Dupont Summit 2017

Science, Technology, and Environmental Policy

December 1, Historic Whittemore House, Washington, DC

Presentation
"Privacy and Security Issues with Internet of Things: Standards and Policies"

The term "Internet of Things" (IoT) was coined in 1999 by Kevin Ashton, who used it in a presentation at Proctor & Gamble to describe how physical objects in the company's supply chain can be accurately tracked by integrating two technologies: Radio Frequency Identification (RFID) and the Internet. Today, IoT is used to describe the myriad Internet-connected devices, such as home security monitors, utility management systems, kitchen appliances, smart televisions, baby monitors, fitness trackers, personal health monitors at home and in hospitals, and smart sensors on the roads and connected automobiles. An IoT system that monitors energy usage in a home, for example, will allow the home owner to change the thermostat setting, turn the lights on or off, and transform windows from transparent to opaque, all from a distance using a smart phone. An IoT home security system that connects to the Internet will likely be able call the police and alert the homeowner, when it detects an intruder. In industry, IoT devices, employed in diverse areas such as manufacturing, mining, agriculture and utilities to monitor and manage goods, equipment and their environment.

An IoT device or object, in short, is an embedded computer device. Because IoT devices are connected among themselves and with human operators, they can share information and make dynamic decisions on their own or assist humans to make decisions. This Internet connectivity better allows for decision making that is more integrated and symbiotic than decision making by individual devices or objects that lacks such coordination.

A 2015 Gartner, Inc. report forecasted there would be 6.4 billion IoT devices worldwide in 2016, up 30 percent from 2015, with the total projected to reach 20.8 billion by 2020. The 2016 growth would have required more than 4 million new devices be connected to the Internet each day. The revenue growth estimated by IDC is even more astounding: from $800 billion in 2017 to $1.35 trillion in 2021.

This massive and rapid upscaling and pervasiveness has profound implication for developing trustworthy, secure software for the devices. IoT devices, by their very nature are embedded devices, and as such, are often resource-constrained, and the market incentive is to devote resources to functionality to keep the cost low. Moreover, well-trained engineers and programmers with assurance and verification background to develop secure software for these hundreds and thousands of diverse IoT devices will continue to be scarce.

In 2014, HP Lab researchers examined the end-to-end security of 10 popular IoT devices and found that the security was dismal. They found that 70% of the devices are vulnerable to attacks! The researchers identified an average of 25 security vulnerabilities per device.

The security risks of IoT devices fall into three categories: (1) facilitating attacks on other system (e.g., use of IoT devices as cheap bots in Distributed Denial of Service attacks), (2) safety-related risks (as they control physical objects, e.g., insulin pumps, brakes in automobiles), and (3) unauthorized access and misuse of personal information.

An effective way to combat this poor state of cybersecurity is set of standards to be developed by the various stakeholders, in particular, vendors, consumer agencies and insurance companies. The security standards must be such that an average consumer can make an informed choice about safely and securely deploying and using a device in her home or place of work. The standards must address several areas of cybersecurity including user/device authentication, code authenticity, data protection, event detection and reporting, and policy management.

As IoT devices invade our home and healthcare, privacy will become a major issue. Device vendors, such as Samsung and Vizio, and service providers, such as Pepco and Con Edison, in their effort to make their devices or operations more efficient or our lives more comfortable, are in a position to collect information about our health and lifestyle and share that information with third parties. Samsung Electronics Company recently demonstrated a refrigerator that sends statistics and pictures of the food inside the refrigerator so you may order groceries remotely, say from work. The contents of your refrigerator—perhaps only beer and cured meat and no vegetables—can certainly be of value to your health insurance provider in determining your premium!

In general, IoT vendors and service providers may mine the information they collect and may share the raw and mined information with third parties, such as advertisers and health insurance providers. We will need privacy standards, perhaps industry-specific, for vendors on their disclosure obligations to owners and consumers on such items as:

- What functionality they intend to support through their data collection
- What data they need to collect to support those functions
- The third parties they will be sharing the data with
- Mechanisms available for the owner to correct erroneous information in the vendor's records
- How they will protect the information collected
- Dispute resolution mechanisms for the data being collected, stored and shared

- Opt-in and opt-out choices on the information collected

I will begin my talk with a brief introduction to IoT devices, and their pervasiveness and scale. I will then describe security and privacy challenges IoT devices pose. Addressing these challenges through standards and policies will then be focus of my talk.

Speaker
Balakrishnan Dasarathy, *PhDProfessor and Program Chair, Cybersecurity & Information Assurance Department Graduate School, University of Maryland University College*