Cybersecurity Approaches for The Internet of Things

David A. Schroeder

University of Wisconsin–Madison; United States Navy

20 February 2017

Table of Contents

"Internet of Things is shorthand for Internet of Things

That Should Not be Connected to the Internet." — Scott Manley

1. Introduction

The "Internet of Things", or "IoT", is a general reference to the range of devices other than traditional computing systems and personal communication devices that are connected to the internet. The IoT is made up of devices like household appliances, clocks, vehicles, so-called "smart meters", personal medical devices, security systems, cameras, smart light bulbs, wearables, and more — almost any electronic device with which humans interact now has a "connected" version intended to increase convenience, utility, or functionality. Once connected to the Internet, these devices become part of the Internet of Things.

The main cybersecurity issue with the IoT is that the devices typically run embedded or custom operating systems in configurations that are not easily patched, updated, or changed by the end user, due partly to a drive to reduce costs for such devices. (Schneier, 2014) This means that while computers and phones get routine software updates and security patches, devices that are part of the IoT may have vulnerabilities that will stay with them, and their owners, for their lifetimes — and can be used to attack or exploit other devices. (Tucker, 2016b)

Security researchers have already demonstrated how anything from a vehicle to a coffee maker can be hacked remotely, usually because of insufficient security measures that often cannot be easily changed after the item has been purchased. (Schneier, 2016b) Intelligence agencies envision a time where ubiquitous connected devices — especially anything with a camera, microphone, or sensor of any sort — can be used for espionage and intelligence gathering. (Tucker, 2014) The unabated growth of the Internet of Things presents major new challenges for personal, enterprise, and global cybersecurity.

2. IoT Security Challenges

The Internet of Things is expected to exceed 20 billion unique devices by 2020. (Stavridis & Weinstein, 2016) the IoT ecosystem becomes a formidable landscape in which attackers and malicious actors can operate. Admiral James Stavridis (2016), active in government cyber policy, observed, “the barriers to entry are becoming low enough that hackers no longer need the backing of a government to carry out crimes or even acts of warfare in cyberspace.”

This represents a troubling shift, with potentially destabilizing attacks no longer requiring the type of resources or support typically associated with nation-states. Just when the environment of traditional computing and mobile devices has come to grips with the reality that deliberate security by design is a priority — in large part because it has been demanded by the marketplace — the IoT threatens to upend that progress, and the integrity of the internet itself.

Because of the nature of IoT devices, many are designed to be “always on” and “always connected”, even when not in use. Depending on the device and the application, IoT devices employ various wired and wireless connectivity technologies such as Ethernet, Wi-Fi (802.11), Bluetooth, Near-field Communication (NFC), wireless mesh networks (WMN), mobile wireless networks (e.g., GSM), Radio Frequency Identification (RFID), cloud connectivity, or a mixture of two or more of these technologies. Each of these is a vector for attackers. (Rose, 2013)

Many IoT devices are also mobile and move with or without the user, such as vehicles or drones; small, such as cameras or baby monitors; or both, such as smart watches or fitness monitors. Others are stationary, but always connected, such as appliances, set-top boxes, or home security systems. Network security measures can provide a partial defense against initial attacks, but the mobility and sheer numbers of devices mean that compromised devices can easily enter secure enclaves, such as corporate networks, effectively bypassing standard security controls.

3. IoT Security Approaches

The functionality and usefulness of IoT devices to their users depend not only on their near-constant availability and connectivity, but also their *inter*connectivity. Unlike conventional "endpoint" devices such as a computer or mobile device, IoT devices often are designed to communicate more broadly with each other and the world of other connected devices around them — for example, by automatically connecting to available wireless networks, or to each other. (Vinel, Chen, Xiong, Rho, Chilamkurti & Vasilakos, 2016)

This allows novel new applications of technology — for example, a "smart building" that understands the number and location of its occupants at any time, and adjusts lighting and environmental controls accordingly; a self-driving car which communicates with traffic systems as it navigates a roadway to understand traffic flow or be notified to potential dangers that lie ahead; or a medical monitor which automatically alters a hospital or other healthcare provider of a problem in real time. (Vinel *et al*, 2016)

Contemporary cybersecurity approaches largely involve protection of systems and networks in known or predictable locations using authentication and authorization (AuthN/Z) via user- or system-based access controls, firewalls and intrusion detection systems, and similar. A typical home-based security model may simply involve a single router's firewall capabilities and the username and password-based authentication for connected devices to protect the network and devices from unauthorized access or use. (Niu, Jin, Lee, Sandhu, Xu & Zhang, 2016)

However, the nature of IoT requires a new and more dynamic approach to cybersecurity of this ecosystem, and security researchers have begun investigating approaches for security design, as well as techniques to secure existing devices. A sampling of these emerging technological solutions and other approaches will be reviewed in the forthcoming sections of this paper.

3.1. Cybersecurity Technologies

Cybersecurity research in this field is in its infancy, but novel approaches to the problems unique to IoT are being explored in literature. Most approaches focus on the necessity for security by design in IoT devices, networks, and infrastructure, and require a cooperative approach and buy-in from manufacturers. The primary challenges of IoT security is that many devices are designed to be as inexpensive as possible, and many IoT vendors have not been compelled to make security a priority; the answer may ultimately lie in a combination of market forces, industry and government responses to serious IoT cybersecurity events, and regulation.

Trustworthy crowdsourcing. For IoT devices designed to automatically detect, discover, and connect to one another, researchers have proposed a notional trust architecture for these "social IoT" (SIoT) devices, based on crowdsourcing. A combination of user feedback and automated mechanisms is utilized in conjunction with the social cloud to identify devices which are not trustworthy, with the social crowdsourcing component providing real time feedback to the larger social cloud network. This mechanism assigns levels of "trust" and identify rogue or malicious devices faster than automated controls alone. (Wang, Qi, Shu, Deng, & Rodrigues, 2016)

End-to-end biometrics-based security. The explosion of ubiquitous connectivity for IoT devices presents unique challenges for authenticating authorized users. Two-factor authentication supported by traditional usernames and passwords and a second factor is not reliable or efficient enough for many IoT applications. A mulit-layered security model is proposed to utilize unique biometric traits along with pairing-based cryptography to provide secure and easy-to-use security for IoT devices upon initial configuration and subsequent use. The authorized user must present these biometric traits for the device to function. (Hossain, Muhammad, Rahman, Abdul, Alelaiwi, & Alamri, 2016)

Dynamic tunneling and mobile IP management. Researchers have suggested that the explosion of IoT devices have ushered in the "post-PC era, in which mobile computing devices such as smartphones and wearables are used more than PCs." (Lee, 2016) A security scheme is proposed to use Proxy Mobile IPv6 (PMIPv6), an existing standard for network management of mobile devices, along with authenticated, dynamic tunneling to enable secure, end-to-end mobile device connectivity while retaining the usability benefits of PMIPv6. (Lee, 2016)

Location-based controls. The mobility of many IoT devices also present novel security challenges. One solution is location-aware devices, or the networks that serve them, which enable or disable devices — in whole or in part — depending on the nature of the device, and their physical location. Further, when location services are in use, there is also a need to protect the privacy of location data. An approach is proposed to allow for the obfuscation and pseudonymization of identifiers unique to a device, thereby concealing the identity of specific devices on the network, while still allowing the network to manage access and security. (Kang, Yu, Huang, Jonsson, Bogucka, Gjessing, & Zhang, 2016)

Distributed access control frameworks. Because of the sheer numbers of devices, and considering the exhaustion of IPv4 addresses, IPv6 is considered the realistic solution to enable unique addressing and interoperability requirements of IoT devices. However, connectivity is only one piece of the puzzle. Security researchers propose a distributed access control framework model in which connected subordinate devices dynamically inherit appropriate access in a hierarchy based on parameters established by the network operator. Access is dynamically granted or revoked based on network load, security requirements, or other conditions. (Li, Chai, Chen, & Loo, 2016)

Quantum cybersecurity. Current common cryptographic systems rely on technologies that can be easily defeated with upcoming advances in quantum computing. Approaches are required that implement new cybersecurity systems that are resistant to both classical and quantum attacks. Because cryptosystems are resource intensive, IoT devices face unique challenges, as many such devices often are physically small, or are designed to consume as little power as possible — both of which present problems for strong cryptography. New research provides some solutions for cryptographic schemes suitable for the often-constrained environments of IoT devices. (Cheng, Lu, Petzoldt, & Takagi, 2016)

Localized "kill switches". The notion of a network "kill switch" is related to, but separate from, core IoT cybersecurity issues — even if it is rogue or insecure IoT devices that are the catalyst of or enabler for an attack. Regardless of the mechanism of the attack, enterprises may choose to develop an ability to selectively or completely disable network access in the event of a cyberattack or other adverse event, implement procedures for when to act, and identify personnel empowered to make the decision. (Daly, 2014) This measure may give an organization time to mitigate the attack and begin remediation, and does not rely on technology in IoT devices.

These examples are just a few of the forward-looking approaches being explored for the security of the IoT ecosystem. None have yet been implemented in a meaningful way outside of narrow applications; many are theoretical or notional in nature. This point is important enough to be repeated: IoT devices are largely designed and treated as conventional "endpoints" on the internet, but with a host of new vectors for attack. (Ho, Leung, Hosseini, Song, & Wagner, 2016) Traditional cybersecurity approaches and controls have proven a minimal deterrent at best. Ultimately, a regulatory approach may be required to compel adoption of future accepted baseline cybersecurity measures. (Schneier, 2016ab; Washington Post Editorial Board, 2016)

3.2. Security in Practice

While there are billions of IoT devices, the IoT cybersecurity landscape is in its infancy as of this writing. Network providers, businesses and enterprises, and government organizations are largely managing IoT devices as they manage conventional endpoints. As such, the nascent discussion in the cybersecurity community with respect to IoT is largely a "call to action" directed at those who have influence with IoT device design, implementation, and purchasing. (Ahlmeyer & Chircu, 2016)

The primary issues with IoT lie in a combination of the mobility, interconnectedness, rapid growth, consumer apathy, and the security design — or lack thereof — of IoT devices. The marketplace has demonstrated a clear and increasing demand for the utility and convenience IoT devices offer, without a commensurate demand for the security of these devices, and network operators and organizations have no choice but to respond pragmatically to security concerns. The reality is that the growth of IoT has exceeded our ability to adequately defend it. (Greenemeier, 2016)

Current security mitigation for IoT devices typically involve network-level access controls disallowing unauthorized devices from connecting to the network. This prevents IoT devices themselves from connecting, but many IoT devices are paired or associated with another device that may itself be authorized, such as a computer or mobile device. One example of this would be a smart watch that is paired with the user's mobile phone — if the IoT device is compromised via other means, that can provide a vector that allows an attacker to compromise a device and then move laterally within target networks to which the user has access. (Tucker, 2016a) It is the same challenge faced by organizations dealing with mobile devices, exacerbated by additional vectors of attack enabled by the IoT device. (Niu *et al*, 2016)

3.3. Security Case Study

IoT has enabled significant attacks on scales not previously possible, except via nation-state level actions, or only partially possible with sophisticated attacks against traditional computing devices. The numbers of similar devices with security vulnerabilities opens a whole new world for attackers, in which anyone from terrorist organizations to hobbyist hackers can create significant impacts.

Distributed Denial of Service (DDoS) attacks. In 2016, a massive network of over 150,000 IoT devices compromised by IoT botnet code known as Mirai demonstrated DDoS attack capabilities exceeding 1 terabyte per second (Tbps). (Hill, 2016) Initially, this attack was aimed at security researcher and journalist Brian Krebs, known for detailed articles revealing the identities of malicious hackers involved in these very activities. But in October 2016, the same botnet was used to attack core internet DNS infrastructure belonging to Dyn, causing a nationwide, multi-hour partial outage impacting Twitter, Spotify, Netflix, Reddit, the *New York Times*, Pinterest, PayPal and other major sites. (Conditt, 2016)

In November 2016, a new, another IoT botnet called Linux/IRCTelnet, based on another botnet known as Aidra, was detected after it had infected 3,500 new devices in just five days. (Goodin, 2016) In this case, the malware does not have "persistence", in that it only resident in a device if it has power, or until it is restarted. But the command and control (C&C) server keeps track of the IP addresses of devices it has infected, and will reinfect them as soon as the device regains contact. This kind of high infection rate is driven by the insecure default configurations — some of which cannot be secured by any means — or default usernames and passwords of targeted IoT devices. These attacks and infection rates enable "assaults … capable of delivering malicious data in volumes that were almost unimaginable just a few years ago." (Goodin, 2016)

Unpatchable, insecure IoT devices. Cybersecurity researchers have written extensively about the nature of the devices that are enabling this worrisome new era of vulnerability and attacks. In the case of DDoS attacks, this is not an inherently new attack mechanism, but rather the scale, scope, and impact of the attacks that are enabled via IoT. In the case of the attack on Brian Krebs — which exceeded 650 megabits per second (Mbps) and forced content distribution network provider Akamai to stop providing services for Krebs' web site — the attack used "CCTV cameras, digital video recorders, home routers, and other embedded computers attached to the internet as part of the Internet of Things." (Schneier, 2016a)

Security researchers have already demonstrated the ability to remotely commandeer Internet-enabled vehicles, deployed ransomware against the users of Internet-enabled smart thermostats, taken over networks of smart light bulbs with drones, and shown remote vulnerabilities in health monitoring devices and even implanted medical devices, in addition to higher profile targets such as voting machines and power plant equipment. (Schneier, 2016b) These kinds of attacks can enable destruction of property or equipment — seen with the employment of *Stuxnet* against the Siemens microcontrollers attached to centrifuges of Iran's nuclear program — or even loss of life. (Schneier, 2016b)

Hundreds of device vendors, many based in China, make thousands of IoT devices, sold to end users by the millions, with little to no effective security controls, which will be around for years or decades. Many of these devices are vulnerable either because of inherent technical vulnerabilities, hard-coded or default usernames and passwords, or lack of even basic security for connections to or from the networks around them. There is no comprehensive catalog of these devices or their security status, but the most important takeaways for IoT devices are these: if possible, update or patch the device; and if possible, change its default passwords. (Krebs, 2016)

4. Government Efforts

One significant feature of this problem with IoT security is that device owners typically don't care about the security of these devices, because *they are not affected* — the device is cheap, appears to function to the user, and that's all that matters. Users want "a webcam — or thermostat, or refrigerator — with nice features at a good price. Even after they were recruited into this botnet, they still work fine — you can't even tell they were used in the attack." (Schneier, 2016b)

Traditionally, cyberattacks have directly impacted the user or organization that owns the device in an adverse way. Major incidents of personal or organizational financial loss, data theft, identity theft, legal liability, loss of consumer confidence, and similar, have led to the market demanding that technology vendors think about cybersecurity measures and principles when designing their devices. The market demanded, and vendors supplied.

For commodity operating systems like Windows, macOS, iOS, and Android, this has resulted in a stable and reasonably secure ecosystem. But no similar demands have been made of IoT vendors, and as such this universe of devices remains insecure. (Rose, 2013) Security researcher Bruce Schneier argues this state of affairs represents a market failure, and that legislation is required. (Schneier, 2016b)

Schenier argues the problem is twofold: the lack of security expertise on the teams involved in designing inexpensive IoT devices, because the market won't stand for the additional costs required to design secure devices; and neither the seller nor the buyer care that the device may be insecure as long as it works (or appears to work) as advertised. Schneier calls these networks of insecure and compromised devices a form of "invisible pollution," and that, like pollution, "the only solution is to regulate." (Schneier, 2016b)

4.1. Regulatory Approaches

A regulatory approach calls for government rules — in the form of legislation or regulatory rule-making via bodies like the Federal Communications Commission (FCC) — that impose minimum cybersecurity standards on IoT devices. A rules-based standardization approach would force vendors wishing to sell products into the US market to conform to baseline cybersecurity and other technical standards, even though the buyers of those devices still may not care about the details — and end users should not have to care, or worry whether their connected kitchen appliance will be used in an attack against a hospital across the country.

Regulations could also impose liability on manufacturers, allowing victims of cyberattacks to file lawsuits for damages against companies whose devices are used in attacks. These approaches utilize regulation, rather than market forces alone, to increase the costs to vendors of designing and selling insecure devices. While such an approach by the US government may only impact devices sold in the US, the size and nature of our market would force vendors to comply if they wish to sell into this market. The US can be a global driver of this solution.

4.2. Legislation

After several years of failed attempts, only by placing cybersecurity legislation in the FY16 omnibus approriation bill did any form of cybersecurity legislation become law in 2015. (Bennett, 2015) The Cybersecurity Information Sharing Act (CISA) is focused mostly on national and enterprise level cyber information sharing, and while some of its provisions may help the United States detect and respond to damaging attacks, the result is largely reactive. If there is loss of life or significant propery destruction from IoT attacks, the government may be compelled to act — but we should think about the implications of acting in haste, as opposed to having a deliberate and deliberative conversation about IoT cybersecurity.

5. Conclusion

The IoT security landscape is disjointed and in many cases virtually nonexistent, as implemented across the whole of the ecosystem. Unique factors of IoT devices such as miniaturization, low power requirements, size, portability, and more, along with ubiquitous presence in kitchens, bedrooms, bathrooms, living rooms, office complexes, power plants, government buildings, vehicles, and even inside our own bodies, create a challenging landscape for cybersecurity.

Governments, too, have taken notice of the promise of IoT — along with criminal hackers and terrorist organizations. Intelligence agencies are seeking ways to exploit IoT devices themselves (Tucker, 2014), while worrying how transnational terrorist actors may use them against us. (Tucker, 2016b) As some observers have noted, the Internet of Things has been weaponized. (Tucker, 2016a)

Security researchers have outlined novel and sophisticated systems for ensuring cybersecurity and privacy in various use cases. But these are at present notional and theoretical, and will only be realized in a framework of compliance, and a culture of dedication to cybersecurity. Regulation is the answer to enable the application of these emerging security technologies, to fully realize the potential of a fully functional — and secure — IoT.

The Internet of Things holds promise to bring new levels of convenience, entertainment, efficiency, and utility to all aspects of our lives. The unique nature of these devices has allowed them to become an integral part of our lives in just a few years. It is time to act to ensure their security — the future of a free and open Internet may depend on it.

All the while, billions of connected devices are sensing, listening, looking, waiting... *Alexa! Turn off the lights!*

References

Ahlmeyer, M., & Chircu, A. M. (2016). SECURING THE INTERNET OF THINGS: A REVIEW. *Issues in Information Systems*, 17(4).

Bennett, C. (2015, December 16). Long-delayed cyber bill included in omnibus. *The Hill.* Retrieved February 21, 2017, from http://thehill.com/policy/cybersecurity/263403-long-delayed-cyber-billincluded-in-omnibus

Bertino, E., & Islam, N. (2017). Botnets and Internet of Things Security. *IEEE Computer*, 50(2), 76-79.

Cheng, C., Lu, R., Petzoldt, A., & Takagi, T. (2017). Securing the Internet of Things in a Quantum World. *IEEE Communications Magazine*, 55(2), 116-120.

Conditt, J. (2016, October 21). Blame the Internet of Things for today's web blackout. *Engadget.* Retrieved February 19, 2017, from https://www.engadget.com/2016/10/21/mirai-botnet-hacked-cameras-routers-internet-outage

Dabbagh, M., & Rayes, A. (2017). Internet of Things Security and Privacy. In *Internet of Things From Hype to Reality* (pp. 195-223). Springer International Publishing.

Daly, M. (2014, July 23). Agencies must prepare for security risks of Internet of Things. *Government Computer News.* Retrieved February 20, 2017, from https://gcn.com/articles/2014/07/23/risks-iot.aspx

Goodin, D. (2016, November 01). New, more-powerful IoT botnet infects 3,500 devices in 5 days. *Ars Technica.* Retrieved February 19, 2017, from http://arstechnica.com/security/2016/11/new-iot-botnet-that-borrows-from-notorious-mirai-infects-3500-devices/

Greenemeier, L. (2016, October 25). The Internet of Things Is Growing Faster Than the Ability to Defend It. *Scientific American.* Retrieved February 19, 2017, from https://www.scientificamerican.com/article/iot-growing-faster-than-the-ability-to-defend-it/

Hill, B. (2016, September 27). Latest IoT DDoS Attack Dwarfs Krebs Takedown At Nearly 1Tbps Driven By 150K Devices. *Hot Hardware.* Retrieved February 19, 2017, from http://hothardware.com/news/latest-iot-ddos-attack-dwarfs-krebs-takedown-at-nearly-1-terabyte-per-second

Hossain, M. S., Muhammad, G., Rahman, S. M. M., Abdul, W., Alelaiwi, A., & Alamri, A. (2016). Toward end-to-end biometrics-based security for IoT infrastructure. *IEEE Wireless Communications*, 23(5), 44-51.

Han, G., Shu, L., Chan, S., & Hu, J. (2016). Security and privacy in Internet of things: methods, architectures, and solutions. *Security and Communication Networks*, 9(15), 2641-2642.

Ho, G., Leung, D., Mishra, P., Hosseini, A., Song, D., & Wagner, D. (2016, May). Smart locks: Lessons for securing commodity internet of things devices. In *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security* (pp. 461-472). ACM.

Kang, J., Yu, R., Huang, X., Jonsson, M., Bogucka, H., Gjessing, S., & Zhang, Y. (2016). Location privacy attacks and defenses in cloud-enabled internet of vehicles. *IEEE Wireless Communications*, 23(5), 52-59.

Krebs, B. (2016b, October 16). Who Makes the IoT Things Under Attack? *Krebs on Security.* Retrieved February 19, 2017, from https://krebsonsecurity.com/2016/10/who-makes-the-iot-things-under-attack/

Lee, J. H. (2016). Secure authentication with dynamic tunneling in distributed IP mobility management. *IEEE Wireless Communications*, 23(5), 38-43.

Li, Y., Chai, K. K., Chen, Y., & Loo, J. (2016). Distributed access control framework for IPv6-based hierarchical internet of things. *IEEE Wireless Communications*, 23(5), 17-23.

Niu, J., Jin, Y., Lee, A. J., Sandhu, R., Xu, W., & Zhang, X. (2016, June). Security and Privacy in the Age of Internet of Things: Opportunities and Challenges. In *Proceedings of the 21st ACM on Symposium on Access Control Models and Technologies* (pp. 49-50). ACM.

Rose, A. (2013, January 11). The Internet of Things Has Arrived — And So Have Massive Security Issues. *WIRED.* Retrieved February 19, 2017, from https://www.wired.com/2013/01/securing-the-internet-of-things/

Schneier, B. (2014, January 06). The Internet of Things Is Wildly Insecure — And Often Unpatchable. *WIRED.* Retrieved February 19, 2017, from https://www.wired.com/2014/01/theres-no-good-way-to-patch-the-internet-of-things-and-thats-a-huge-problem/

Schneier, B. (2016a, October 06). We Need to Save the Internet from the Internet of Things. *Motherboard.* Retrieved February 19, 2017, from http://motherboard.vice.com/read/we-need-to-save-the-internet-from-the-internet-of-things

Schneier, B. (2016b, November 03). Your WiFi-connected thermostat can take down the whole Internet. We need new regulations. *Washington Post.* Retrieved February 19, 2017, from https://www.washingtonpost.com/posteverything/wp/2016/11/03/your-wifi-connected-thermostat-can-take-down-the-whole-internet-we-need-new-regulations/

Sicari, S., Cappiello, C., De Pellegrini, F., Miorandi, D., & Coen-Porisini, A. (2016). A security-and quality-aware system architecture for Internet of Things. *Information Systems Frontiers*, 18(4), 665-677.

Singh, J., Pasquier, T., Bacon, J., Ko, H., & Eyers, D. (2016). Twenty security considerations for cloud-supported Internet of Things. *IEEE Internet of Things Journal*, 3(3), 269-284.

Stavridis, J., & Weinstein, D. (2016, November 03). The Internet of Things Is a Cyberwar Nightmare. *Foreign Policy.* Retrieved February 19, 2017, from http://foreignpolicy.com/2016/11/03/the-internet-of-things-is-a-cyber-war-nightmare/

Tucker, P. (2014, July 24). The CIA Fears the Internet of Things. *Defense One.* Retrieved February 20, 2017, from http://www.defenseone.com/technology/2014/07/cia-fears-internet-things/89660/

Tucker, P. (2016a, September 08). How Will Terrorists Use the Internet of Things? The Justice Department Is Trying to Figure That Out. *Defense One.* Retrieved February 19, 2017, from http://www.defenseone.com/technology/2016/09/how-will-terrorists-use-internet-things-justice-department-trying-figure-out/131381/

Tucker, P. (2016b, October 22). Someone Weaponized the Internet of Things. *Defense One.* Retrieved February 19, 2017, from http://www.defenseone.com/threats/2016/10/someone-weaponized-internet-things/132553/

Washington Post Editorial Board. (2016, October 25). The Day of the Zombie Baby Monitors: When hackers weaponized the Internet of Things. *Washington Post.* Retrieved February 19, 2017, from https://www.washingtonpost.com/opinions/the-day-of-the-zombie-baby-monitors-when-hackers-weaponized-the-internet-of-things/2016/10/25/167fdf42-9a1b-11e6-b3c9-f662adaa0048_story.html

Wang, K., Qi, X., Shu, L., Deng, D. J., & Rodrigues, J. J. (2016). Toward trustworthy crowdsourcing in the social internet of things. *IEEE Wireless Communications*, 23(5), 30-36.

Vinel, A., Chen, W. S. E., Xiong, N. N., Rho, S., Chilamkurti, N., & Vasilakos, A. V. (2016). Enabling wireless communication and networking technologies for the internet of things [Guest editorial]. *IEEE wireless communications*, 23(5), 8-9.