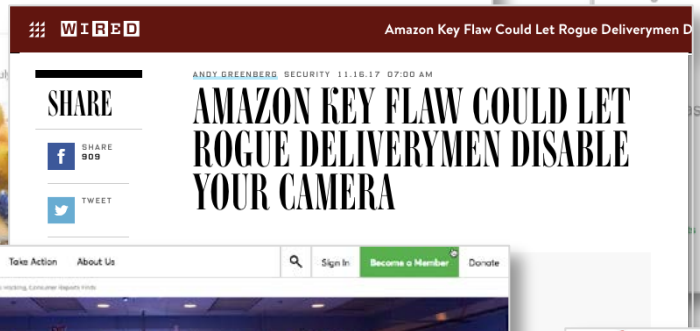
- Session MBS-T10
- Are you an IoT manufacturer, do you manage IoT in the enterprise or neither?
  - A – IoT manufacturer
  - B – Manage enterprise IoT
  - C – Neither

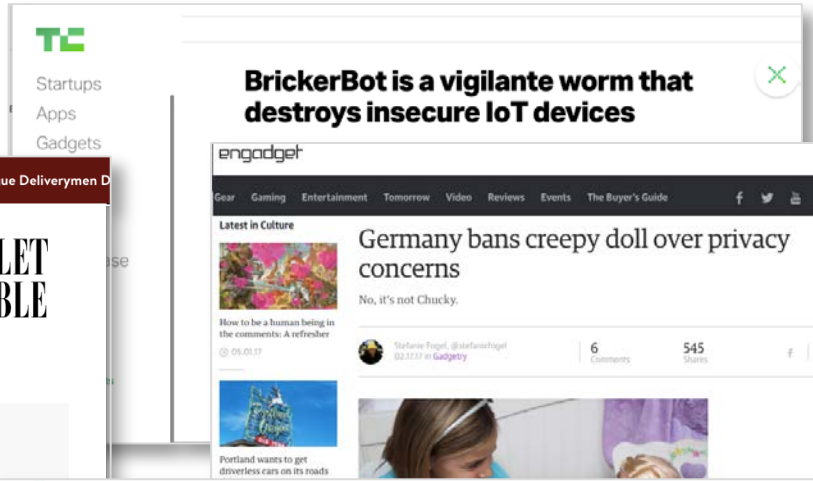
https://rsa1-live.eventbase.com/polls?event=rsa2018&polls=3802

# Why Are We Here?



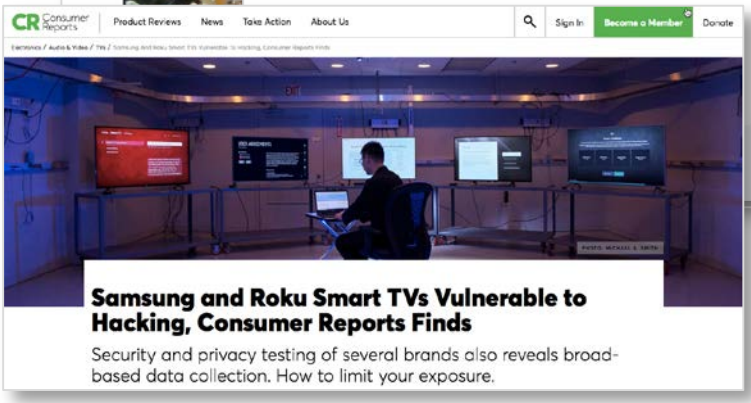


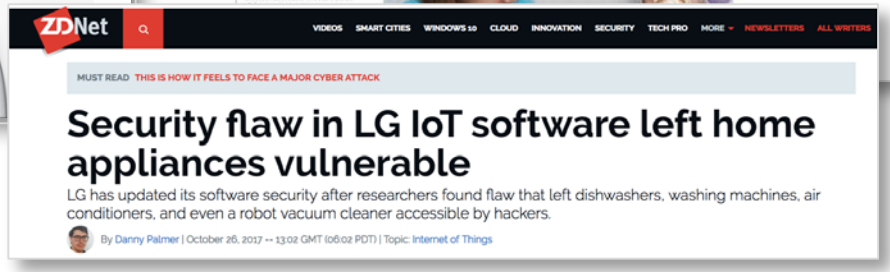









# What's at Risk?

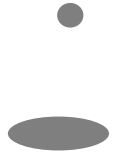


Smartwatches & wearables


Connected thermostats

Home alarm systems

Wireless doorbells



Real-time video monitoring

Smart televisions with built in apps

Streaming boxes for "regular" TVs

Gaming consoles

Plugs to make other things "smart"

Smart lights

Connected appliances

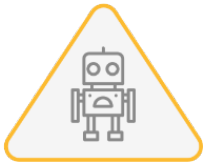
Source: Symantec

# Are Attacks Really Happening?



**22**
Threats Blocked
Per Home, Per Day

~8.3/day
Malware Blocked



~5.4/day
Botnets Blocked

~1/day
Spam Blocked

~1.2/day
Phishing Blocked

~0.4/day
Scams Blocked

~1/day
PUP Blocked

Source: Symantec

# Poll the Audience

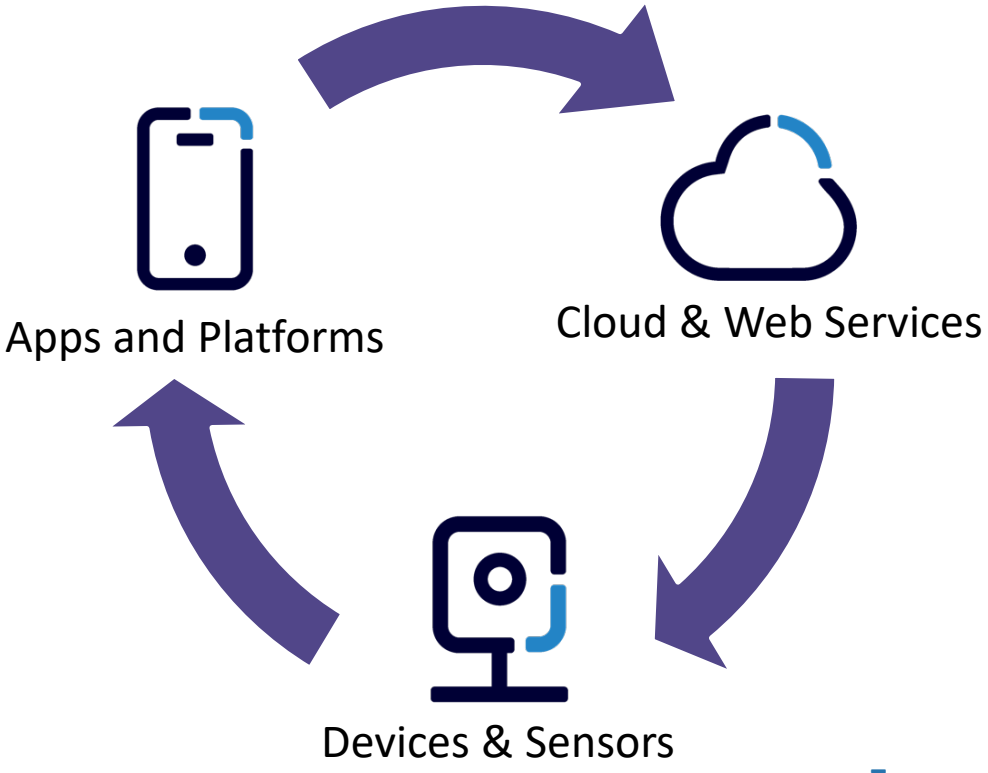



- Session MBS-T10
- Which part of the system requires the most "trust by design" discipline to ensure proper security and privacy?
  - A – Devices and sensors
  - B – Mobile apps
  - C – Back-end services

https://rsa1-live.eventbase.com/polls?event=rsa2018&polls=3803

# Where Do Vulnerabilities Lie?

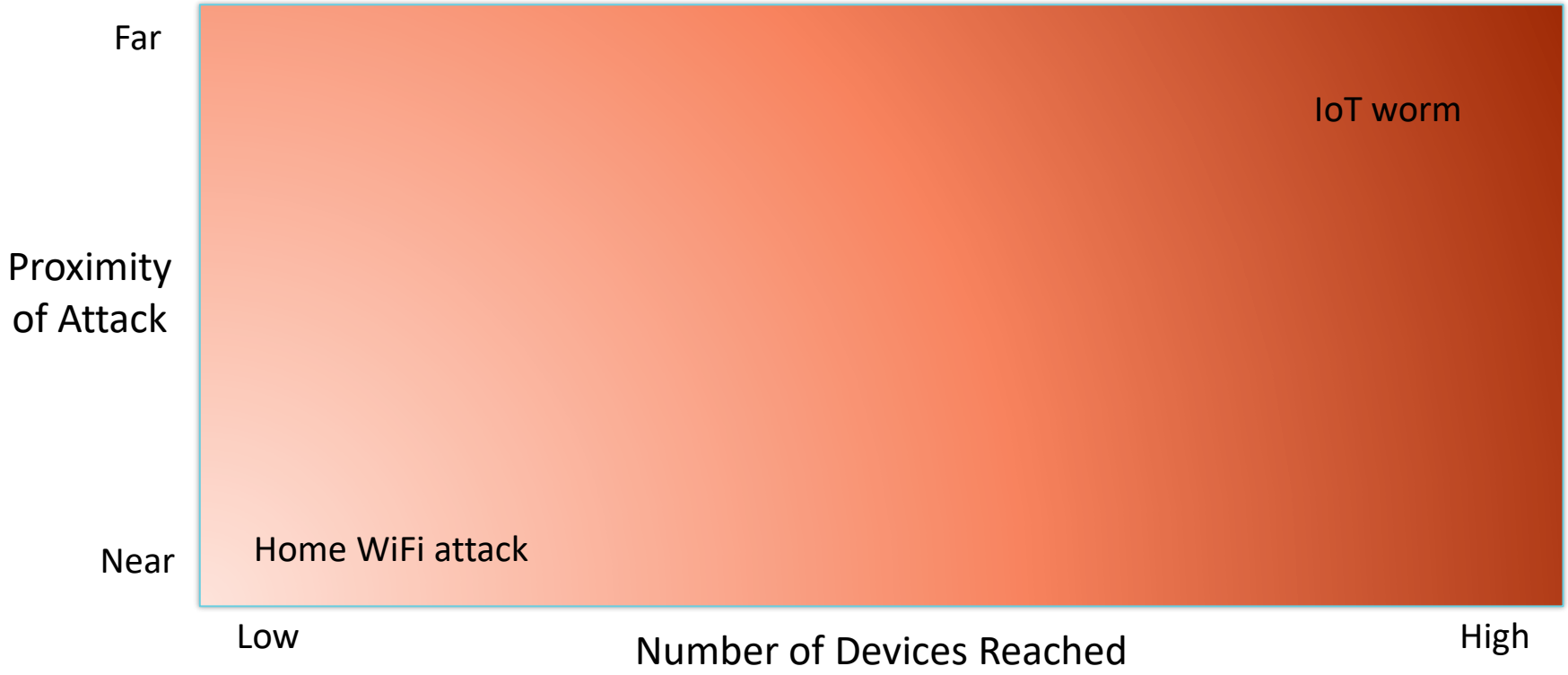





- Key device sub-systems
  - Processor/memory/platform
  - Radios
  - Battery
  - Software stacks

# Assessing Attack “Reach”





# Poll the Audience



- Session MBS-T10
- What is the biggest reason security and privacy capability get compromised when developing consumer-grade IoT products?
  - A – Cost
  - B – Time
  - C – Not a priority

https://rsa1-live.eventbase.com/polls?event=rsa2018&polls=3804

# Addressing IoT Security and Privacy

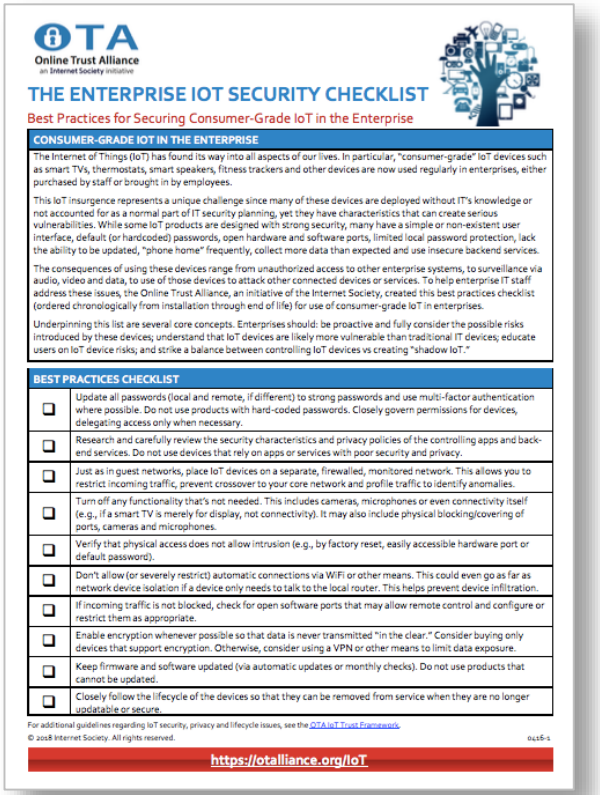


| | | | |
|---|---|---|---|
| Authentication | Encryption | Security | Updates |
| Privacy | Disclosures | Control | Communications |

- The Online Trust Alliance's IoT Trust Framework principles address
  - Security, privacy and lifecycle issues
  - Cover devices/sensors, apps and backend services

# Using Consumer-Grade IoT in the Enterprise





OTA
Online Trust Alliance
an Internet Society initiative

## THE ENTERPRISE IOT SECURITY CHECKLIST

Best Practices for Securing Consumer-Grade IoT in the Enterprise

**CONSUMER-GRADE IOT IN THE ENTERPRISE**

The Internet of Things (IoT) has found its way into all aspects of our lives. In particular, "consumer-grade" IoT devices such as smart TVs, thermostats, smart speakers, fitness trackers and other devices are now used regularly in enterprises, either purchased by staff or brought in by employees.

This IoT insurgence represents a unique challenge since many of these devices are deployed without IT's knowledge or not accounted for as a normal part of IT security planning, yet they have characteristics that can create serious vulnerabilities. While some IoT products are designed with strong security, many have a simple or non-existent user interface, default (or hardcoded) passwords, open hardware and software ports, limited local password protection, lack the ability to be updated, "phone home" frequently, collect more data than expected and use insecure backend services.

The consequences of using these devices range from unauthorized access to other enterprise systems, to surveillance via audio, video and data, to use of those devices to attack other connected devices or services. To help enterprise IT staff address these issues, the Online Trust Alliance, an initiative of the Internet Society, created this best practices checklist (ordered chronologically from installation through end of life) for use of consumer-grade IoT in enterprises.

Underpinning this list are several core concepts. Enterprises should: be proactive and fully consider the possible risks introduced by these devices; understand that IoT devices are likely more vulnerable than traditional IT devices; educate users on IoT device risks; and strike a balance between controlling IoT devices vs creating "shadow IoT."

**BEST PRACTICES CHECKLIST**

| | |
|---|---|
| ❑ | Update all passwords (local and remote, if different) to strong passwords and use multi-factor authentication where possible. Do not use products with hard-coded passwords. Closely govern permissions for devices, delegating access only when necessary. |
| ❑ | Research and carefully review the security characteristics and privacy policies of the controlling apps and back-end services. Do not use devices that rely on apps or services with poor security and privacy. |
| ❑ | Just as in guest networks, place IoT devices on a separate, firewalled, monitored network. This allows you to restrict incoming traffic, prevent crossover to your core network and profile traffic to identify anomalies. |
| ❑ | Turn off any functionality that's not needed. This includes cameras, microphones or even connectivity itself (e.g., if a smart TV is merely for display, not connectivity). It may also include physical blocking/covering of ports, cameras and microphones. |
| ❑ | Verify that physical access does not allow intrusion (e.g., by factory reset, easily accessible hardware port or default password). |
| ❑ | Don't allow (or severely restrict) automatic connections via WiFi or other means. This could even go as far as network device isolation if a device only needs to talk to the local router. This helps prevent device infiltration. |
| ❑ | If incoming traffic is not blocked, check for open software ports that may allow remote control and configure or restrict them as appropriate. |
| ❑ | Enable encryption whenever possible so that data is never transmitted "in the clear." Consider buying only devices that support encryption. Otherwise, consider using a VPN or other means to limit data exposure. |
| ❑ | Keep firmware and software updated (via automatic updates or monthly checks). Do not use products that cannot be updated. |
| ❑ | Closely follow the lifecycle of the devices so that they can be removed from service when they are no longer updatable or secure. |

For additional guidelines regarding IoT security, privacy and lifecycle issues, see the OTA IoT Trust Framework.



0416-1

https://otalliance.org/IoT

- Newly released checklist for handling consumer-grade IoT in the enterprise
- Organized "chronologically", from purchase and installation through maintenance and end of life

# Lessons Learned



# Resources



- OTA IoT Trust Framework –
  - https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework6-22.pdf
- Consumer-Grade IoT in the Enterprise – A Security Checklist
  - https://otalliance.org/system/files/files/initiative/documents/enterprise_iot_checklist.pdf