Intersection of Sexual Assault and IoT Vulnerabilities

Amy Devine
adevine@depaul.edu

Table of Contents

Content Advisory

While the focus of this paper is technology, specifically the security of Internet of Things (IoT) devices, it touches on technology's relationship to sexual and domestic abuse and assault. There are no sexually explicit descriptions and discussion is kept to legal, technical or social implications of the content.

Disclaimer

As I started researching the impacts of hacks on intimate (adult) toys, a topic I thought would be full of embarrassing but light-hearted stories, I stumbled upon the article from the New York Times that quoted a technologist alleging that unauthorized use of a vibrator may actually constitute sexual assault. More research into the claimed physical harm from the cyber domain led me to articles about how hacked IoT devices are being used for assault and for domestic abuse. That is where this went from light-hearted to very real. The challenge lies in understanding how to drive analytic thinking when dealing with actual human harm.

Physical Harm

In 2017, The New York Times published an article discussing the legal actions surrounding Standard Innovation's lack of security in their We-Vibe devices. The lawsuit was settled for $3.75 million. The bulk of the lawsuit involved the alleged unauthorized collection and transmission of personal information to Standard Innovation, with alleged violation of the Federal Wiretap Act and Illinois privacy laws. Under California CCPA laws today, the lack of clear data collection and

transmission could be considered a security breach. [9] But, the most [2] interesting statement was from a hacker presentation at DEF CON 24 about the perceived larger issue.

> "But if you come back to the fact that we're talking about people, unwanted activation of a vibrator is potentially sexual assault."[1] [3]

Legal action citing sexual assault from unwanted activation was not found online however that does not mean it hasn't happened. In fact, with sex toys being illegal in parts of the world, including the United States [4] and the majority of sexual assault cases going unreported [5], it stands likely that this is happening but not reported. Assault is not just limited to sex toys: IoT devices are being hacked with the intent to monitor and control partners, leading to domestic abuse. Unfortunately, with sextortion laws being a "hodgepodge of state and federal laws"[5], prosecution for these assaults is challenging when (and if) they can be attributed to an actor.

A 2018 IEEE article questioned who might be at fault in security violations, unsure if it was software or hardware manufacturer or the network provider. Consumers "expect that technical security is someone else's responsibility".[13] Yet despite the news about cybersecurity violations, consumers do not consider that a possibility for them, a someone else's problem mentality, leaving them vulnerable.

To recap the physical bad, IoT devices are manufactures with price as a driver and not consumer protection. Consumers accept the security risk with a "won't be me" mentality, thinking that hacks will occur to someone else, reinforcing Manufacturer behaviour. Prosecution of harm from a cyber-physical system attack is reviewed by multitudes of state and federal laws which were not designed to handle cyber-physical security incidences. In the end, consumers are at risk of cyber-physical harm from IoT devices with little opportunity to improve their product choices or prosecute the outcomes.

Physical Good

University College London's Gender and IoT project[6] explores "the implications of IoT on gender-based domestic violence and abuse". Devices that have been hacked with the intent to monitor and control their partners. The GIoT project seeks to provide research, education and collaborative solution-building to reduce the barriers to socio-technical issues such as the IoT revolution.[8] In addition, the world of IoT devices can lead to innovations in safety, with the topic being discussed at the University of Pune, India.[7]

From a consumer protection standpoint, California is leading the way with Oregon close behind. The California Consumer Privacy Act (CCPA) seeks to provide clarity on what is at stake. The CCPA articulates the power that companies have when collecting information on clients and acknowledges the potential for physical harm (emphasis added).

> *(f) The unauthorized disclosure of personal information and the loss of privacy can have devastating effects for individuals, ranging from financial fraud, identity theft, and unnecessary costs to personal time and finances, to destruction of property, harassment, reputational damage, emotional stress, and even potential physical harm.*

Moreover, the CCPA provides a definition for personal information (emphasis added).

> *(o)(1)"Personal information" means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following:*
>
> *(A) Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.*

The CCPA goes on to indicate that "reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action". "Reasonable security" is defined in the California IoT Law where a Manufacturer can find guidance as to what security features are legally required by them. [15] These are high-level features which, like most things dealing with law, are subject to interpretation. With the addition of IoT recommendations from the National Institute for Standards and Technology (NIST), hopefully Manufactures are getting the point.

NIST provides guidelines to industry for reasonable cybersecurity practices looking at the entire ecosystem of the product. The NIST recommendation (NISTIR) states the both Consumers and Manufacturers have a role to play in securing IoT devices but acknowledges that the Consumer may not be aware or have the skills to do so (emphasis added). [10] [11]

> *IoT devices are acquired and used by many customers: individuals, companies, government agencies, educational institutions, and other organizations. Unfortunately, IoT devices often lack device capabilities customers can use to help mitigate their cybersecurity risks. Consequently, IoT device customers may have to select, implement, and manage additional or new cybersecurity controls or alter the controls they already have. Compounding this, customers may not know they need to alter their existing processes to accommodate IoT. The result is many IoT devices are not secured in the face of evolving threats; therefore, attackers can more easily compromise IoT devices and use them to harm device customers and conduct additional nefarious acts (e.g., distributed denial of service [DDoS] attacks) against other organizations.*

NISTIR 8259 encourages manufacturers to consider their product from the consumer's point of view, from within their ecosystem. The recommendation contains 6 Activities that provide a good starting point for looking at how to protect an IoT device in situ.

Protecting the IoT

When looking to protect IoT devices, and especially within the aforementioned context, I started drafting up user personas, a technique I use quite often as a certified Scaled Agile Frame Product Owner. The Manufacturer and the Consumer have very different abilities, backgrounds and goals for the same product. This needs to be addressed so that cybersecurity problems – and solutions - can be viewed in context of the whole which can be quite different from the lab in which the device is created.

NISTIR 8259 provides 6 recommendations to consider for security devices, both pre- and post-market launch. The recommendation acknowledges the complex ecosystem in which IoT devices are present and stresses the opportunity for security improvements in pre-market launch of IoT devices upon the manufacturer. As of this writing, CPS lawsuits citing NISTIR 8259 (Draft 2 published in January 2020) has not been found online.

NISTIR 8259 provides activities and questions for the manufacturer to consider when considering launching an IoT device. They appear to be worthwhile to review with the specific implementation falling to the technical experts.

Activity 1: Identify Expected Customers and Define Expected Use Cases

This activity encourages Manufacturers to consider how the Consumer might use the product, physical location, technology ecosystem, etc. It also encourages consideration of how an attacker might attack the device. This would be a great area for technologists to dig in and provide recommendations about how and adversary might attack the device – within the use case. Considerations as to

- What does device do?
  - Research marketing material
  - Reverse Engineering
  - FCC submission documentation for anything that radiates (RF)
- How does it do it?
  - Review marketing material for technologies used
  - Reverse Engineering trial and error
- And how can we get control of it?
  - Port scans to determine what services are available
  - Explore security in data transmitted
  - Look at known hacks for each protocol in place
  - Start to send different commands and values to registers and ports
  - Rip apart the hardware and see if access can be obtained
    - This might not be a consideration as it probably does not fit the use case.

This specifically calls out the Consumer use case which I interpret to be the best case scenario. Adversaries are a creative bunch and can color outside the lines. Meaning that while the use case may have a physically limited range, the adversary can develop creative techniques that go outside that use case. Bring the CPS teams into the product design conversations early to help align the product design with CPS Principles.

CPS Principle	Part of Activity	How
Confidentiality	Yes	Recommendations from CPS team involvement
Integrity		
Availability		
Authentication		
Non-repudiation		
Veracity		
Plausibility		

Table 1: Activity 1 CIANAVR

NISTIR 8259 is still a recommendation which means that it does not require Manufacturers to implement any of their findings.

Activity 2: Research Customer Cybersecurity Goals

NISTIR states that consumers have a responsibility to secure their IoT devices and Manufacturers can make their devices "minimally securable" so that Consumers may be able to mitigate some cybersecurity risk. The extent to which is possible depends on the technical savvy of the Consumer as well as the cybersecurity measures implemented by the Manufacturer which is why Activity 1 is important (identifying the Consumer and the use cases). Consideration to authentication and availability of the device features are considered. Manufacturers are encouraged to consider how their product's features might be adversely impacted when security violations might occur.

Activity 2 is still a though exercise with decision making occurring in Activity 3.

CPS Principle	Part of Activity	How
Confidentiality	Yes	Recommendations from CPS team involvement
Integrity	Yes	Consider UI design so user cannot break it
Availability	Yes	How might a cybersecurity capability affect operations? How does the device fail?
Authentication	Yes	Through understanding of the data and where it resides
Non-repudiation	Yes	Considered in context of the device failing
Veracity	Yes	IoT devices interact with the physical world. Reliability, resilience and safety are discussed.
Plausibility		

Table 2: Activity 1 CIANAVR

Activity 3: Determine How to Address Customer Goals

This is a combination of the Manufacturer implementing cybersecurity measures that help to achieve the cybersecurity goals identified as important for the Consumer. This is where the Manufacturer looks at all the use cases, all the options, and decided what their device will

implement versus what other systems or the Consumer will implement. The recommendation provides a list of basic device cybersecurity capabilities and examples for the Manufacturer.

It is important to note that the effort for all activities to this point is on the Manufacturer side. That being the case, they are free to derive the use cases that suite them and use that as a framework for activities.

Activity 3 also discusses software/firmware updates. IoT devices are very difficult to patch and it is uncertain who has responsibility for creating an deploying patches. [14]

Activity 4: Plan for Adequate Support of Customer Goals

Hardware resources are planned appropriately to support the cybersecurity implementation of the Manufacturer. Questions about verifying software integrity and backtracking into software development methodology to prevent vulnerabilities from being introduced.

Consideration for bloatware is called out as a way to reduce risk exposure.

Activity 5: Define Approaches for Communicating to Customers; and

Activity 6: Decide What to Communicate to Customers and How to Communicate It

How to communicate with the Consumer in plain language so that they understand the cybersecurity implementations addressed by the product vs what is expected by the Consumer.

Activity 6 is when end-of-life and technical support are discussed here.

Further Research Ideas

In my research, I started to question how we arrived in a situation where technology was being used for sexual assault, which primarily affects women, and wondering where the nexus of power lies in the construction of the dynamics in play. With the use of IoT devices purported in women's abuse cases to children's toys being hacked to adult devices being hacked, how are we protecting the "rights of the weakest in society"?[12] How do socio-economic factors play in to the construction of this dynamic?

References

[1] Freytas-Tamura, Kimiko de. “Maker of ‘Smart’ Vibrators Settles Data Collection Lawsuit for $3.75 Million.” *The New York Times*, March 14, 2017, sec. Technology. https://www.nytimes.com/2017/03/14/technology/we-vibe-vibrator-lawsuit-spying.html.
[2] Top Class Actions. “Vibrator Maker Will Pay $3.75M to Settle Privacy Class Action,” March 13, 2017. https://topclassactions.com/lawsuit-settlements/lawsuit-news/534274-vibrator-maker-pay-3-75m-settle-privacy-class-action/.
[3] *DEF CON 24 - Goldfisk, Follower - Breaking the Internet of Vibrating Things*. Accessed May 9, 2020. https://www.youtube.com/watch?v=v1d0Xa2njVg.
[4] “Anti-Obscenity Enforcement Act.” In *Wikipedia*, April 17, 2020. https://en.wikipedia.org/w/index.php?title=Anti-Obscenity_Enforcement_Act&oldid=951434434.
[5] Engadget. “The Law Isn’t Ready for the Internet of Sexual Assault.” Accessed May 9, 2020. https://www.engadget.com/2017-05-24-sextech-hacking-laws.html.
[6] UCL. “Gender and IoT.” UCL Department of Science, Technology, Engineering and Public Policy, September 17, 2018. https://www.ucl.ac.uk/steapp/research/digital-technologies-policy-laboratory/gender-and-iot.
[7] Varade, Sayali, Tejshree Itnare, Harshada Parande, Pooja Sonawane, and Rakhi Bhardwaj. “Advanced Women Security System Based on IOT.” *International Journal on Recent and Innovation Trends in Computing and Communication* 5, no. 12 (n.d.): 5.
[8] Lopez-Neira, Isabel, Trupti Patel, Simon Parkin, George Danezis, and Leonie Tanczer. “‘Internet of Things’: How Abuse Is Getting Smarter.” *SSRN Electronic Journal*, 2019. https://doi.org/10.2139/ssrn.3350615.
[9] Keating, David, Jim Harvey, and Dan Felz May 2020. “A CCPA Private Right of Action on the Horizon.” LawJournalNewsletters.com. Accessed May 9, 2020. http://www.lawjournalnewsletters.com/2020/05/01/a-ccpa-private-right-of-action-on-the-horizon/.
[10] April 2020, Ashley Thomas. “States Take the Lead on Securing IoT.” LawJournalNewsletters.com. Accessed May 9, 2020. http://www.lawjournalnewsletters.com/2020/04/01/states-take-the-lead-on-securing-iot/.
[11] Fagan, Michael, Katerina Megas, Karen Scarfone, and Matthew Smith. “Recommendations for IoT Device Manufacturers: Foundational Activities and Core Device Cybersecurity Capability Baseline (2nd Draft).” National Institute of Standards and Technology, January 7, 2020. https://doi.org/10.6028/NIST.IR.8259-draft2.
[12] “The Bright-Eyed Talking Doll That Just Might Be a Spy - The New York Times.” Accessed May 9, 2020. https://www.nytimes.com/2017/02/17/technology/cayla-talking-doll-hackers.html.
[13] Sivaraman, Vijay, Hassan Habibi Gharakhelil, Clinton Fernandes, Narelle Clark, and Tanya Karliychuk. “Smart IoT Devices in the Home.” IEEE Technology and Society Magazine, June 2018.
[14] Stanislav, Mark, and Tod Beardsley. “Hacking IoT: A Case Study on Baby Monitor Exposures and Vulnerabilities.” *#IoTsec*, September 29, 2015.
[15] “Bill Text - SB-327 Information Privacy: Connected Devices.” Accessed May 11, 2020. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327.