DIGITAL FUTURES PROJECT

October 2017

Internet of Things Device Security and Supply Chain Management

By Stacia Lee and Jessica L. Beyer

From refrigerators (Brandom, 2016) to buildings, nearly everything in our everyday lives is connected to the Internet (Intel, n.d.). While the Internet of Things (IoT), provides valuable modern conveniences, it also raises new security concerns. Unlike rigorous national and international standards for aviation and automobile safety, or even an established "Good Housekeeping" seal for certain household products (Good Housekeeping, 2014) – there are no conventions dictating or communicating the security of IoT devices.

Currently, the average consumer has little choice but to equate the safety of their devices with the reputation of the company from which it was purchased. The foundation of this insecurity is supply chain vulnerability—and policies relating to electronic supply chain security at national level are lacking. In the absence of norms, whether they are federal law or merely international principles, connected Americans are unnecessarily exposed to risk that can and should be more efficiently managed.

However, developments at non-governmental and industry levels are a promising start toward greater resilience. International organizations relating to technology, such as the Open Group Trusted Technology Forum, are working with large technology companies to expand security certification programs, and the nonprofit organization *Consumer Reports* is

Wilson Center

THE HENRY M. JACKSON
SCHOOL OF INTERNATIONAL STUDIES
UNIVERSITY of WASHINGTON

slated to include privacy and security factors in its product reviews. Some companies, such as Microsoft, have made it a priority to secure their supply chain and communicate security guarantees to its consumers. And, a bipartisan bill has been introduced in the Senate that would regulate devices provided to the U.S. government. While there is considerable room for improvement in the way governments, organizations, and companies communicate and ensure supply chain integrity, there is also room to be optimistic for better security assurances in the near future.

Background

IoT devices collect sensitive personal data. This data is then sent to the cloud and big data centers, which are targets for digital criminals (Francis, 2017). Furthermore, a hack to just one WiFi-connected IoT device can provide access to multiple devices on one network (Brandom, 2016). When the IoT device in question has a camera, the feeling of insecurity becomes even more pressing (Korolov, 2016).

Device insecurities aren't outwardly apparent, and many go undetected. In 2016, security researchers discovered unknown actors were exploiting a backdoor built into over 700 million Android devices (Bing, 2016). The devices had been infected with malware and were quietly sending user data to a server in China. Malware is a serious security threat – malware has also been found on PCs before they were even shipped to consumers, suggesting that criminals accessed PCs during manufacturing and assembly (Associated Press, 2012).

A central component in creating such vulnerabilities are supply chains. A device is only as secure as its supply chain, and today information and communication technology (ICT) supply chains are vulnerable due to their internationalization. For example, the components of an iPhone are manufactured all over the world before converging in China or India for assembly (Costello, 2017). At each step in the construction process there are multiple opportunities for breaches. It is not difficult to imagine that, even given Apple's dedication to privacy and security, vulnerability could be added to an iPhone's software or hardware by one of Apple's various manufacturers.

Without security requirements for computers, mobile phones, and other products connected to the Internet in the United States, consumers are dependent on the security assurances of ICT companies when considering device safety. Meanwhile, although companies try their best to follow piecemeal governmental and industry guidelines for supply chain security, this vigilance is only as strong as a company's dedication to security.

National Initiatives

The 2008 Comprehensive National Cybersecurity Initiative suggests that the American government recognizes the great importance of managing risk stemming from global supply chains. However, federal attempts to successfully mitigate cybersecurity risk are minimal, resulting in limited policy that is reactionary instead of proactive and resilient.

The most successful policy initiative concerning supply chain security is the 2011 National Defense Authorization Act. The Act allows the Department of Defense, Energy, Army, Navy, and Air Force to exclude vendors without a hearing if they believe that vendors pose a security risk (Charney and Werner, 2011). The Act also requires supply chain risk to be included as an evaluation factor in the procurement process (Covington & Burling LLP, 2015). While this Act attempts to ensure the safety of electronics relating to national security, it needs to become far more proactive. It takes organizations around 146 days to detect breaches, meaning that a supply chain could already be breached but still in operation before the government identifies vulnerability and excludes it from its supply chain (Gerritz, 2016). Since vulnerabilities in the defense industry have very real security consequences for the United States, the Act could promote security more strongly by helping companies to secure their supply chains instead of waiting for insecurities to develop.

Shortcomings in national supply chain security most likely arise because cybersecurity issues are highly complex and difficult for policymakers and industry leaders to reach agreement upon. In 2014, two Congress members introduced the Cyber Supply Chain Management and Transparency Act (H.R. 5793). The Act would have mandated that security contractors provide a bill of all materials used in their products, including open-source software, and that each contractor demonstrates strong cybersecurity practices (Heaton, 2015). However, the Act never materialized due to pushback from contractors and national ICT leaders (Mance, 2016).

On August 1, 2017, a bill was introduced in the Senate called the Internet of Things Cybersecurity Improvement Act of 2017. The bill is a bipartisan effort that proposes certain requirements on any purchased government devices. Among other things, the bill requires that IoT devices are patchable, that they are free of known vulnerabilities, that devices use standard protocols, and that the devices are free from hardcoded passwords — among other requirements. The bill has not yet passed, but has received praise from security experts (Sterling, 2017).

There are no national policies that mandate digital supply chain protections in the private sector, but the Department of Commerce's National Institute of Standards and Technology (NIST) provides some guidance for industry to follow. In the past five years, NIST has developed a Cybersecurity Framework and published a paper on best practices in Cyber Supply Risk Management. However, since NIST is not a regulatory body, the recommendations made in each framework are completely nonbinding (Mance, 2016), although as of 2015, around 30% of American industry was utilizing NIST cybersecurity standards in their operations. Nevertheless, there is ample room for greater NIST framework adoption across the industry – a 2016 study cited by NIST suggests that 60% of surveyed companies do not monitor the security of their third-party vendors (Center for Responsible Trade & Enterprise, 2016). In essence, federal policy surrounding supply chain security is lacking, particularly as it pertains to the private sector and its civilian consumers.

Non-Governmental Initiatives

At a non-governmental level, some international organizations encourage dialogue to promote the optimization of supply chain cybersecurity across borders. While the guidelines produced by well-meaning international organizations are also nonbinding, they may signal the ascent of international norms surrounding device integrity.

The Open Group Trusted Technology Forum (OTTF), a working group comprised of universities and ICT companies, has produced a set of standards relating to supply chain security guidelines for ICT companies, called the O-TTPS V1.1 (The Open Group, n.d.). The OTTF also offers a certification program, in which suppliers and distributors can signal to business partners and consumers that their products have met certain safety standards (The Open Group, n.d.). With greater public awareness and industry adoption, the OTTF Certification program could easily become a way for users to manage digital risk when they adopt new technologies.

The International Organization for Standardization (ISO) has adopted the O-TTPS V1.1 as a standard for supply chain cybersecurity (The Open Group, n.d.). The ISO has also produced the Common Criteria for Information Technology Security Evaluation, which enables companies in each of the 26 participating nations to rigorously test their products against a set of rigorous security standards. Like the OTTF certification program, successful participating companies can receive certificates guaranteeing device security (Cisco, n.d.). The ISO is currently working to expand its Common Criteria and certification beyond finished products to each stage of a device's manufacture and assembly.

In the United States, *Consumer Reports* will begin including evaluations for data security in its product reviews. While *Consumer Reports* has always written about security breaches, its review system is an important evolution in the way consumers can learn to manage digital risk (Consumer Reports, 2017). Together with the nonprofits Ranking Digital Rights and The Cyber Independent Testing Lab, *Consumer Reports* is developing "The Digital Standard" for industry and consumers to follow; all cybersecurity reviews will be evaluated according to this new Standard (Consumer Reports, 2017). *Consumer Reports'* new cybersecurity reviews are poised to make a difference: as a trusted, independent authority with broad readership, *Consumer Reports* can broadcast important safety information to the general public in a way that highly technical organizations such as the OTTF and ISO cannot. Perhaps *Consumer Reports* can amplify the efforts of international organizations to certify secure practices to the general public and make such initiatives more commonplace.

Industry Initiatives

In the absence of significant national and international leadership, ICT companies are largely on their own to ensure the integrity of their products. While there many different ways in which a company can promote integrity, Microsoft serves as an example of a company using a multi-faceted, multi-sector approach to supply chain security.

Like most ICT companies, Microsoft utilizes internal security units to evaluate security at all stages of product development, manufacturing, and assembly. Some of Microsoft's internal security units focus on the technical aspects of integrity: their Digital Crimes Unit works to fight botnets disrupting critical infrastructure, while the Microsoft Security Development Lifecycle (SDL) monitors threats, and minimizes and eliminates software vulnerabilities that may occur at any phase in the development process (Microsoft Corporation, 2013). The SDL also subjects a product to a final security review before it ships (Storch, 2014). Microsoft complements its technical approach with non-technical programs such as the Global Procurement Group and Device Supply Chain Group, which ensure that all third-party inputs meet privacy, security, environmental, health, and labor standards (Microsoft Corporation, 2016).

Microsoft also places a strong emphasis on dialogue and cooperation with international organizations and within the industry. Its security standards complement standards set by NIST and the ISO (Microsoft Corporation, 2016), and Microsoft participates in organizations such as SAFECode, which work to promote enhanced security in the global software supply chain (Nicholas, 2009). Microsoft certainly isn't alone in its gravitation toward international cooperation – a handful of other technology giants participate in international discussions surrounding cybersecurity, perhaps suggesting a degree of industry convergence that could benefit consumers in subsequent years.

Conclusion

Electronics bring considerable convenience and considerable risk to our everyday lives. Since electronic insecurities are not always apparent or immediately detectable, it is extremely important for consumers to know that the devices they purchase and rely upon are safe. Device safety is the product of a highly complex supply chain, and maintaining supply chain integrity requires considerable vigilance from technology companies.

While a current lack of norms – national, international, or industry-led – governing standards in supply chain security can be troublesome for consumers, some consensus on security standards is emerging. At an international level, major ICT companies are participating in forums and organizations that promote security certifications that can easily be expanded and introduced to the public, perhaps through *Consumer Reports*' promising new cybersecurity review and standards system. Overall, while supply chain insecurity is currently one of the greatest sources of digital vulnerability, nascent collaboration between industry and non-governmental organizations provide a viable opportunity for companies and consumers to more effectively manage their digital risk moving forward.

Sources

Associated Press. (2012). "Malware Being Installed on Computers in Supply Chain, Warns Microsoft." The Guardian, September 14, https://www.theguardian.com/technology/2012/sep/14/malware-installed-computers-factories-microsoft

Bing, C. (2016). "Chinese-Authored Spyware Found on More than 700 Million Android Phones." Cyberscoop, November 15, https://www.cyberscoop.com/android-malware-china-huawei-zte-kryptowire-blu-products/

Brandom, R. (2016). "Samsung's Fridge of the Future Will Let You Check Spoilage from Your Phone." The Verge. January 4, http://www.theverge.com/2016/1/4/10707894/samsung-smart-refrigerator-connected-fridge-iot-ces-2016

Center for Responsible Trade & Enterprise. (2016). "NIST Cybersecurity Framework: The Supply Chain and Third Parties." CREATe.org. June 3, https://create.org/news/nist-cybersecurity-framework-supply-chain-third-parties/

Charney, S., and Werner, E. (2011). "Cyber Supply Chain Risk Management: Toward a Global Vision of Transparency and Trust." Microsoft Corporation, July 26, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REXXtT

Cisco. (n.d.). "Achieve Cyber Security with the Help of Common Criteria Certification," http://www.cisco.com/c/dam/en_us/solutions/industries/docs/gov/cyber.pdf

Consumer Reports. (2017). "Consumer Reports to Begin Evaluating Products, Services for Privacy and Data Security." Consumer Reports. Accessed March 7, 2017. https://www.consumerreports.org/privacy/consumer-reports-to-begin-evaluating-products-services-for-privacy-and-data-security

Costello, S. (2017). "Where Is the iPhone Made? (Hint: Not Just China)." Lifewire. Accessed March 13, https://www.lifewire.com/where-is-the-iphone-made-1999503

Covington & Burling LLP. (2015). "DoD Issues Final Rule Addressing Exclusion of Contractors That Present Supply Chain Risk in National Security System Procurements." Covington & Burling LLP, November 2, https://www.cov.com/~/media/files/corporate/publications/2015/11/dod_issues_final_rule_addressing_exclusion_of_contractors_that_present_supply_chain_risk.pdf

Francis, R. (2017). "Data Breaches through Wearables Put Target Squarely on IoT in 2017." CSO Online, January 3, http://www.csoonline.com/article/3150881/internet-of-things/data-breaches-through-wearables-put-target-squarely-on-iot-in-2017.html

Gerritz, C. (2016). "Breach Detection by the Numbers: Days, Weeks or Years?" Infocyte, July 27, https://www.infocyte.com/blog/2016/7/26/how-many-days-does-it-take-to-discover-a-breach-the-answer-may-shock-you

Good Housekeeping. (2014). "About the GH Limited Warranty Seal." Good Housekeeping, March 31, 2014. http://www.goodhousekeeping.com/product-reviews/history/about-good-housekeeping-seal

Heaton, B. (2015). "Will Open Source Security Be on the Federal Agenda in 2015?" Government Technology. January 8, http://www.govtech.com/security/Will-Open-Source-Security-Be-on-the-Federal-Agenda-in-2015.html

"H.R.5793 - 113th Congress (2013-2014): Cyber Supply Chain Management and Transparency Act of 2014," December 4, 2014. https://www.congress.gov/bill/113th-congress/house-bill/5793.

Intel. (n.d.). "Smart Buildings with Internet of Things Technologies." Intel. Accessed February 24, 2017: http://www.intel.com/content/www/us/en/smart-buildings/overview.html

Korolov, M. (2016). "Report: Surveillance Cameras Most Dangerous IoT Devices in Enterprise." CSO Online, November 17, http://www.csoonline.com/article/3142484/internet-of-things/report-surveillance-cameras-most-dangerous-iot-devices-in-enterprise.html

Mance, M. (2016). "Supply Chain Cyber Security." National Congress of State Legislatures, June 15, http://www.ncsl.org/documents/task_forces/0151_001.pdf

Microsoft Corporation. (2016). "Responsible Sourcing," Microsoft Corporation. October, https://www.microsoft.com/en-us/about/corporate-responsibility/responsible-sourcing

Microsoft Corporation. (2013). "Supply Chain Security." Microsoft Corporation. February, https://www.google.com/url?sa=t&url=http%3A%2F%2Fdownload.microsoft.com%2Fdownload%2FB%2F8%2F2%2FB8282D75-433C-4B7E-B0A0-FFA413E20060%2Fsupply_chain_security.pdf&usg=AFQjCNHJoz-Lv_X5qmPnKF9qklybitPpkg

Nicholas, P. (2009). "Working with SAFECode to Help Secure the Software Supply Chain." Microsoft Secure Blog, July 22, https://blogs.microsoft.com/microsoftsecure/2009/07/22/working-with-safecode-to-help-secure-the-software-supply-chain/

Sterling, B. (2017). "Spime Watch: the fact sheet for the Internet of Things Cybersecurity Improvement Act of 2017." Wired. August 11, https://www.wired.com/beyond-the-beyond/2017/08/spime-watch-fact-sheet-internet-things-cybersecurity-improvement-act-2017/

Storch, T. (2014). "Toward a Trusted Supply Chain: A Risk Based Approach to Managing Software Integrity." Microsoft Trustworthy Computing. https://www.slideshare.net/d501159/toward-a-trusted-supply-chain-white-paper

The Open Group. (n.d.). "The Open Group Trusted Technology Forum," http://www.opengroup.org/getinvolved/forums/trusted

The Open Group (n.d.). "The Open Trusted Technology ProviderTM Standard (O-TTPS) Certification Program," http://www.opengroup.org/certifications/o-ttps

DIGITAL FUTURES PROJECT

October 2017

Stacia Lee

Stacia Lee received her B.A. in International Studies from the University of Washington's Jackson School of International Studies. She is a Cybersecurity Policy Fellow with the International Policy Institute's Cybersecurity Initiative and a law student at the University of Michigan.

Jessica Beyer

Jessica Beyer is a lecturer in the University of Washington's Jackson School of International Studies and co-directs the International Policy Institute's Cybersecurity Initiative.

The Wilson Center

🌐 wilsoncenter.org

f facebook.com/WoodrowWilsonCenter

🐦 @TheWilsonCenter

☎ 202.691.4000

Digital Futures Program

🌐 wilsoncenter.org/program/digital-futures-

✉ projectdigitalfutures@wilsoncenter.org

f facebook.com/WilsonCenterDFP

🐦 @WilsonCenterDFP

☎ 202.691.4002

Woodrow Wilson International Center for Scholars
One Woodrow Wilson Plaza
1300 Pennsylvania Avenue NW
Washington, DC 20004-3027

THE HENRY M. JACKSON
SCHOOL OF INTERNATIONAL STUDIES
UNIVERSITY of WASHINGTON

Wilson
Center