Data Privacy Day **Carnegie Mellon University**

Privacy for IoT Devices

What is the "Internet of Things"?

The "Internet of Things" (IoT) is a shorthand to refer to the phenomenon whereby the decreasing cost of powerful networking hardware and sensors has led to the incorporation of connectivity and data acquisition to ever-greater numbers of devices. IoT devices can include:

- "smart home" devices such as Web-enabled thermostats, intelligent personal assistants, baby monitors, etc.
- "smart" Consumer Products such as SmartTVs, connected toys for children, location trackers (e.g. Tile), and many other innovative products, some not yet dreamed up!
- Internet-connected wearable devices such as fitness step-counters, medical heart-rate or other biosignal monitors, Lifelogging-capable hardware (e.g. Google Glass), etc.
- Automotive technologies such as OnStar, Tire Pressure Monitoring Systems, and numerous electronic control units (E.C.U.s) that manage interconnected parts of a car autonomously.

What are some privacy and security concerns with "Internet of Things" devices?

- **Tracking**: The Center for Democracy and Technology (CDT) and the Federal Trade Commission (FTC) have investigated a practice called cross-device tracking, whereby a device generates an inaudible sound (such as a TV broadcasting a TV commercial with this inaudible sound embedded) that can be received by various apps on IoT and mobile devices, and used to track a user's activities over multiple sessions on different devices [1]. The most prominent company in this space is called SilverPush. The CDT notes that advertisers could create detailed profiles of people not possible from collection from a single device, hypothesizing the scenario in which an individual searches for STD-related terms on their desktop, looks up nearby STD clinics on their mobile, and then visits that nearest location (perhaps while carrying their mobile or another location-broadcasting wearable); such cross-device tracking could enable an advertiser to assume, rightly or wrongly, that an individual received treatment for an STD [1].

- **Device Re-purposing**: Connected medical devices such as pacemakers may provide increased value by allowing remote doctors to monitor a patient's health for early diagnoses and preventive interventions. If a malicious user were to gain access to an unsecured device, however, they could re-program the device for any malicious purpose. Just looking at the pacemaker example, they could administer lethal shocks that could upset cardiac rhythm and cause a heart attack! This scenario has already been shown to be feasible by an ethical hacker who re-purposed demo pacemakers and made them give what would be lethal doses if the device were inside a person [2]. Connected car features have been hacked by academic researchers, some of whom have successfully hacked demo cars with remote unlock features and driven away with them, and others of whom have taken over a car's steering and braking system [3].

- **Botnet Assimilation**: Sometimes, overt re-purposing is not the goal of an attacker. Many devices are being compromised and simply being bundled together into "botnets" by attackers interested in creating Distributed Denial of Service (DDoS) attacks. When a machine is added to a botnet, it can be made to secretly send traffic to a target of interest to the attacker simultaneously with all of the other compromised machines in the "botnet;" the massive number of simultaneous requests causes the target's web server to overload and crash. With the proliferation of unsecured IoT devices, the scale of these DDoS attacks has grown to unprecedented levels and caused major disruptions. Most recently, a botnet was reported to have used a particular malware called Mirai to infect a vast numerous of unsecured IoT devices. It is surmised that this botnet was at least partially responsible for taking down the Dyn DNS service provider on October 21st, 2016, and causing service disruptions to major web services such as Amazon, Netflix, The New York Times, Reddit, Twitter, and more [4].

- **Surveillance**: The decreasing cost of security cameras, and practices such as lifelogging that are enabled by technologies such as Google Glass, are creating a society in which one can expect to be under the gaze of a camera in more and more settings. This can lead to what has been dubbed the "chilling effect," whereby individuals are inhibited from acting as they would were there no surveillance, and may have societal implications such as people engaging in self-censorship [5].

What are some things I can do to protect my privacy?

- **Smart Consumption:** Know Before You Buy! Be selective in the products you buy by including privacy criteria in your decisions.
- **Use Privacy Settings When Available:** Leading IoT companies incorporate privacy features that let you to control how your information is collected, processed, and shared: Learn if your products use them, and take advantage of them when they are available.
- **Adopt Security Best Practices, Within Reason:** Use usably secure passwords and not default passwords for your devices, update often and maintain good information security hygiene, give devices only as much data as needed for their purpose, opt for encryption when available, etc.
- **Stay Abreast of the Latest Privacy Developments:** Researchers and leading industry players are working hard on technologies to enable more usable control over the vast array of devices with myriad settings. Stay informed about these developments and adopt recommended practices to stay ahead while relieving your overhead!

[1] C. Calabrese, et al. "Comments for November 2015 Workshop on Cross-Device Tracking." *Center for Democracy and* Technology, 2015.
[2] J. Kirk. "Pacemaker hack can deliver deadly 830-volt jolt" *Computerworld*, 2012. Available at: http://www.computerworld.com/article/2492453/malware-vulnerabilities/pacemaker-hack-can-deliver-deadly-830-volt-jolt.html
[3] S. Checkoway, et al. "Comprehensive Experimental Analyses of Automotive Attack Surfaces." *USENIX Security Symposium*. 2011.
[4] B. Krebs. "DDoS on Dyn Impacts Twitter, Spotify, Reddit" *KrebsonSecurity*, 2016. Available at: https://krebsonsecurity.com/2016/10/ddos-on-dyn-impacts-twitter-spotify-reddit/
[5] H. Nissenbaum. *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press, 2009.