INTERNET OF THINGS (IOT) RISKS TAKE CENTER STAGE, WAVE OF INNOVATION WILL REQUIRE ENHANCED SECURITY

KEY ISSUE:

IoT Devices Take Center Stage as Vulnerabilities Exposed

Automobiles are a small part of a growing class of devices that are becoming increasingly complex and connected, building an ecosystem referred to as the Internet of Things (IoT). IoT devices represent a unique information security challenge because of legacy design constraints.

In July, Fiat Chrysler and Ford identified vulnerabilities in their automobiles. These vulnerabilities could not be mitigated through an online patch, but required either a recall or manual update. Some automakers rely on these expensive options while they look for innovative ways to update these devices.

- Fiat Chrysler Automobiles recently released a patch to their vehicles which required a download to a USB "thumb drive" to mitigate vulnerabilities associated with their Uconnect internet-enabled software system. This system provided access to a multitude of functions, including GPS, steering, transmission and braking systems. [1]
- On July 2, Ford announced a recall of over 400,000 automobiles in order to fix a software vulnerability that could prevent vehicles from turning off.
- In January BMW also announced that they found a vulnerability that would allow attackers to open car doors with their smartphone, although this patch was delivered remotely over the internet. [2,3]
- Veracode recently found vulnerabilities in a number of home devices that used poor inherent security design for passwords and traffic encryption. [4]

CHALLENGES AND OPPORTUNITIES:

IoT Innovations Poised to Reshape the Workplace

IoT represents an enormous benefit to society, and all industries are exploring how to leverage IoT as well as manage the new risks. According to Cisco and Telefonica, the growth of delivery of IoT devices will be 100 percent (from 25 to 50 billion) between now and 2020. [5,6,7,8]

- In terms of the number of IoT connections, Verizon has seen the following growth rates:
  - › A roughly 50 percent increase in energy;
  - › A 200 percent increase in manufacturing;
  - › A 45 percent increase in the public sector; and,
  - › An 80 percent increase in transportation. [9]
- Automakers are forming an Auto ISAC (Information Sharing and Analysis Center) to manage the new risks posed by these devices. The ISAC will rapidly disseminate information on these vulnerabilities and threats. According to USA Today, some auto manufacturers are investing in people and R&D to improve vehicle security. [10]

- The Department of Homeland Security warned last October that federal officials were investigating over 20 cases of security flaws related to medical devices. [11]
- Applications on IoT devices are hard to update because they were designed for low power consumption, processing power and human interaction. **Incentives are not yet aligned to force better application lifecycle management.** [12 13]
- In January, security technologist Bruce Schneier outlined why patching systems is a limited strategy for IoT devices for multiple reasons, such as: the inability to patch binary code, devices aren't typically engineered for patching, and a lack of alerting regarding the need for patches. [14]

THE PATH FORWARD:

Enable IoT Adoption by Providing a Higher Level of Trust

Take this opportunity to enable IoT when it becomes a part of business strategy. Users and consumers will need to build trust in these systems, and security strategy will remain a key component to building that trust.

Applied research teams have been tackling this problem for quite some time and work along side enterprise teams to support identification, remediation and design of systems to support that trust model. Enlisting outside perspectives is invaluable in determining what solutions will work best for a specific level of maturity.

A. *Challenging long-held assumptions*

- Specific misconceptions that should be challenged are:
  - "My devices are too simple to be exploited by an attacker."
  - "My devices are too old or too customized to be targeted."
  - "My devices are not capable of being updated, therefore there are no security controls at my disposal."
  - "The risks posed by my IoT devices are not as severe as other more traditionally connected machines, therefore these devices are a lower priority."
  - "My vendors are not delivering patches."

B. *Prioritize gaps in IoT security using threat modeling, starting with low impact devices*

Challenging these key assumptions will help identify gaps in risk mitigation that were previously overlooked. Ask the basic questions of risk management, even if only in a qualitative way:

A) "What is the likelihood that this device will be compromised?"

B) "If this device is compromised, what will be the direct effect on my business core functions?"

Threat modeling is essential to a successful IoT defensive strategy. Threat modeling will identify ways IoT devices can be attacked and compromised, and provide better input into your likelihood analysis as mentioned above.

C. *Address key gaps in security with people, process and technology*

People: Invest in IoT commensurate with your business model. Start by dedicating some portion of the security team's portfolio to this new class of vulnerabilities in order to maintain situational awareness. The assigned analyst should be familiar with the vulnerability management team . Enlist architects and engineers who understand the unique security needs, and testers who can develop strategies for IoT testing.

Process: Focus on low impact IoT devices that won't cause health and safety issues if you break them. Move on to higher impact devices once standard processes are more developed. Incremental change on specific devices that pose low impact to core business functions will likely be easier to initially implement into the vulnerability management program.

Technology: IoT devices are a fundamentally different type of device, and traditional endpoint and network security controls are insufficient. Security providers are responding to this by developing tools that address specific protocols used by IoT devices and enhancing device authentication. [15 16 17 18]

Security teams will be key to enhancing IoT adoption

The Internet of Things represents one of the most exciting waves of innovation of our time, with the potential to automate tasks in all industries and improve the quality of life for many.

The IoT ecosystem is made up of potentially expensive equipment with long life cycles, demanding that security design mitigate current and future threats. Threat modeling is essential to help ensure proper investment in security solutions. With proper planning, assessment and risk mitigation, the benefits of the IoT ecosystem will be realized and security will play a pivotal role in speeding adoption.

[1] Gibbs, Samuel. “Jeep owners encouraged to update their cars after hackers take remote control.” The Guardian. July 21, 2015. Retrieved from: http://www.theguardian.com/technology/2015/jul/21/jeep-owners-urged-update-car-software-hackers-remote-control?CMP=share_btn_tw

[2] Tom’s Guide. January 30, 2015. Retrieved from: http://www.tomsguide.com/us/hackers-unlock-bmws-remotely,news-20385.html

[3] Bomey, Nathan. “How easily can your car be hacked?.” USA Today. July 24, 2015. Print edition.

[4] Veracode. “The Internet of Things Research Study.” Veracode. April 2015. Retrieved from: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CB4QFjAAahUKEwiK2OLHy-7GAhUBz4AKHR2KAV4&url=https%3A%2F%2Fwww.veracode.com%2Fsites%2Fdefault%2Ffiles%2FResources%2FWhitepapers%2Finternet-of-things-whitepaper.pdf%3Fmkt_

[5] Federal Trade Commission. “Internet of Things: Privacy and Security in a Connected World.” January, 27 2015. p. i. Retrieved from: https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

[6] Evans, Dave. “The Internet of Things: How the Next Evolution of the Internet is Changing Everything.” Cisco. April 2011. p. 3. Retrieved from: http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.

[7] Paullin, Carlos Morales, et al. “Connected Car Industry Report 2013.” Telefonica. 2013. p.9. Retrieved from: http://websrvc.net/2013/telefonica/Telefonica%20Digital_Connected_Car2013_Full_Report_English.pdf

[8] HP. “Internet of Things Research Study.” HP. p.4. Retrieved from: http://h20195.www2.hp.com/V2/GetDocument.aspx?docname=4AA5-4759ENW&cc=us&lc=en

[9] Verizon Research. “State of the Market: The Internet of Things 2015.” Verizon. p.4.

[10] Bomey, Nathan. “How easily can your car be hacked?.” USA Today. July 24, 2015. Print edition.

[11] Kelley, Andrew. FTC: Security risks within ‘Internet of Things’ may require new industry regulations. January 28, 2015. Reuters. Retrieved from: http://rt.com/usa/227111-ftc-internet-things-risks/

[12] Wind River. “Security in the Internet of Things.” Wind River. Date. Retrieved from: http://www.windriver.com/whitepapers/security-in-the-internet-of-things/wr_security-in-the-internet-of-things.pdf

[13] Schneier, Bruce. “The Internet of Things is Widely Insecure and Often Unpatchable.” Wired. January 6, 2015. Retrieved from: http://www.wired.com/2014/01/theres-no-good-way-to-patch-the-internet-of-things-and-thats-a-huge-problem/

[14] Schneier, Bruce. “The Internet of Things is Widely Insecure and Often Unpatchable.” Wired. January 6, 2015. Retrieved from: http://www.wired.com/2014/01/theres-no-good-way-to-patch-the-internet-of-things-and-thats-a-huge-problem/

[15] Wind River. “Security in the Internet of Things: Lessons from the past to secure the future.” Wind River. January, 2015. Retrieved from: http://www.windriver.com/whitepapers/security-in-the-internet-of-things/wr_security-in-the-internet-of-things.pdf

[16] Verizon Research. “State of the Market: The Internet of Things 2015.” Verizon. p.20.

[17] Intel. “Intel Announces Expanded Choices in Silicon and Software for Gateways.” Intel. Retrieved from: https://www-ssl.intel.com/content/www/us/en/embedded/solutions/iot-gateway/overview.html

[18] IoT Analytics. “The Top 20 Internet of Things Companies Right Now.” IoT Analytics. February 24, 2015. Retrieved from: http://iot-analytics.com/20-internet-of-things-companies/

OPTIV

1125 17th Street, Suite 1700
Denver, CO 80202

800.574.0896 | optiv.com

Optiv is the largest holistic pure-play cyber security solutions provider in North America. The company’s diverse and talented employees are committed to helping businesses, governments and educational institutions plan, build and run successful security programs through the right combination of products, services and solutions related to security program strategy, enterprise risk and consulting, threat and vulnerability management, enterprise incident management, security architecture and implementation, training, identity and access management, and managed security. Created in 2015 as a result of the Accuvant and FishNet Security merger, Optiv is a Blackstone (NYSE: BX) portfolio company that has served more than 12,000 clients of various sizes across multiple industries, offers an extensive geographic footprint, and has premium partnerships with more than 300 of the leading security product manufacturers. For more information, please visit www.optiv.com.

8.15 | F1