Eric Gonzalez

Stephen Sebesta

ISACA Essay/Research Paper

October 19, 2016

The Challenges of Securing the Growing Internet-of-Things World

Today's world is full of incredible technology that we never imagined would ever exist outside of Hollywood movies. But in fact, these high-tech devices do exist and new ones are created seemingly every day. The data that these new devices create have been labeled the Internet-of-Things, that is, these everyday objects are now connected to the world-wide network and can send and receive data at an unprecedented rate. A simple wrist-watch seeming now has more computing power than many super computers did 30 years ago, our thermostats can tell manufacturers and energy companies how we heat and cool our homes, and even our cars are more software enabled than the metal and plastic that make up their frame. The challenges with these types of technological advances can be plentiful, including how and where to store all of the unstructured data that is being generated by these devices, how to analyze this information to make it useful to manufacturers, policy makers, governments, etc., and how to secure this information as well as the devices themselves from hacking-type attacks. This paper will take a deeper look into the growing need for security in an Internet-of-Things world.

The New York Times and Gartner Research forecast that by the year 2020 there will be approximately 20.8 billion devices that make up the Internet-of-things world. In fact, the market for these devices has increased in the last two years by 70% to over 6.4 billion devices. The types of devices cross every industry from farming and food production to healthcare, transportation, and energy consumption. One example, home automation, is one of the primary reasons I decided on a career in technology. My home has two Nest Thermostats controlling the heating and cooling, Wink in order to control lighting and other items throughout the home, Rachio sprinkler control for lawn irrigation and monitoring the overall health of my sprinkler system, Ring cameras and doorbell for home safety and security, and the list goes on-and-on. These devices allow me to control and monitor every aspect of my home using my smart-phone or a computer from anywhere in the world. The challenge though is, if I can do it, so could someone else if they were able to break into my home-network and compromise any or all of these devices. Security is extremely important not only for access into all of these devices but for the data that these devices contain about how I live my life. For example, if I open my garage door using an application on my phone each day at 8AM then not again until 5PM and this device was hacked, criminals would be able to use the data themselves or sell the information to others that there does not seem to be anyone at my home during these hours making it a prime target for a burglary.

Researchers at Level 3 Communications working in conjunction with the Pentagon realize that security of these devices are paramount and they think in new and innovative ways to enhance security. Organizations are going as far as creating contests with prize winnings in the millions of dollars to develop new automated defense systems to secure software vulnerabilities exploited by cyber-criminals. As a result of these contests, many firms began seeing attacks on websites using Internet-of-Things devices as their hosts rather than the traditional data center systems or home routers.

Dale Drew, CSO at Level 3 Communications, recommends that the very first thing one should do is change the default passwords on their devices, something simple but surprisingly not something everyone does. Also, passwords should contains letters and symbols that make it more difficult for people to gain access to the devices. Additionally, Drew recommends looking for devices that use an internet hub in order to control these devices as well as add an additional layer of security. For example, I use a Wink Hub in my home in order to control my lights, door locks, cameras, thermostats, and even my garage door opener. Wink uses several forms of security including certificate pinning, encryption, dual-factor authentication, and performs its own security audits to ensure they are using the latest advances in security technology.

Security of these devices themselves, though, is not the only concern. A device may have a complex design and the latest security technology securing the device itself, but if the company infrastructure is also not secure where the unstructured data created by the device lives, then none of this matters. The amount of data generated by these devices is creating a challenge in itself for each of these product companies. Traditional data types were easier to store because they were considered structured meaning there was some sort of organizational pattern to the data. Unstructured data is essentially just the opposite which means that traditional technologies used to store the data may not be suitable. As a result, there tends to be much more data which requires storage and encryption, new ways to analyze the data must be developed, and so on. All of these factors create new challenges for security in ensuring that the data is kept out of the wrong hands.

In today's economy, one of the biggest challenges for developers when it comes to security is time. Once a company comes up with a new idea for a product or feature, the countdown clock begins ticking and the need to introduce it to the market before their competition is critical. Security may be deemed "good enough" to be rolled out in the first version resulting in very minimal safeguards being included in the product release. Additionally, there is a shortage of the necessary skills needed in order to build the needed security into these new devices. The Cloud Security Alliance released a guidance report from their Internet of Things Working Group that stated that all device makers need to focus on 13 areas in creating IOT products and services:

1. Secure Development Methodology
2. Secure Development and Integration Environment
3. Identity Framework and Platform Security Features
4. Establish Privacy Protections
5. Hardware Security Engineering
6. Protect Data

7. Secure Associated Apps/Services
8. Protect Interfaces/APIs
9. Provide Security Update Capability
10. Implement Secure Authorization
11. Establish Secure Key Management
12. Provide Logging Mechanisms
13. Perform Security Reviews

All of the above steps are important but the group states that the most important step an organization can take is to regularly perform security reviews on their organization. Not only does this ensure that the company is staying on top of the latest and greatest technologies but it ensures the technology being developed is in fact safe and secure.

The challenges of the Internet-of-Things world is tremendous, that is, this is uncharted territory for many organizations. Taking traditional products and converting them into data-driven machines takes careful planning and countless hours of design and testing. As a result, it is important for consumers to research all of this technology and the companies that are releasing it in order to ensure that their information isn't compromised. But the responsibility of security is equally shared with the consumer in many cases meaning it is up to us to change our passwords regularly and make them more difficult to crack. If these simple safeguards are followed, there is no end to the technology that is out there to enhance our lives!

Bibliography

Lohr, Steve. "Stepping Up Security for an Internet-of-Things World." *The New York Times*. The New York Times, 16 Oct. 2016. Web. 18 Oct. 2016.

Tchuang@denverpost.com, By Tamara Chuang |. "Don’t Let Your Internet of Things Home Go to the Dark Side." *The Denver Post*. TAMARA CHUANG, 19 Oct. 2016. Web. 19 Oct. 2016.

By Working Together to Reinforce Existing Technologies and Develop New Ones-all While Sharing with the Community-we Hope to Make the Connected World Better for Everyone. "A Simpler Smart Home." *Wink*. Wink, n.d. Web. 22 Oct. 2016.

@BrightPlanet. "Structured vs. Unstructured Data - BrightPlanet." *BrightPlanet*. 9Clouds /wp-content/uploads/2016/05/BrightPlanet-site-logo-2-300x158.png, 09 May 2016. Web. 19 Oct. 2016.

GRIFFIN, JOEL. "Securing the Internet of Things | SecurityInfoWatch.com." *SecurityInfoWatch.com*. SecurityInfoWatch, 07 Oct. 2016. Web. 19 Oct. 2016.