Cooley

Congressional Hearings and NIST Publication Continue Focus on IoT Security

November 29, 2016

Two actions in the past few weeks reflect the continuing government involvement in and concern over the security of Internet of Things (IoT) devices. Attacks using connected devices have highlighted security vulnerabilities and led some witnesses at a recent House hearing to call for direct government regulation. House members, however, struck a more cautionary note, calling for greater coordination and adoption of best practices. Coincidentally, immediately prior to the House hearing, the National Institute of Standards and Technology (NIST) released best practices guidance for engineers developing IoT devices. Industry failure to adopt such practices will likely heighten regulators resolve to prescribe standards, especially if disruptive attacks continue.

IoT security hearing by the House Energy and Commerce Committee

On November 16, 2016, the US House Energy and Commerce Committee held a hearing to examine the role of the IoT in recent cyber attacks. The hearing follows in the wake of a number of distributed denial of service (DDoS) attacks that used armies of hacked IoT devices, such as webcams, baby monitors, printers, and DVRs, to interfere with or cause victims' computer systems to crash. The weak security on these everyday household devices allowed them to be compromised and used without the knowledge of their owners.

As summed up by Bruce Schneier, Lecturer and Fellow at the Harvard Kennedy School of Government, for the House Committee, IoT cyber attacks represent a fundamental market failure: "[Y]our security on the Internet depends on the security of millions of Internet-enabled devices, designed and sold by companies you've never heard of to consumers who don't care about your security…[T]he market has prioritized features and costs over security." Equating the emerging IoT landscape to pollution, Schneier encouraged the House Committee to take action: "[T]he only solution is to regulate. The government could impose minimum security standards on IoT manufacturers, forcing them to make their devices secure even though their customers don't care. [Doing so] would raise the cost of insecurity and give companies incentives to spend money making their devices secure."

It is estimated that 50 billion devices will be connected to the internet by 2020. As connected devices proliferate, the risk associated with them multiplies exponentially. Dale Drew, Chief Security Officer for Level 3 Communications told the House Committee: "The current lack of any security standards for IoT devices is certainly part of the problem that ought to be addressed. In particular, IoT manufacturers and vendors should embrace and abide by additional security practices to prevent harm to users and the internet. In this context, there may be a role for the government to provide appropriate guidance."

While expressing concern over the risks associated with connected devices, members of the House Committee were hesitant to endorse legislation as the solution, in part due to concerns over stifling innovation in this burgeoning industry. As stated by the Honorable Greg P. Walden, Chairman of the Subcommittee on Communications and Technology: "How do we make ourselves more secure without sacrificing the benefits of innovation and technological advances? The knee-jerk reaction might be to regulate the Internet of Things, and while I am not taking that off the table, the question is whether we need a more holistic solution."

NIST guidance for engineering trustworthy secure systems

The National Institute of Standards and Technology (NIST), which recently published guidance for securing interconnected devices, was promoted at the House Committee hearing as the author of a strong set of security

recommendations to which industry and government can look for guidance. The NIST Special Publication (SP) 800-160, Systems Security Engineering represent a holistic approach to creating trustworthy and secure systems, by encouraging the incorporation of engineering-based security design principles into the basic architecture and design of a system.

Three things about SP 800-160 should be immediately noted. First, at 257 pages, it actually represents a 50-page reduction from the second public draft for comment published in May of 2016. Second, the phrase "Internet of things" appears a total of one time in those 257 pages. Third, SP 800-160 represents only the sixth major NIST publication authored by Dr. Ron Ross, who has been described by NIST as "the father of the Federal Information Security Management Act (FISMA) security standards, a 'cyber rock star' and an international cybersecurity ambassador." The fact that Dr. Ross personally co-authored this publication indicates the importance of the topic. Given that SP 800-160 only mentions IoT once indicates another important aspect of the topic of cybersecurity – it must be viewed from a systems engineering perspective that encompasses "hardware, software, communications, physical, personnel and administrative-procedural safeguards."

The document states at the very beginning that it is meant to be used in a very flexible fashion, in order to meet the needs of a diverse set of stakeholders. Additionally, it is "not intended to provide a specific recipe for execution." Instead, readers should view it as a catalog of mechanisms for achieving a desired set of security outcomes based on a systems engineering approach.

To achieve its stated goals, Chapter Two of the publication begins with an overview discussion of the discipline of systems security engineering, including descriptions of a system, the elements of a system, and the associated environment. It then describes a system from a security perspective and introduces concepts that allow the system to be deconstructed into such things as the protection needs of the system, security relevance and architecture, trustworthiness, and assurance. Readers should keep in mind that all of this discussion of an overall system focus stems from issues echoed in the comments of Chairman Walden, mentioned above, regarding a holistic solution. Specifically, SP 800-160 states that "today's systems have dimensions and an inherent complexity that require a disciplined and structured engineering approach in order to achieve" a workable approach to securing those systems.

SP 800-160 then moves into the heart of the topic in Chapter Three – a discussion of the processes that define a system life cycle that leads to security. These include the agreement process, organizational project-enabling processes, technical management processes, and detailed technical processes. Clearly this is not a document to be consumed by just one type of stakeholder. For example, the agreement process described at the beginning of the chapter focuses on the supply chain issue, including sections on the acquisition process and the supply process. The legal agreement between the parties provides one particular area of focus in these two sections. The rest of this chapter focuses on the technical processes needed for securing systems.

Whether industry will step up to the challenge or government regulation will kick in remains to be seen. Ultimately, security will need to be addressed as the IoT continues to be rolled out. The communications and privacy & data protection practice groups at Cooley have highly complementary skills that uniquely situate the firm to help companies address the IoT and related issues. The communications group has a deep and sophisticated understanding of communications networks while the privacy & data protection practice group have technical expertise and substantial experience in assessing risks and responding to cybersecurity threats. We can help you understand the implications of Committee hearing on IoT, as well as the various related activities and how they apply to your organization.

This content is provided for general informational purposes only, and your access or use of the content does not create an attorney-client relationship between you or your organization and Cooley LLP, Cooley (UK) LLP, or any other affiliated practice or entity (collectively referred to as "Cooley"). By accessing this content, you agree that the information provided does not constitute legal or other professional advice. This content is not a substitute for obtaining legal advice from a qualified attorney licensed in your jurisdiction, and you should not act or refrain from acting based on this content. This content may be changed without notice. It is not guaranteed to be complete, correct or up to date, and it may not reflect the most current legal developments. Prior results do not guarantee a similar outcome. Do not send any confidential information to Cooley, as we do not have any duty to keep any information you provide to us confidential. When advising companies, our attorney-client relationship is with the company, not with any individual. This content may have been generated with the assistance of artificial intelligence (AI) in accordance with our AI Principles, may be considered Attorney Advertising and is subject to our legal notices.

Key Contacts

Randy Sabett **Washington, DC**	**rsabett@cooley.com** **+1 202 728 7090**
Lindsy Solanki Palo Alto	lsolanki@cooley.com +1 650 843 5220

This information is a general description of the law; it is not intended to provide specific legal advice nor is it intended to create an attorney-client relationship with Cooley LLP. Before taking any action on this information you should seek professional counsel.

Copyright © 2023 Cooley LLP, 3175 Hanover Street, Palo Alto, CA 94304; Cooley (UK) LLP, 22 Bishopsgate, London, UK EC2N 4BQ. Permission is granted to make and redistribute, without charge, copies of this entire document provided that such copies are complete and unaltered and identify Cooley LLP as the author. All other rights reserved.