ISC2 Virginia Peninsula Chapter

response to

NIST Request for Information number 2016-18948

Information on Current and Future States of Cybersecurity in the Digital Economy

September 9, 2016

The Virginia Peninsula ISC2 chapter is proud to provide the following in following recommendations and observations as they pertain to your focus questions for “Internet of Things”. We met as an organization on August 24, 2016 having invited students to provide perspectives ranging from High School, Undergraduate, and Graduate students as well as seasoned Cyber Security and Information Technology professionals.

Attendees

Thomas Harris, Chapter President, CISSP
Pat Stone, Chapter Treasurer, CISSP
Dr. William Lamarsh, Acting Vice President and Membership Chair, CISSP
Dr. Michael Collins, Member and Professor, Christopher Newport University, CISSP

Peninsula ISC2 Members
Christopher Newport University students

1. Current and future trends and challenges in the selected topic area

Manufacturers produce products based on consumer demand and, generally, people are not concerned with security in IoT. They prefer products that are easy to install and operate. They either don't care or are oblivious of the fact that simplification of settings typically destroys security. Coupled with the prolific nature of IoT devices and their ability to sense, monitor, log, and transmit wide swaths of data leads to loss of individual and societal privacy.

On a distinctly different note, the proliferation of devices also ensures in the future there will be greater interference between devices (and other technology) as more of the available wireless spectrum is consumed sensing, monitoring, and transmitting data.

2. Progress being made to address the challenges

Besides technical research and development, the biggest visible impact in addressing these issues is the legal requirement to notify affected individuals in the aftermath of a breach. Negative publicity alone is ample reason to avoid such situations, however the more direct impact of the cost of notification and credit monitoring ensures the C-suite pays attention to their exposure level (and therefore increases the likelihood of support for cybersecurity budget requests in quantities sufficient to at least show due diligence).

3. The most promising approaches to addressing the challenges

The most promising approaches offered were training and awareness, industry standards, and shifting liability.

Training and awareness should be focused on changing the perspective of the developer and the consumer. If developers were more aware of cyber principles and application then the trade-offs they make in design decisions would be better informed and thereby provide "baked-in" security when possible. Educated consumers could make informed decisions on product purchases, product installation, and product maintenance over its useful life.

Industry standards in development and testing is another recommended attention area. The group was split on whether the free market or the government should lead standards creation. Regardless who leads, standards should be created for independent testing methodologies (akin to Consumer Reports testing or UL Listing testing) highlighting cybersecurity in IoT devices.

Finally, changing liability would nudge the free market to improve their cyber security development requirements. Designing, building, or selling an insecure device leading to negative consumer consequence would expose companies throughout the supply chain to monetary and non-monetary damages depending on their level of control and influence over the development and delivery period of the product life-cycle. This could have the effect of improved open- and closed-source solutions and drive a culture change (supported by education and training).

4. What can or should be done now or within the next 1-2 years to better address the challenges; and
5. What should be done over the next decade to better address the challenges.

Near- to intermediate-term solutions include applying changing the paradigm on device security, improve education, and other innovative ideas.

To change the paradigm on device security the industry standard should be to provide devices fully locked down with a wizard to loosen security based on the individual user requirement or a self-aware device that searches the environment and recommends specific settings based on that context. Further, create different levels of security based on user-defined attributes. For example, a military application may require a highly secure device for resilience in austere conditions and contested environments where NOAA may only care that a device reads and transmits weather sensors hourly.

Education can be improved by providing more cyber training in information technology curriculum and pushing that curriculum to lower levels of education (potentially into primary and certainly into secondary education). To encourage students to enter the field, create more scholarships for cyber programs. Further, encourage outside training like the ISC2-offered "Safe and Secure Online" training.

Not all ideas are easily stratified into a particular category and therefore are offered together in bullets.

- Expand use of IPv6 to use built-in security to secure data transmission in the IoT
- As price points drop devices should become disposable and with the expectation that the embedded security will be sufficient for longer than the product will be considered viable
- Develop a standard for Internet Protocol address hopping (akin to frequency hopping in RF communications) to increase the difficulty of tracking data streams and to automatically shift to unused IP addresses in case of conflict
- Develop a standard for encryption key hopping (akin to frequency hopping in RF communications or IP hopping above) to increase the difficulty of decrypting data streams without the initial key and salt (or some other schema)
- Develop and support IoT "Hack-a-Thons" to identify weaknesses and encourage secure design
- Challenge legality of industry data collection and aggregation

6. Future challenges that may arise and recommended actions that individuals, organizations, and governments can take to best position themselves today to meet those challenges

Future challenges include both the ethical and challenges created by decisions made today as well as those made tomorrow with an eye towards short-term gains. While some of these ideas seem fantastic, the rate of technological growth has proven exponential and continues to increase in breadth and velocity.

Data collection through the internet of things will allow individual, discrete, and identifiable information to be collected, transmitted, stored, and analyzed at very low cost (the consumer buys and applies the technology rather than the company paying for the information). Further, the future of commerce involves autonomous delivery (drones, driverless cars, etc.) which require sensors and data collection and storage to improve algorithms, prove liability in accidents, etc.

While it may be argued that the aforementioned is a violation of individual privacy, it probably is not because the person whose information is collected either agreed to collection through a highly complicated an unnecessarily lengthy End User License Agreement (EULA) or it is collected in an area where the individual has no expectation of privacy.

This level of monitoring leads to big data and its storage and security issues. At some point the data set be saturated (i.e. information known about an individual is close, or it, a full data set ("perfect information")). What techniques will be employed to store and secure big data sets and at what point will the value of the aggregated exceed the holder's ability to secure it properly in the face of determined attackers. For example, a subset of the data will certainly be biometric data which can be coupled with answers to typical password reset questions. Using 3D printers (and like technology) biometric data based on a person's physical attributes can be recreated to defeat entry control systems (something you are). This could potentially be extended to near-cloning entire people given research funding and a database of DNA pairs and resulting attributes (gathered through observation) on a grand scale. Knowing personal historical data about a person (something you know) and having biometric evidence (something you are) effectively weakens three-factor identification to the point where it cannot be trusted except for the most trivial application.

Further, the types of technology for surreptitious monitoring attacks against individual and societal privacy exist and will continue to grow. Currently, users are routinely asked to give applications loaded to their mobile devices access to usage information and settings though in many cases the access is not required. While this attack is fairly pedestrian, it is conceivable that technology will advance to allow reading of brainwaves from greater distances and with greater accuracy and fidelity.

This collection and aggregation will almost certainly be used to create and maintain Orwellian Societies for despots around the world. While cliché, it is not a question of whether we can, but whether we should take certain courses of action.

In the United States specifically, the biggest challenge is the government keeping up with technology challenges in both policy and funding.

Other challenges in the next decade:

- Implications of Artificial Intelligence
- Security of IoT implants for human health and enhancement
- Friendly and enemy autonomous weaponry
- Autonomous vehicle security (cars, drones, etc.)
- IoT devices as appoint of unauthorized network entry (theft, espionage, etc.)
- Strong encryption protects innocent people from punishment for free thought but also challenges authorized searches in the United States and abroad