The Internet of (Vulnerable) Things: On Hypponen's Law, Security Engineering, and IoT Legislation

Mikko Hypponen and Linus Nyman

The Internet of Things (IoT) and the resulting network-connectedness of everyday objects and appliances in our lives bring not only new features and possibilities, but also significant security concerns. These security concerns have resulted in vulnerabilities ranging from those limited in effect to a single device to vulnerabilities that have enabled IoT-based botnets to take over hundreds of thousands of devices to be used for illegal purposes. This article discusses the vulnerable nature of the IoT – as symbolized by Hypponen's law – and the parts both manufacturers and consumers play in these vulnerabilities. This article makes the case for the importance of security engineering for IoT manufacturers, highlights some significant issues to help consumers address these vulnerabilities, and argues for legislation as perhaps the only reliable means of securing the Internet and its connected devices.

Introduction

As security expert Bruce Schneier (2015) has noted, the appliances and gadgets that are part of our everyday lives are becoming computers that can do other things. Our phones have become computers that can also make phone calls. Our cars are becoming computers that can also drive. Our washing machines are becoming computers that can also wash clothes. These computers are commonly connected to a network – often, though not necessarily, the Internet. The phenomenon as a whole is called the Internet of Things (IoT; tinyurl.com/lqdsl4n). Between 2014 and 2020, the number of these connected things has been projected to grow at an annual compound rate of 23.1%, reaching 50.1 billion things in 2020 (Press, 2016).

This emerging ubiquity of network-enabled computers raises a host of significant privacy and security concerns. As Chief Research Officer for F-Secure, a Finnish cybersecurity company, this article's main author has spent more than a quarter of a century working to make computers safe. As the first IoT devices, or "smart" devices, began appearing on the market, Hypponen, along with many other security experts, began taking a closer look at them. The results were very worrying indeed: these connected devices almost invariably contained significant vulnerabilities.

The vulnerable nature of network-connected devices has been covered before in both the popular press (e.g., Franceschi-Biccierai, 2016a; Greenberg & Zetter, 2015; Schneier, 2014) as well as in academia (e.g., Abomhara & Køien, 2015; Greene, 2015; Patton et al., 2014). Particularly within the security community, these topics have been discussed and warned about for years. And yet, both in the popular press as well as among security researchers, there are many who believe the situation re-

The Internet of (Vulnerable) Things

Mikko Hypponen and Linus Nyman

garding IoT vulnerabilities is getting worse, not better (e.g., Franceschi-Biccierai, 2016b; Porup, 2016; Schneier, 2017). IoT vulnerabilities have been shown to affect not only the quality of individual products and networks, but also even the stability of the very backbone of the Internet itself. By extension, these vulnerabilities impact the wellbeing of human life as well.

This article is primarily for readers with limited to no experience in security engineering. It is part academic essay on the vulnerable nature of the Internet of Things and part plea to manufacturers and consumers to take these vulnerabilities seriously. We believe it will be of particular interest to three main groups. First, to managers or manufacturers who are considering entering the world of IoT. Second, to consumers who want to better understand some of the risks of their smart products and how to mitigate them. And, third, to legislators concerned with the safety and security of our everyday devices.

The remainder of this article is structured as follows. We begin with a brief discussion of the rise of the IoT and its part in transforming traditional companies into software companies. We then examine the vulnerable nature of smart devices, provide examples of vulnerabilities, and discuss some key reasons why these vulnerabilities exist. Finally, we recommend actions that can be taken by both manufacturers and consumers to address these vulnerabilities, and we conclude with a brief discussion of legislation as a means of securing the IoT.

IoT: Old Concepts, New Software Companies

The Internet of Things as a phenomenon is not new. In 2014, the IoT made the top of Gartner's list of the most hyped emerging technologies (Gartner, 2015). However, the concepts that form the building blocks of the IoT are considerably older; the phenomenon itself is made possible by half a century of advances in computing. Among the more significant changes over the past decade that have enabled IoT's meteoric rise are a significant drop in cost for the necessary component parts of smart devices and the widespread availability of Wi-Fi. In other words, getting things online is becoming very inexpensive and getting them connected is becoming very easy.

Although there are notable challenges to monetizing the IoT (e.g., Westerlund et al., 2014), predictions about the IoT being headed for massive growth are the norm. Over the longer term, some believe its growth will surpass even that of the early Internet (e.g., Gershenfeld & Vasseur, 2014). Over the shorter term, estimates for both IoT market size and growth are also substantial. McKinsey puts IoT market size estimates at increasing from $900M USD in 2015 to $3.7B in 2020 (e.g., Forbes, 2016), and Bain predicts that, by 2020, the annual revenue for vendors of IoT hardware, software, and "comprehensive solutions" may exceed $470B (Forbes, 2016).

Indeed, we have already seen companies take strong strategic stances in support of the IoT. Samsung Co-CEO Boo-Keun Yoon proclaimed, back in 2015, that 90% of Samsung products would be IoT-enabled by 2017, and 100% by the year 2020 (Sims, 2016). Yoon did not state that Samsung would add IoT-enabling components to all those products where an Internet connection would offer some consumer benefit. Rather, that it would make *all* of its products IoT-enabled. And Samsung is not alone. Even a brief glance at the plethora of smart products flooding the market suggests that there is an abundance of companies striving to make anything and everything IoT-enabled. The resulting spectrum of IoT devices covers everything from more self-evidently useful implementations such as smart security cameras to increasingly odd, even bizarre, implementations including toasters (Vanhemert, 2014), mattresses (Crook, 2016), showerheads (Krupitzer, 2015), and underwear (Graham, 2016).

Consumers may not see the benefits of an Internet connection in all of their devices. IoT features may, instead, be intended to benefit the company that produces them, in the form of collected data. Data was, of course, considered a crucial topic even before the emergence of IoT. (In fact, when IoT made Gartner's [2015] list of the most hyped technologies, it did so by displacing "Big Data".) IoT devices are in a unique position to gather data for their manufacturers about the product's use: how often we wash our clothes, how many cups of coffee we drink each day, and so forth. In an effort to, in part, offer products with new IoT features, but also in an effort to gather additional valuable data, numerous companies that just a few years ago had nothing to do with software are now rushing to join the IoT revolution – and, in the process, are becoming software companies. A significant reason why this shift is problematic, and indeed the underlying cause behind so many of the vulnerabilities we see today, is the resulting lack of experience in security engineering among these new software companies.

The Internet of (Vulnerable) Things

Mikko Hypponen and Linus Nyman

Hypponen's Law: Smart Means Vulnerable

Hypponen's law is a simple yet important concept – so simple, in fact, that it was first put forth as a single tweet in December 2016 (http://twitter.com/mikko/status/808291670072717312) "Hypponen's law: Whenever an appliance is described as being 'smart', it's vulnerable." Whether it is a car, a TV, or a toothbrush, if it is smart – if it is connected to a network – then it is vulnerable. This notion of the vulnerability of smart objects is of course not limited to appliances, but is equally true of other Internet-enabled things. Indeed, the ever-growing list of IoT devices ranges from mousetraps (Corfield, 2017) and tea kettles (Bode, 2015) to sniper rifles (Greenberg, 2015), cars (Greenberg, 2016), and beyond.

Our hope with this article is to reach out beyond the confines of the security community to further underline the simple yet important point of IoT vulnerability. If you are in the market for a smart product, you will be buying a vulnerable product. If you are designing a smart product, you are designing a vulnerable product.

The Far-Reaching Effects of IoT Vulnerabilities

Vulnerabilities can have very real and very bad results. A vulnerable IoT device can become a bridge between a private network and a public one. A vulnerable IoT device can be exploited to gain sensitive information, including passwords. The network-connectedness of IoT devices can serve as a means for malware to access not only the IoT device itself, but also other devices connected to the network. IoT vulnerabilities can even have consequences that extend far beyond the scope of a single device or local area network. This was the case in October of 2016, when large parts of the backbone of the Internet came under the largest attack in the history of the Internet. This attack was not conducted by supercomputers, or indeed even powerful desktop computers – it was conducted by over 100,000 IoT appliances. These appliances, unbeknownst to their owners, became part of the "Mirai botnet", whose initial targets ranged from an individual security journalist (Krebs, 2016a) to several waves of attacks against a company that provides core Internet services for dozens of popular sites, among them Twitter, Spotify, Reddit, and the New York Times (Etherington & Conger, 2016; Krebs, 2016b; Newman, 2016). This latter attack brought down a significant portion of the Internet for several hours.

Connecting things to the Internet can lead to vulnerabilities for reasons unrelated to the devices themselves. An example of this is an industrial control system interface that has been connected to the Internet without including security measures such as requiring the user to log in or enter a password. These kinds of interfaces may have been connected to the Internet intentionally but then security measures, such as requiring a password, were forgotten to be implemented. Alternatively, an interface may have initially been set up on a separate network that was not connected to the Internet. Then, perhaps several years later, that network was connected to the Internet, without those who connected it having realized that connecting it made the industrial control system interface accessible to anyone on the Internet. For example, security researchers at F-Secure have discovered such unsecured systems that control prescription drug orders, home automation and security systems (to control temperature, security cameras, alarms, and even curtains), car washes, pumping stations, swimming pools, restaurant point-of-sale systems, solar panels, biogas plants, ski lifts, wind turbines, hospital bed monitoring stations, funeral parlour crematoriums, and steel furnaces.

Why Is Smart Vulnerable?

There are two basic causes of IoT vulnerabilities: technical problems and people problems. In the following subsections, we discuss each type of problem individually.

Technical problems

By technical problems, we mean problems that can be fixed with an update. There will never come a time when new vulnerabilities are no longer discovered, and therefore the security of any system depends on that system being kept up-to-date. People are notoriously poor at regularly updating their systems – this is a "people problem" – which is why automatic updates have become common. One significant problem in IoT devices is that it may be difficult, or even impossible, to update their software. Both the operating system and the software running the IoT device must be updateable. If they are not, or even if updating one or both of them is not easy, the emergence of exploitable vulnerabilities in a product is a near certainty. To make matters worse, some IoT devices ship with outdated operating systems, meaning the devices may have known vulnerabilities before they are even unboxed.

In addition to outdated software, a further significant source of vulnerabilities stems from the failure of IoT manufacturers to take advantage of lessons already learned by others. Many technical problems have been solved years ago, even decades ago, resulting in

The Internet of (Vulnerable) Things

Mikko Hypponen and Linus Nyman

evolving sets of best practices in the computer industry. However, vulnerabilities that should no longer be a problem continue to plague the IoT. An example of this is the Telnet communications protocol. Telnet is an unsecured means of communicating over a network. Due to its lack of encryption, the computer industry moved away from Telnet roughly two decades ago. However, Telnet can still be found among the causes of current IoT vulnerabilities (e.g., Franceschi-Bicchierai, 2016c; Krebs, 2016).

People problems

Whereas technical problems typically can be fixed with an update, people problems require education and learning, as well as an interest in addressing the issue or problem. In theory, people problems should be the easier of the two to fix. In practice, however, this is rarely the case. For example, consider the VHS recorder clock display. Readers old enough to remember the VCR are likely to have come across displays that showed a blinking "12:00" rather than the current time. In the case of the VCR, the effects of the user not making an effort to learn how to set the time were insignificant. However, this same phenomenon of user ignorance or indifference in the context of IoT appliances has a much greater impact. A key example of this is device default passwords. The Mirai botnet, for instance, was designed to search the Internet for IoT devices, trying a number of different common default usernames and passwords in order to gain control of the devices it found (e.g., Franceschi-Biccierai, 2016c). Something as simple as changing the default password on a device would have protected against this attack. We as users need to both know that default passwords are insecure and then also care enough about the issue to change them. A device capability, including security capabilities such as the ability to change a password, can be made ineffective through user ignorance or indifference.

Towards a More Secure IoT

It is our sincere hope that, ten years from now, we will be able to say about the IoT revolution what we can now say about the Internet revolution: the good outweighed the bad. However, this result will not come about by itself – concrete action is needed to curb IoT vulnerabilities. In the remainder of this article, we discuss some steps manufacturers, consumers, and legislators can take to mitigate IoT vulnerabilities.

Manufacturers

It is not our goal with this article to offer a checklist for securing IoT devices. Rather, the crucial point we want to make is that, if a manufacturer is heading into an IoT domain, it should think of itself as a software company. And, any company that takes it upon itself to develop software must also take it upon itself to secure its software. This means committing to taking security engineering seriously, by investing in both educating employees as well as hiring new specialists where needed.

The case for security engineering need not be made from the perspective of civic duty – there are also clear financial arguments supporting such investments. One important example is new legislation underway in Europe. The General Data Protection Regulation (European Parliament, 2016), which will take effect in May 2018, focuses on strengthening and unifying data protection for individuals within the European Union (EU). However, the directive also addresses the exportation of personal data outside the EU. Thus, even some manufacturers outside of the EU will be affected. An in-depth examination of the General Data Protection Regulation is beyond the scope of this article, but it is significant to note that it is broad in scope and covers not only responsibilities and accountability, but also sanctions. Furthermore, the stipulated sanctions are significant. Among them, manufacturers can be fined up to 20M EUR or up to 4% of the annual worldwide turnover of the preceding financial year in case of an enterprise, whichever is greater (European Parliament, 2016: Article 83, paragraph 5–6). Thus, securing IoT devices, which commonly gather data wherever they are in the world, should be made a priority.

Securing IoT devices is the responsibility of a manufacturer's security engineering team. However, we offer the following initial recommendations to manufacturers:

- Make sure your product's software as well as its operating system can be updated. Make this update automatic, but also make it possible to postpone if the consumer needs to do so. (As the first author of this paper can attest, drones have fallen out of the sky due to unexpected mid-air updates.)

- Try to mitigate human problems. Make it as difficult as possible for the consumer to use their device in an unsafe manner. For instance, passwords as an authentication system are inherently flawed and you should look into adding additional or alternative security tokens. However, if you do use passwords, set up your devices so that default passwords have to be changed when the device is taken into use.

The Internet of (Vulnerable) Things

Mikko Hypponen and Linus Nyman

- Learn from the mistakes of the computer industry. One example we brought up earlier is to not leave Telnet enabled. However, there are many other deprecated protocols still in wide use. Close all ports that do not need to be open. Extend this discussion with your security engineering team to include network security.

- Even with a team of security engineers, it is still important to commit both time and resources to security audits and penetration testing. In other words: try to break into your own systems.

- Some vulnerabilities may be found by people from outside of your organization. For this reason, it is important to also have a system in place through which vulnerabilities and bugs can be reported. Offering bug bounties – rewards for finding bugs – may encourage others to find and report vulnerabilities.

There are many, many more things to take into consideration, both regarding security as well as privacy. For this reason, we are not suggesting that manufacturers should follow some external checklist, but rather we urge them to make security engineering a central part of what their company does.

Consumers

IoT vulnerabilities can affect not only a product itself, but also anything from other devices connected to a network to the entire Internet itself. And, again, there are privacy issues, but they are beyond the scope of the current discussion. With the stakes being as high as they are, we encourage consumers to take an active interest in the security of their IoT devices by offering the following recommendations:

- Bear in mind that you are no longer buying washing machines and toasters – you are buying computers that can wash clothes and toast bread. And computers need to be secured. When shopping for an IoT device, be sure to ask about security. Also, check online for known device vulnerabilities before buying.

- When purchasing IoT devices, ask about updates. It is important that you be able to update both the software for the device as well as the operating system that runs it. These updates should preferably be automatic, but with the option to postpone the update if needed.

- Do not buy anything with hard-coded passwords. In other words, if a device uses passwords, it must be possible for you to change the default password.

- Once you have set up your IoT device, always change default passwords immediately.

- Just because a device can connect to a network does not mean that it has to be connected or that that network has to be the Internet. If a connection is required, differentiate between IoT devices that need to be connected to the Internet and those that do not. For instance, if you are installing a security camera, it is likely that you will want to be able to access the feed from the Internet. However, a washing machine, toaster, or any number of other household appliances is likely to be something that does not need to be connected to the Internet. For such appliances, connect them to a local area network, but not to the Internet.

Legislators

There are a number of challenges, both regarding consumer and manufacturer behaviour, that compound the problem of IoT vulnerabilities. We are not entirely hopeful that a greater understanding among manufacturers and consumers of IoT vulnerabilities alone will inspire the necessary actions towards securing the IoT. It seems more likely, if not inevitable, that legislation will be needed to keep IoT vulnerabilities in check. Arguing for legislation has its own problems, and there are certainly examples where legislation has failed. However, it might be that we cannot expect individual manufacturers to invest heavily in IoT security, given that the required investment may hamper their profitability in the name of improving a feature that consumers rarely know to ask about or appreciate. Legislation that makes manufacturers liable for damages caused by the vulnerabilities of their products would force all manufacturers to invest in security engineering, thereby levelling the playing field.

As an example, take home appliances: manufacturer liability for the safety of these devices is already regulated. If your brand-new washing machine short circuits and burns down your house, the manufacturer is liable. Thus, it would seem a small and logical next step to also regulate the security of these devices, making that same manufacturer liable if the damages are of a digital, rather than physical, nature. We do not believe that legislation would need to detail the specifics of how this securing should be accomplished. Merely making manufacturers liable for the cost of not just physical, but also digital faults in their products would ensure a much-needed manufacturer focus on security engineering.

The Internet of (Vulnerable) Things

Mikko Hypponen and Linus Nyman

Conclusion

The IoT revolution is already underway. With its unprecedented number of interconnected computers has come a host of vulnerabilities. These vulnerabilities must be addressed if we are to secure both the future of the IoT as well as a functioning Internet. To achieve this goal, manufacturers will need to put considerable focus on security engineering, policymakers will need to assess the situation to see if legislation is indeed needed to ensure this focus on security engineering takes place, and consumers will need to understand what they can do to minimize the vulnerabilities inherent in their devices.

About the Authors

Mikko Hypponen is Chief Research Officer at F-Secure. He has written about his research for The *New York Times, Wired,* and *Scientific America,* and he has lectured at several universities, among them Stanford, Oxford, and Cambridge. He has been selected as one of the 50 most important people on the web by *PC World Magazine* and was included in the FP Global Thinkers list. He is a member of the board of the Nordic Business Forum and the advisory board of the t2 infosec conference.

Linus Nyman is an Assistant Professor at the Hanken School of Economics in Helsinki, Finland. He has lectured on a range of topics, including corporate strategy and open source software development. His current research focuses on information security and privacy, which are topics he also covers in a blog for the Finnish daily newspaper *Hufvudstadsbladet.* Linus holds a PhD and a Master's degree, both from the Hanken School of Economics.

References

Abomhara, M., & Køien, G. M. 2015. Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks. *Journal of Cyber Security,* 4(1): 65–88. http://dx.doi.org/10.13052/jcsm2245-1439.414

Bode, K. 2015. Easily Hacked Tea Kettle Latest to Highlight Pathetic Internet of Things 'Security'. *Techdirt,* October 23, 2015. Accessed April 10, 2017: https://www.techdirt.com/articles/20151015/13551232547/easily-hacked-tea-kettle-latest-to-highlight-pathetic-internet-things-security.shtml

Columbus, L. 2016. Roundup of Internet of Things Forecasts and Market Estimates, 2016. *Forbes,* November 27, 2016. Accessed February 27, 2017: https://www.forbes.com/sites/louiscolumbus/2016/11/27/roundup-of-internet-of-things-forecasts-and-market-estimates-2016/

Corfield, G. 2017. More Brilliant Internet of Things Gadgetry: A £1,300 Mousetrap. *The Register,* February 23. 2017. Accessed April 10, 2017: https://www.theregister.co.uk/2017/02/23/rentokil_1300_pound_iot_mousetrap/

Crook, J. 2016. New Smart Mattress Will Tell You If Your Partner Is Cheating. *TechCrunch,* April 18, 2016. Accessed April 10, 2017: https://techcrunch.com/2016/04/18/new-smart-mattress-will-tell-you-if-your-partner-is-cheating/

Etherington, D., & Conger, K. 2016. Large DDoS Attacks Cause Outages at Twitter, Spotify, and Other Sites. *TechCrunch,* October 21, 2016. Accessed February 27, 2017: https://techcrunch.com/2016/10/21/many-sites-including-twitter-and-spotify-suffering-outage/

European Parliament. 2016. *Regulation (EU) 2016/679 of the European Parliament and of the Council on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation).* Brussels: European Parliament. http://eur-lex.europa.eu/eli/reg/2016/679/oj

Franceschi-Biccierai, L 2016a. The Looming Disaster of the Internet of (Hackable) Things. *Motherboard,* November 7, 2016. Accessed April 10, 2017: https://motherboard.vice.com/en_us/article/the-looming-disaster-of-the-internet-of-hackable-things

Franceschi-Biccierai, L 2016b. In the Future, Hackers Will Build Zombie Armies from Internet-Connected Toasters. *Motherboard,* July 5, 2016. Accessed April 10, 2017: https://motherboard.vice.com/en_us/article/in-the-future-hackers-will-build-zombie-armies-from-internet-connected-toasters

Franceschi-Biccierai, L 2016c. The Internet of Things Sucks So Bad Even 'Amateurish' Malware Is Enough. *Motherboard,* October 3, 2016. Accessed April 10, 2017: https://motherboard.vice.com/en_us/article/internet-of-things-malware-mirai-ddos

Gartner. 2015. Gartner's 2015 Hype Cycle for Emerging Technologies Identifies the Computing Innovations That Organizations Should Monitor. *Gartner,* August 18, 2015. Accessed February 27, 2017: https://www.gartner.com/newsroom/id/3114217

The Internet of (Vulnerable) Things

Mikko Hypponen and Linus Nyman

Gershenfeld, N., & Vasseur, J. P. 2014. As Objects Go Online: The Promise (and Pitfalls) of the Internet of Things. *Foreign Affairs,* March/April. Accessed February 27, 2017: https://www.foreignaffairs.com/articles/2014-02-12/objects-go-online

Graham, J. 2016. Meet the World's First Smart Bra. *USA Today,* January 4, 2016. Accessed April 10, 2017: https://www.usatoday.com/story/tech/2016/01/04/ces-2016---meet-worlds-first-smart-bra/78247554/

Greenberg, A. 2015. Hackers Can Disable a Sniper Rifle – Or Change Its Target. *Wired,* July 29, 2015. Accessed April 10, 2017: https://www.wired.com/2015/07/hackers-can-disable-sniper-rifleor-change-target/

Greenberg, A. 2016. The Jeep Hackers Are Back to Prove Car Hacking Can Get Much Worse. *Wired,* August 1, 2016. Accessed April 10, 2017: https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/

Greenberg, A., & Zetter, K. 2015. How the Internet of Things Got Hacked. *Wired,* December 28, 2015. Accessed April 10, 2017: https://www.wired.com/2015/12/2015-the-year-the-internet-of-things-got-hacked/

Greene, J. 2015. TIM Lecture Series – The Internet of Everything: Fridgebots, Smart Sneakers, and Connected Cars. *Technology Innovation Management Review,* 5(5): 47–49. http://timreview.ca/article/898

Krebs, B. 2016a. KrebsOnSecurity Hit With Record DDoS. *KrebsOnSecurity,* September 16, 2016. Accessed February 27, 2017: https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/

Krebs, B. 2016b. DDos on DYN Impacts Twitter, Spotify, Reddit. *KrebsOnSecurity,* October 16, 2016. Accessed April 10, 2017: https://krebsonsecurity.com/2016/10/ddos-on-dyn-impacts-twitter-spotify-reddit/

Krupitzer, C. 2015. Technology Is Improving Our Day-to-Day Lives, from the Boardroom to the… Bathroom? *Thinglogix,* March 12, 2015. Accessed April 10, 2017: http://www.thinglogix.com/building-the-bathroom-of-the-future-with-iot-technology/

Newman, L. 2016. What We Know about Friday's Massive East Coast Internet Outage. *Wired,* October 21, 2016. Accessed April 10, 2017: https://www.wired.com/2016/10/internet-outage-ddos-dns-dyn/

Patton, M., Gross, E., Chinn, R., Forbis, S., Walker, L., & Chen, H. 2014. *Uninvited Connections: A Study of Vulnerable Devices on the Internet of Things (IoT).* Paper presented at the IEEE Joint Intelligence and Security Informatics Conference (JISIC), September 24–26, 2014. http://dx.doi.org/10.1109/JISIC.2014.43

Porup, J. 2016. "Internet of Things" Security Is Hilariously Broken and Getting Worse. *Ars Technica,* January 23, 2016. Accessed April 10, 2017: https://arstechnica.com/security/2016/01/how-to-search-the-internet-of-things-for-photos-of-sleeping-babies/

Press, G. 2016. Internet of Things By The Numbers: What New Surveys Found. *Forbes,* September 2, 2016. Accessed April 11, 2017: https://www.forbes.com/sites/gilpress/2016/09/02/internet-of-things-by-the-numbers-what-new-surveys-found/

Schneier, B. 2014. The Internet of Things Is Wildly Insecure – And Often Unpatchable. *Wired,* January 6, 2014. Accessed April 10, 2017: https://www.wired.com/2014/01/theres-no-good-way-to-patch-the-internet-of-things-and-thats-a-huge-problem/

Schneier, B. 2015. *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World.* New York: Norton & Company.

Schneier, B. 2017. Botnets of Things – The Relentless Push to Add Connectivity to Home Gadgets Is Creating Dangerous Side Effects That Figure to Get Even Worse. *MIT Technology Review,* March/April.

Sims, G. 2015. Samsung Says All Its Products Will Be IoT Enabled within 5 Years. *Android Authority,* January 6, 2015. Accessed February 27, 2017: http://www.androidauthority.com/samsung-says-products-will-iot-enabled-within-5-years-578576/

Vanhemert, K. 2014. A Toaster that Begs You to Use It: Welcome to the Bizarre Smart Home. *Wired,* March 17, 2014. Accessed April 10, 2017: https://www.wired.com/2014/03/addicted-products/

Westerlund, M., Leminen, S., & Rajahonka, M. 2014. Designing Business Models for the Internet of Things. *Technology Innovation Management Review,* 4(7): 5–14. https://timreview.ca/article/807

Citation: Hypponen, M., & Nyman, L. 2017. The Internet of (Vulnerable) Things: On Hypponen's Law, Security Engineering, and IoT Legislation. *Technology Innovation Management Review*, 7(4) 5–11. http://timreview.ca/article/1066

Keywords: cybersecurity, Internet of Things, IoT, smart devices, vulnerability, security engineering, consumers, manufacturers, legislation, Hypponen's law