Building Trust & Enabling Innovation for Voice Enabled IoT

Lynn Terwoerds

JULY 30 - AUGUST 4, 2016 / MANDALAY BAY / LAS VEGAS

From the Keyboard to the Microphone

- 1952 – first voice recognition device recognized single digits
- 2016
  - Siri, Cortana, Echo, Google Home, Hello Barbie, Sony SmartWatch 3, Samsung Smart TV, Honeywell thermostat, GirlTech Password Journal, Skully Smart Helmet, Dragon Dictation – just to name a few
  - USD $6.4 billion IoT business (projected to be USD $2 trillion in 2020[1])

Source = Jim Tully, VP & lead IoT researcher for Gartner, 2015

Opportunity

- Development community has an opportunity to innovate and fundamentally change the way we interact with technology
- Customers *naturally* will speak to their devices, developers will not need to teach new habits
- Significant opportunity to embed voice even more into IoT and capture valuable data
- Voice can be used for many things
  - Recognition (already widely applied)
  - Biometrics
  - Converge with other emerging tech such as AI, data analytics, block chain, avatars

Risk

- Voice is deeply personal and unique
- Customers have already reacted with the fear their device is always “listening”
- Voice is easy to capture (maybe unintentionally)
- A new attack vector, plus the same old weaknesses
- Customers can change their password, get a replacement credit card, even get a new social security number, but they cannot change their voice

A Matter of Trust

- Lack of trust could stifle innovation
- A serious incident will have ripple effects across the sector, not just a single company
- While there are new security & privacy concerns, many of the problems remain the same
- It's not just a technology problem
  - Educate customers & press
  - Address the FUD right away
  - Leverage years of existing security resources (e.g. SANS, CVE)
  - Speak the language of the customer
  - Proper transparency

The Power of Industry Collaboration

- Thought leadership
- Enable innovation
- Save time, money, reputations
- Tangible deliverables
  - **Toolkit for developers**
  - Legal thought leadership through “Legal Pad Notes”
  - Consumer infographics
- Open to everyone – men and women
- To join, email voiceprivacy@ewf-usa.com
- Follow @voiceprivacy

Voice Privacy Alliance
an EWF Initiative

VPA Innovation Toolkit http://www.ewf-usa.com/voiceprivacy

- Specifically for developers, peer reviewed by developers
- 41 Agile security stories
- Can be adapted for any development methodology
- Focuses on voice IoT specific considerations
- Toolkit is open source, meant to be adapted, modified
- Next revision scheduled for Jan/Feb 2017
- Join the Voice Privacy Alliance and improve the toolkit! voiceprivacy@ewf-usa.com

Voice Privacy Alliance
an EWF Initiative

From the VPA Toolkit

Security Story	Guidance
Customers and the press have concerns the device is "always listening" and this makes them uncomfortable, especially if the device is in a home.	Give customers a "mute" capability when a device or application is always listening, even if it's just listening for a wake word (phoneme). And a hardware kill switch is best because hackers could disable a software kill switch. Giving customers this kind of control may help alleviate fears and uncertainty with devices that need to “listen” as critical requirement. You might also consider being transparent with customers how much you buffer when in listen mode. For example, your device might have a 30 second buffer as it listens for a wake word. After 30 seconds the buffer is cleared and the cycle repeats until the customer uses the wake word. Being transparent may alter customer perceptions and make them more comfortable with your product. Allow customers the ability to "mute" when a device or application is always listening, even if it's just listening for a wake word. This could ease fears of someone always listening. You might also consider being transparent with customers how much you buffer when in listen mode. For example, your device might have a 30 second buffer as it listens for a wake word. After 30 seconds the buffer is cleared and the cycle repeats until the customer uses the wake word. Being transparent may alter customer perceptions and mitigate this fear.

From the VPA Toolkit

Security Story	Guidance
Customers fear what they say will live on forever. Their concerns might be expressed as, "If you record something I say, can I delete it? What if I said something I'm ashamed of or embarrassed by? Since your device lives in my home or is something I wear, it's possible you'll record something very personal or potentially embarrassing."	If you are storing customer voice data, give them control over their own data. Allow customers the ability to delete their voice data, even if there are UX implications to the product. You may also want to inform the customer how deleting their voice data could negatively impact their user experience.

From the VPA Toolkit

Security Story	Guidance
Customers understand that companies share customer data with 3rd parties. Sharing voice data, especially an actual voice recording may cause concern and mistrust.	If you authenticate a customer to a 3rd party service, do so securely and make sure the customer is aware they have crossed over a trust boundary. Again there is a fundamental difference between lower risk voice recognition scenarios where a customer might request a stock quote, you convert that request to text, send it to a third party and the customer gets a response to their request. If you are sending voice data to a 3rd party to analyze, maybe parse and store, then you should consider securing that communication.

From the VPA Toolkit

Security Story	Guidance
Can my voice enabled device just respond to me? In my home and with my wearables, I live in a dynamic environment and I wonder if my device could respond to someone else's command.	Verify if a single user should have a unique session connection with your product or if multiple sessions are allowed. For example, Hello Barbie may have several people interact with her, but the doll is associated with a child and that child's authorizing adult. Consider if there are use cases where it would be appropriate to reject sessions not initiated by the authorized user. Amazon Echo is the opposite, designed to respond to anyone who invokes the wake word

From the VPA Toolkit

Security Story	Guidance
Customers want to know you are keeping up with current threats. Rogue wireless networks are a known threat and many customers lack the knowledge to protect themselves against this problem.	Ensure your device can verify it’s communicating with legitimate devices or networks. It's possible you can be fooled into connecting to a rogue wireless network or your customer can be fooled.

From the VPA Toolkit

Security Story	Guidance
Most customers are aware of the problems associated with lost or stolen devices.	Consider physical tampering scenarios. Wearables and IoT devices are shrinking in size. Developers must consider physical threats against lost or stolen devices. Automatic logoff or session timeout may help (cf.#63). If there is valuable and very personal data on the device, consider encryption at rest.

From the VPA Toolkit

Security Story	Guidance
If your device communicates with the customer, how will your customer know it's your device talking and not some interloper like a hacker?	Develop use case scenarios where an attacker might intercept the conversation between a customer and their device, potentially compromising the confidentiality and integrity of the conversation. For example, a voice enabled children's toy is made to say something wholly inappropriate to a child because the communication channel has been compromised. When protecting voice data in transit you can transmit via TLS – or another acceptably secure protocol – that will protect the data from interception or modification regardless of the configuration of the local home network. A solid overview of using TLS to protect communications can be found in the OWASP TLS Cheat Sheet: https://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet Overall, it's best to assume the home wireless network is insecure.

Final Thoughts

- Let's not repeat old mistakes
- Embed security early in the development lifecycle to save time, money, churn
- Industry can demonstrate leadership ahead of
  - Regulation
  - Litigation
  - FUD
- Download the toolkit http://www.ewf-usa.com/voiceprivacy