BIOGRAPHIES

About Kymberlee Price, Senior Director of Researcher Operations

With over 13 years experience in product security, Kymberlee Price pioneered the first security researcher outreach program in the software industry, was a principal investigator in the Zotob criminal investigation, and analyzed APT's at Microsoft. She then spent 4 years investigating product vulnerabilities in BlackBerry's Security Response Team. Today she is responsible for directing the efforts of Bugcrowd's global red team of more than 25,000 security researchers, optimizing vulnerability discovery and reporting for customers and researchers, and aiding 'the Crowd' with ongoing skill development and overall success in Bugcrowd programs. Ms. Price holds a Bachelor of Science degree in Behavioral Psychology and a Bachelor of Science degree in Public Health Education. She has previously spoken at a number of conferences, including Black Hat USA, RSA, Kaspersky Security Analyst Summit, Metricon, NullCon, and Derbycon.

About Jason Haddix, Director of Technical Operations

As director of technical operations at Bugcrowd, Jason trains and works with internal security engineers to triage and validate hardcore vulnerabilities in mobile, web, and IoT applications/devices. He also works with Bugcrowd to improve the security industries relations with the researchers. Jason's interests and areas of expertise include mobile penetration testing, black box web application auditing, network/infrastructural security assessments, and static analysis. Jason lives in Santa Barbara with his wife and two children. Before joining Bugcrowd Jason was the Director of Penetration Testing for HP Fortify and also held the #1 rank on the Bugcrowd leaderboard for 2014.

COMMENTS FOR NTIA:
ANSWERED BY JASON HADDIX

1. Are the challenges and opportunities arising from IoT similar to those that governments and societies have previously addressed with existing technologies, or are they different, and if so, how?

The technologies that IoT is comprised of (mobile, APIs, web servers, embedded devices, distributed cloud architecture, etc) have all had inspection in the realm of security. Some have fared better than others. For instance, web servers are significantly more secure than 10 years ago. The opposite case of mobile and API security leave much to be desired. When you combine these technologies into "IoT" you face a myriad of problems. In the private sector these devices are developed by manufacturers that have never been held to any security standards. They simply don't have a security review process and have been 100% focused on shipping a working product. These manufacturers are now being pushed into an "IoT" market and are connecting the devices to the internet with the same process. Undertrained and unaware manufacturers are leaving a decade of security learning behind. On top of this, these same manufacturers are simultaneously playing "catch up" in some of the other newer areas (mobile for instance). The pressure to ship a product is too high and their awareness too low, and there is no governing body policing the market with security concerns in mind.

a. What are the novel technological challenges presented by IoT relative to existing technological infrastructure and devices, if any? What makes them novel?

The sheer purview of the devices being networked and connected to cloud interfaces and on-the-internet APIs is one the of hardest facets of the problem. These connection points often are under-secured in the worst ways. Each product can also be massively distributed, making PII breaches almost a certainty. Each manufacturer handles their own development of these systems. Keeping in mind the resource problems outlined above, the challenge the industry faces is to create and regulate a standard that IoT companies must adhere to or implement a turn-key technological solution to the problem (which is unlikely given the diverse applications/devices of IoT). Another challenge is the physical aspect of security when it comes to IoT devices. Should they be held to a standard that requires not only protection from remote exploitation, but also having protections from reverse engineering a device that an adversary has physical access to? If so, the requirements become very high in the development and electrical engineering aspects of these devices/systems.

b. What are the novel policy challenges presented by IoT relative to existing technology policy issues, if any? Why are they novel? Can existing policies and policy approaches address these new challenges, and if not, why?

The challenge to implement a regulation, standard, or policy for the security of IoT devices is apparent when you start looking at the definition of "IoT". In the broadest sense of the definition you include devices from all private market verticals (and some public too). With this wide distribution, threat modeling a device and implementing broad security standards becomes hard to do. Should a pacemaker have the same standards as a baby monitor? Should a Fitbit (a health tracking wristband) have the same standard as a IoT thermostat? Or garage

door opener? What about a refrigerator? More scarily, what about a car? Or fourth generation Industrial Control Systems (SCADA)? Some existing efforts have been made to classify the devices by the confidentiality of data these devices handle. Even this proves to be troublesome with such a large diversity of devices. Any one of these market verticals has had trouble doing this (think automotive). Real security experts need to come together representing each vertical and devise such a policy.

c. What are the most significant new opportunities and/or benefits created by IoT, be they technological, policy, or economic?

The benefits are numerous. IoT puts us on the verge of a major technological revolution. Interconnection at scale, for everything. “Smart” cities, smart restaurants, improvement in personal health/healthcare, productivity, social interactions, social services, etc, are all subject to drastic improvements. Devices that enable these functions can be interconnected and talking to each other. A future where a virtual personal assistant can help run your life is no longer science fiction. There is no single “most significant” opportunity. Human quality of life will improve in many areas in a future where IoT has matured and been done responsibly.

ANSWERED BY KYMBERLEE PRICE

2. The term ‘‘Internet of Things’’ and related concepts have been defined by multiple organizations, including parts of the U.S. Government such as NIST and the FTC, through policy briefs and reference architectures. What definition(s) should we use in examining the IoT landscape and why? What is at stake in the differences between definitions of IoT? What are the strengths and limitations, if any, associated with these definitions?

As identified in the NIST definition of IoT, this field is an incredibly broad reaching term that encompasses subcategories of devices such as internet enabled children’s toys, household appliances, automobiles, industrial control systems, medical devices, and more. The strength of most IoT definitions is that it is easy to conceptualize what an IoT device is. But the limitation is the subcategorization which makes policy setting difficult for both the policy maker and the IoT vendor. The security risks posed by an exploited Barbie doll are very different from exploitation of an insulin pump, which makes blanket policy application ill advised.

Unfortunately, many internet enabled device manufacturers have not yet fully realized that they are now complex software vendors, shipping not only the embedded control system on a toy or vacuum, but frequently also managing mobile applications across multiple platforms, web applications, cloud storage, and web APIs. They have a responsibility to ensure product security throughout the life of the device. However, many IoT devices have poor software update mechanisms that compound the impact of design flaws and security vulnerabilities.

4. Are there ways to divide or classify the IoT landscape to improve the precision with which public policy issues are discussed? If so, what are they, and what are the benefits or limitations of using such classifications? Examples of possible classifications of IoT could include: Consumer vs.

industrial; public vs. private; device-to-device vs. human interfacing.

While all IoT vulnerabilities present information security risk, the most critical differentiation to be made is not whether a device is consumer or industrial, but whether or not it can cause bodily harm to humans if exploited. This factor ranges across vehicles, elevator controls, thermostats, power plants, medical devices and more. Loss of life is more critical than information disclosure in all real world scenarios, and must be defended at all costs.

17. How should the government address or respond to privacy concerns about IoT?

a. What are the privacy concerns raised specifically by IoT? How are they different from other privacy concerns?

IoT manufacturers are collecting large amounts of life pattern behavior on their users, as well as accessing home and work networks. This is a treasure trove of useful data for those that would target phishing attacks or product marketing, or pivot off these relatively insecure devices to compromise other systems on the network that contain more valuable data.

b. Do these concerns change based on the categorization of IoT applications (e.g., based on categories for Question 4, or consumer vs. industrial)?

Yes, critical infrastructure data leakage will result in different types of exploitation than consumer data leakage will cause.

c. What role or actions should the Department of Commerce and, more generally, the federal government take regarding policies, rules, and/or standards with regards to privacy and the IoT?

While this may be controversial, it is worth investigating implementation of HIPAA like compliance requirements on IoT vendor SDL processes to ensure appropriate precautions are taken to protect consumer privacy, with vendor liability consequences if not met and consumers are harmed as a result. Very few information security practitioners believe that compliance checklist-driven security programs are adequate, but they do create consistent and predictable baseline security requirements. When you look at the Hello Barbie situation, where privacy advocates raised concerns pre-release that were largely ignored by the vendor, and Hello Barbie was actively exploited… That could have been prevented.

--

[redacted]