MINTZ

Let's talk about Networks of Things, baby. Let's talk about you and me.

August 09, 2016 | Blog | By Julia Siripurapu, **Michael B. Katz**

VIEWPOINT TOPICS

- Privacy & Cybersecurity

RELATED PRACTICES

RELATED INDUSTRIES

It is easy to see networks all around us. The printers at the office, your child's videogame, the food ordering app on your phone, the fitness band or smart watch on your wrist, the electricity grid for your city, the self-driving cars being tested on our roads, all rely at least in part on networked solutions. The ubiquity of networks is already staggering and the pace of research and development in this area is poised to increase for years to come. As the things in our world get smarter and the network of these smart things grows larger, a little-known agency in the U.S. Department of Commerce, the **National Institute of Standards and Technology** ("NIST" or "Agency"), decided it was time that stakeholders smartened up about the way they discuss networks, connected "smart" things, and the privacy and security challenges associated with them.

The Agency recently released **NIST Special Publication 800-183** ("Publication") designed to offer a vocabulary and intellectual framework for thinking about *Networks of Things* ("NoT's"). To be clear, if the "smart" things being discussed are somehow connected to the Internet, you might hear someone refer to the *Internet of Things* ("IoT") when describing this web-enabled NoT. Our references to NoT's in this blog post are meant to capture both concepts.

The bulk of the Publication is focused on describing what NIST calls the five basic building blocks of NoT's or the "primitives":

1. **Sensor:** an electronic tool that measures physical properties and generates data;
2. **Aggregator:** a software tool that aggregates raw data from the sensor;
3. **Communications channel:** a medium that transmits raw data or aggregated data;
4. **eUtility:** a piece of software or hardware that receives and processes aggregated data; and

5. **Decision Trigger:** a mechanism that creates results in line with the purpose of the network.

The primitives are useful as a conceptual tool because they broadly apply to all NoT's and can facilitate precise and actionable discussion about network vulnerabilities and threats. "The vocabulary and science of the Network of Things," said Jeffrey Voas, an NIST computer scientist and author of the publication, "will help researchers understand how the components of IoT interoperate, and compare the security risks and reliability tradeoffs."

For example, a developer considering the adoption of automated temperature controls for its buildings will need to consider sensor and aggregator security to understand if an attacker could introduce fake data into the system and produce a harmful result (e.g., increasing the temperature in a room used for storing computers in order to disable the equipment). Or a manufacturer of "smart home" applications employing a security camera should focus on the integrity of components such as the communications channel and eUtility to make sure that a hacker could not intercept images collected from inside a home or conduct a denial of service attack sufficient to disable the whole system.

An IoT survey conducted by Enterprise Management Associates found that while 47% of the 351 organizations surveyed consider the IoT essential to their business, nearly 30% of these organizations are hesitant to use IoT due to the quality, reliability and privacy issues associated with such solutions. NIST acknowledges these are paramount concerns and articulates six additional elements that are "key players" in trusting NoT's:

1. the ***environment*** in which the network operates,
2. the ***costs*** and ***geographic location*** associated with the primitive components,
3. the ***owner*** of the network,
4. the ***device identifier*** connected to transmitted data, and
5. the notion of a "***snapshot***" or instant of time influencing the operation and output of a solution.

According to the Agency, these elements have a profound impact on the security of networked systems and should factor into any conversation about NoT's and consideration of NoT's.

One research firm predicts that the global market for web-enabled networked solutions could reach $1.7 trillion by the year 2020, and other experts believe that as many as fifty (50) billion devices could be connected to the Internet by that time. With a future so powered by networks, recognition in the present that our technologies are deeply vulnerable is hugely important. The Publication highlights the wide-ranging security and privacy concerns associated with NoT's and offers a model to help us discuss and troubleshoot the networks surrounding us. Now, it is incumbent on industry leaders, academics and the consumer public to pick up the conversation.

Authors

Julia Siripurapu

Michael B. Katz, Associate

Michael B. Katz is a Mintz corporate attorney who focuses on mergers & acquisitions, private equity transactions, and venture capital financings. He regularly assists clients with commercial contract negotiations, licensing agreements, and data privacy & security matters and advises startup and emerging companies.