RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: AST2-W02

Diffusing the IoT Time Bomb—Security and Privacy Trust Code of Conduct

MODERATOR: **Craig Spiezle**

Executive Director & President
Online Trust Alliance
@otalliance @craigspi

PANELISTS:

Harvey Anderson
General Counsel, Chief Privacy Officer
AVG Technologies
@AVGFree

Paul Plofchan
VP, Government & Regulatory Affairs, Chief Privacy Officer
ADT
@paulplofchan

Brian Witten
Senior Director, IoT
Symantec
@WittenBrian

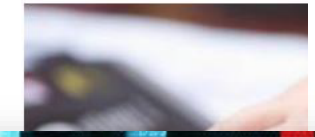
#RSAC

The Landscape

Baby monitor vulnerabilities bring IoT security issues into sharp focus

Share this article:

In research that should strike fear in the heart of any new parent—and those professionals concerned about the security implications of the Internet of Things—a security pro at Rapid7 found



Exec fears predators can reach kids through new Barbie

By Kevin Dugan

January 16, 2016 | 1:36am

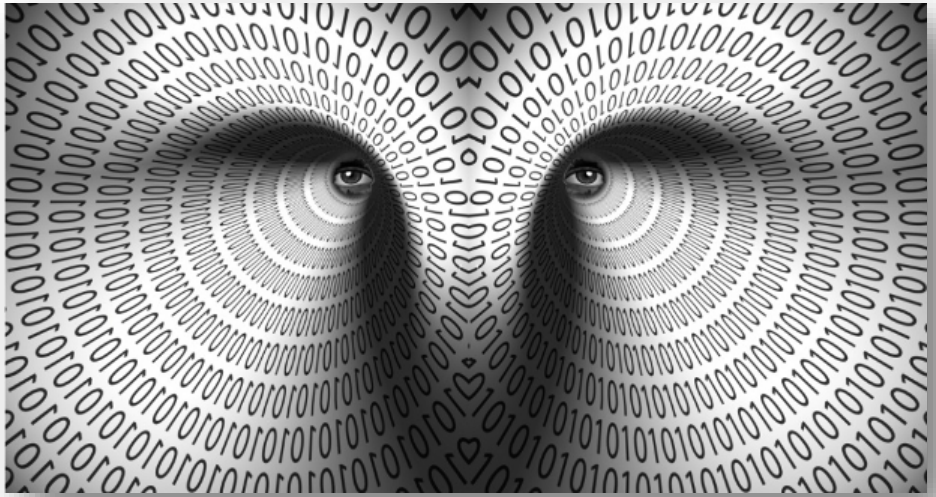
Consumer Electronics Mobility Security

Wearables, apps disclose user passwords and location: Symantec

Nestor Arellano

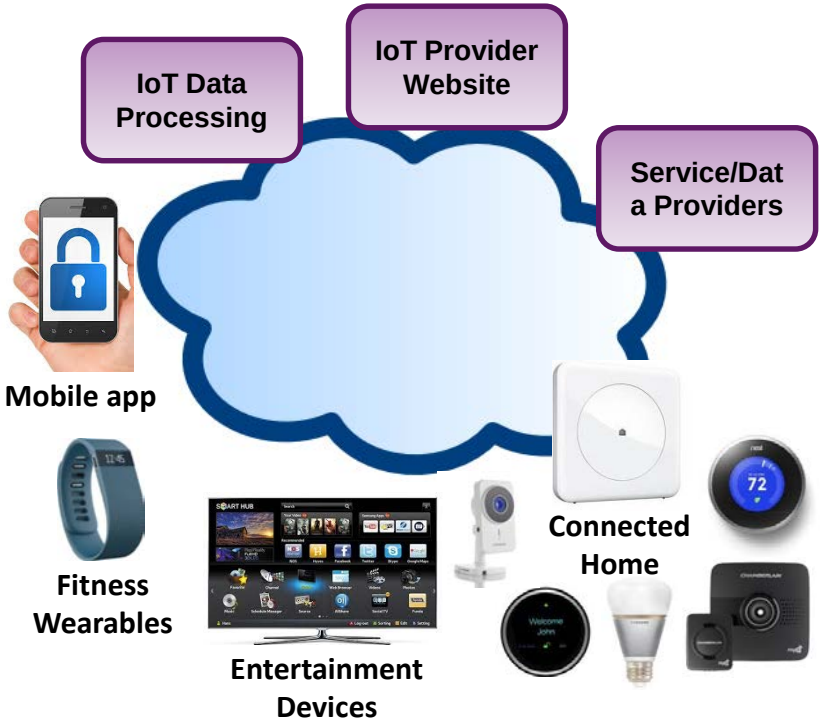
Challenge - Ambient Data Collection

- Growing number of devices & sensors
- Sharing with unknown/undisclosed third parties
- May be “benign” today, but harmful tomorrow



Challenges - IoT Ecosystem

- Highly personal, dynamic, persistent data collection.
- Combination of devices, apps, platforms & cloud services.
- Multiple data flows, touch points and disclosures.
- Lack of defined standards.
- Non-traditional vendors.



The Consumer

- 93% of adults state being in control of who has access to their information is important.
- 90% do not wish to be observed without approval.
- 88% say it is important that they not have someone watch or listen to them without their permission. [1]
- **47% of respondents pointed to security and privacy as obstacles to adopting such technology.**
- **18% quit using IoT devices due to lack of service guarantees.** [2]

[1] Pew Research Center, 2015
[2] Accenture Research 1/2016, n = 28,0000

Overview – IoT Trust Framework

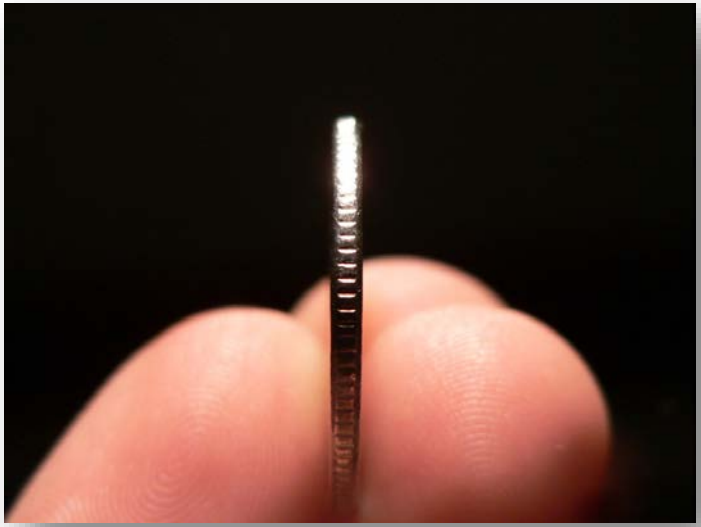
Multi-Stakeholder working group formed in February 2015

Code of Conduct

- Foundation for certification

30 Principles Addressing:

- Security
- Privacy
- Sustainably; *from purchase to end of life*



Framework – 30 Baseline Criteria

IoT Trust Framework ● Required ○ Recommended N/A – Not Applicable	Connected Home	Wearable Tech
SECURITY		
1. Ensure devices support current generally accepted security transmission protocols. All personally identifiable data in transit and in storage must be encrypted using current generally accepted security standards. This is including but not limited to wired, WI-FI and Bluetooth connections.	●	●
2. All authentication credentials, including but not limited to passwords shall be salted and hashed and/or encrypted.	●	●
3. All IoT support web sites must fully encrypt the user session. Current best practices include HTTPS or HTTP Strict Transport Security (HSTS) by default, also known as AOSSL or Always On SSL.	●	●
4. IoT support sites must implement regular monitoring and continual improvement of site security and server configurations to acceptably reduce the impact of vulnerabilities. Perform generally accepted penetration tests at least annually.	●	●
5. Establish and maintain processes and systems to receive, track and promptly respond to external vulnerabilities reports from third parties including the research community. Remediate post product release design vulnerabilities and threats in a publically responsible manner either through remote updates and/or through actionable consumer notifications, or other effective mechanism(s).	●	●

Breaking News

FEB 17, 2016 @ 10:26 AM 6,150 VIEWS

Samsung Fails To Secure Thousands Of SmartThings Homes From Thieves

Thomas Fo… Brewster …

I cover crime, p…

FOLLOW ON F…

When Samsung bought… 2014, it wanted to incor… That meant it inherited…

ASUS Settles FTC Charges That Insecure Home Routers and "Cloud" Services Put Consumers' Privacy At Risk

FOR RELEASE

February 23, 2016

TAGS: deceptive/misleading conduct | Technology | Bureau of Consu…

Privacy and Security | Consumer Privacy | Data Security

Taiwan-based computer hardware maker ASUSTeK Computer, Inc. has a… charges that critical security flaws in its routers put the home networks of… risk. The administrative complaint also charges that the routers' insecure… thousands of consumers' connected storage devices, exposing their sens…

'CSI: Cyber' Episode Guide (Feb. 21): A Jogger is Found Dead

Line Spacing Font Size

Open Dialog


High
Medium
Low
Informational
False Positive


UPDATE


DON'T
COLLECT
WHAT YOU
CAN'T
PROTECT


ANNOUNCEMENT

Apply What You Have Learned Today

- **Next week you should:**
  - Review the IoT Framework & Resource Guide
  - Complete a Self-Assessment - Review your and your vendors' privacy policies
  - Review with your developers & engineers
- **In the first three months following this presentation you should:**
  - Complete an internal & external assessment
  - Identify security & privacy opportunities for product enhancements
- **Within six months you should:**
  - Have an updated security & privacy roadmap with company wide buy-in
  - Make security & privacy part of your value position
  - Update your breach and incident response plan

More Information

IoT Trust Working Group https://otalliance.org/Iot

Symantec www.symantec.com/iot

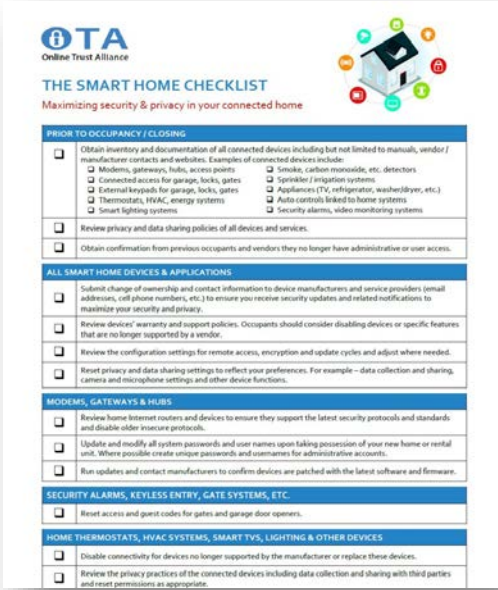
OTA Meet & Greet – Today 10 am – South Upper Lobby

Blended Intelligence Reception

Tonight Jewish Museum 5 to 9 PM

Education - The Connected Home

- Partnership with the National Association of Realtors
- Security, Privacy & Personal Safety
- Prior to occupancy, rental & at “closing”
- Prescriptive advice
- https://otalliance.org/SmartHome



OTA
Online Trust Alliance

THE SMART HOME CHECKLIST

Maximizing security & privacy in your connected home

PRIOR TO OCCUPANCY / CLOSING

- ❑ Obtain inventory and documentation of all connected devices including but not limited to manuals, vendor / manufacturer contacts and websites. Examples of connected devices include:
  - ❑ Modems, gateways, hubs, access points
  - ❑ Connected access for garage, locks, gates
  - ❑ External keypads for garage, locks, gates
  - ❑ Thermostats, HVAC, energy systems
  - ❑ Smart lighting systems
  - ❑ Smoke, carbon monoxide, etc. detectors
  - ❑ Sprinkler / irrigation systems
  - ❑ Appliances (TV, refrigerator, washer/dryer, etc.)
  - ❑ Auto controls linked to home systems
  - ❑ Security alarms, video monitoring systems
- ❑ Review privacy and data sharing policies of all devices and services.
- ❑ Obtain confirmation from previous occupants and vendors they no longer have administrative or user access.

ALL SMART HOME DEVICES & APPLICATIONS

- ❑ Submit change of ownership and contact information to device manufacturers and service providers (email addresses, cell phone numbers, etc.) to ensure you receive security updates and related notifications to maximize your security and privacy.
- ❑ Review devices’ warranty and support policies. Occupants should consider disabling devices or specific features that are no longer supported by a vendor.
- ❑ Review the configuration settings for remote access, encryption and update cycles and adjust where needed.
- ❑ Reset privacy and data sharing settings to reflect your preferences. For example – data collection and sharing, camera and microphone settings and other device functions.

MODEMS, GATEWAYS & HUBS

- ❑ Review home Internet routers and devices to ensure they support the latest security protocols and standards and disable older insecure protocols.
- ❑ Update and modify all system passwords and user names upon taking possession of your new home or rental unit. Where possible create unique passwords and usernames for administrative accounts.
- ❑ Run updates and contact manufacturers to confirm devices are patched with the latest software and firmware.

SECURITY ALARMS, KEYLESS ENTRY, GATE SYSTEMS, ETC.

- ❑ Reset access and guest codes for gates and garage door openers.

HOME THERMOSTATS, HVAC SYSTEMS, SMART TVS, LIGHTING & OTHER DEVICES

- ❑ Disable connectivity for devices no longer supported by the manufacturer or replace these devices.
- ❑ Review the privacy practices of the connected devices including data collection and sharing with third parties and reset permissions as appropriate.

Education – Connected Devices

- Connected devices within the connected city & home.
- Targeting buyers / recipients of connected devices during 2015 Holiday
- Prior to purchase & set up.
- Proactively raise awareness of Security & Privacy considerations.
- https://otalliance.org/SmartHome

OTA
Online Trust Alliance

SMART DEVICE PURCHASE & SETUP CHECKLIST

Maximizing Security & Privacy with Your Smart TV & Connected Devices

SECURITY

- ❑ Prior to purchase confirm your ability to return the device for a refund if on set up you find the security and/or privacy practices do not comply with industry best practices or your personal requirements. If you cannot opt out of sharing data with third parties or are not provided the option of opting in, consider alternative products.
- ❑ Prior to purchase review device's warranty and support policies and verify the security and software patches are provided for the life of the product, beyond that of the device warranty period offered by the manufacturer.
- ❑ Register your device providing your contact information and primary email address with the manufacturer to help ensure you receive security updates and related notifications to help maximize your security and privacy.
- ❑ Verify your device is updated and patched directly from the manufacturer. Install updates as soon as they become available. If possible enable automatic updates on the device setup options.
- ❑ Use a unique user name and password which does not identify your family or the brand/model of the device and change them frequently. This can reduce the threat of your device being maliciously targeted by hackers.
- ❑ When downloading apps to your device, install them directly from the manufacturer's official site where possible and carefully review any requested permissions such as location tracking, use of the camera and microphone.
- ❑ When browsing sites with your connected device, exercise the same caution as you would with your personal computer.
- ❑ Turn off and unplug your device(s) if you are gone for extended periods of time to reduce the risk of your device being hacked, being susceptible to power surges and save on energy use.
- ❑ If possible, connect your device directly through a wired connection. If your home router has a guest network use it to isolate your device(s) from other networks.
- ❑ Disable or protect remote access to your connected device(s) when not needed to reduce the risk of hacking.
- ❑ Any device that connects to the Internet should be guarded by a firewall to help prevent unauthorized access. Use a router-based firewall and turn on any built-in firewall settings your device might have.
- ❑ Document all of the smart devices and applications you use. List the company URL, passwords, contact email and phone numbers. Password protect the document or use a password "vault" mobile application.

PRIVACY

- ❑ If you are selling your connected device, reset the device to factory settings and/or clear any saved data. If you are purchasing or using a previously owned or opened device, be sure the device has been reset to factory settings (including advertising identifiers, parental controls and all privacy settings) before using it.
- ❑ Review the privacy practices of connected devices you own or are considering buying including data collection and sharing policies with third parties. Reset permissions to reflect your preferences (for example – data collection and sharing, camera and microphone settings and other functions). If your settings cannot be modified, consider the "reset to factory settings" option to start a clean setup.
- ❑ To maximize your privacy, disable use of the camera and microphone. Consider removing the camera, flipping it to face the wall or covering the camera lens to prevent accidental or unauthorized use. Doing so means the camera will only capture a black image or the wall.
- ❑ Create user profiles with unique settings for children's use of the device.

https://otalliance.org/SmartHome