Research Note

The Internet of Things: A Dark Precursor

Kyle McNulty

Published: October 2018
Written: October 2017

Keywords: cybersecurity; the Internet of Things; smart technology; Internet connected devices.

Abstract: This paper explores the growing risks associated with the spreading web of internet-enabled devices across consumers' lives. The explosive proliferation of Internet-connected devices has resulted from rapid progress in technology and expanding demand for internet-connected capabilities from consumers. However, this technological advancement and consumer behavior has also created a significant vulnerability: cybersecurity. The current risks associated with the Internet of Things will only have more serious consequences if left unaddressed.

The number of Internet-connected devices reached a count of 13 billion in 2017, estimates research firm Gartner. That number is projected to double by 2020 and reach global revenues of $1.7 trillion for the ecosystem.[1] The idea of the "Internet of Things" (IoT) refers to the collective whole of Internet-enabled devices. Included in this collection are devices that range from personal laptops and mobile phones, to household appliances such as refrigerators, coffee makers, and lamps. These so-called "smart" devices are penetrating households across the world, and the industry as a whole is rapidly expanding as technology miniaturizes, and consumers increasingly demand connectivity and convenience in their everyday lives.

This explosive proliferation of Internet-connected devices has lead to incredible technological progress, but has also created a significant and gaping hole: security. A pair of researchers from Trend Micro discovered more than 178 million vulnerable and exposed IoT devices in 10 major U.S. cities. These included webcams, medical devices, databases, and routers.[2] Simple tools such as Shodan, a free database and search engine for identifying IoT devices, serve as reconnaissance tools for hackers allowing them to easily access and take control of these devices.

We have already seen hackers capitalizing on these exposed and vulnerable devices. "Mirai" is malware that turns Linux and Windows devices into "bots" that can be used at the infector's command in DDoS (Distributed Denial of Service) attacks. These attacks leverage the "botnet" to send out a deluge of requests to overwhelm a target device and cause it to crash. One of the most prominent cases of the Mirai botnet was in September 2016 against the popular security blog site Krebs on Security. The site was receiving traffic at a rate of 620 Gbit/s, the largest in history up to that point. Then a month later, the French cloud computing company OVH was the victim of a 1Tbit/s Mirai attack, 61% larger than the previous attack.[3]

The growing prevalence of these attacks is attributed not only to the rapid increase in the number of devices that exist, but also to the carelessness of implementing sound cybersecurity practices when these devices reach consumers and end-users of the devices. The apparent apathy towards cybersecurity stems from lack of awareness, the fuel of competition in cutthroat markets, and the inevitability of human error.

Cybersecurity has only recently been acknowledged as noteworthy of attention within organizations. Many

companies now have policies to prevent cyber-attacks, but these policies are often outdated or ignored. According to a survey of medical device manufacturers done by Ponemon Institute, only 17% of the individuals surveyed say their organization takes significant measures to prevent attacks.[4] In May of 2017, the "Wannacry" ransomware, an attack that locks users out of their systems until the attackers receive money, struck hospitals around the world. The vulnerability exploited in these attacks was disclosed with a patch in March, but the hospitals declined to patch their affected devices. Hospitals are often reluctant to patch devices because of the potential impact on patient care, but the resulting security environment leads to issues of its own. Because of these lackluster policies and procedures, vulnerabilities can remain in production systems for years after their disclosure, which ultimately leads to a larger host of vulnerable devices on the Internet.

Additionally, competition and the feature-centric attitude of the modern consumer dissuades manufacturers from concerning themselves with security. There are hundreds of companies competing for IoT market share. In 2015, technology giant Amazon jumped into the IoT market with offerings for cloud compatibility between IoT devices and other Amazon Web Services. Other major players include Microsoft, Oracle, and Siemens.[5] With fierce competition comes pressure from executives to meet quotas and get products to market. As a result, small and large companies alike are forced to forgo product changes they see as optional like security, in favor of features more tangible to consumers such as computing speed. While the average consumer remains impartial to the security of the product he/she purchases, companies will continue to omit security under pressure to compete and finish projects on budget.

Finally, even if consumers and producers alike recognize the importance of security, insecurity is inevitable. Humans are imperfect. Vulnerabilities stem from errors on behalf of humans. Whether the developer lazily coded and failed to remove a backdoor, an entry point to a system that bypasses authentication procedures, or the product security team failed to identify a vulnerability; these mistakes happen. Additionally, software developers are often content after shipping a product, whereas attackers are constantly looking for workarounds. Vulnerabilities will continue to occur because humans will continue to make mistakes, and as technology gains an increasingly important role in society the stakes of these vulnerabilities will rise exponentially.

Humans have all sorts of dreams for technology: self-driving cars, virtual reality, and jetpacks. The list may sound far-fetched, but we are making tangible progress towards all of the above. In 2016, technology accounted for 7.1% of the total U.S gross domestic product.[6] Because of the funding and investment in the industry, large companies like Amazon and Google have the freedom to experiment on technology that seems dreamlike. Elon Musk announced his new venture, Neuralink, earlier this year. Neuralink is centered on creating chips to place in the human brain in order to keep pace with advances in artificial intelligence. With the crucial impact these chips would play in the lives of their beholders, the security implications of these devices will become a major concern for the safety and wellbeing of the users.

The ability to impact the physical world through malware has been seen before. In 2009, an American-Israeli built virus dubbed Stuxnet was deployed in Iran to curb their growing nuclear program. Stuxnet is malware that targets programmable logic controllers, which are used in the automation of electromechanical processes in factories around the world.[7] Stuxnet was used to cause Iranian nuclear centrifuges to spin out of control and explode. Between 2009 and 2010, Stuxnet is estimated to have destroyed approximately a fifth of the nuclear centrifuges in the Natanz plant.[8] And cyber warfare is playing an ever-increasing role in government tactics today.

In President Trump's budget for 2018, he allotted over $1 billion for cybersecurity for the Department of Homeland Security.[9] In 2014, the FBI launched a cyber hiring initiative aimed at recruiting talented cybersecurity individuals into the Bureau. This focus on cyber reinforces the role it is expected to play in the future of the US government, both on offense and on defense.

The combination of focus on research and growth of the industry, with a goal of enhancing convenience for human consumers in every aspect of life, can lead to catastrophe in the coming years. As self-driving cars become a thing of reality, the possibility of manipulating the driving system and causing a fatal wreck also materializes. In 2015, Security Innovation, a Seattle-based cybersecurity-consulting firm, hacked autonomous cars by simply shining a laser pointer at the camera and effectively blinding the sensors.[10]

Cybersecurity threats also affect industries that are not directly technology focused. In 2013, two researchers for the security company Cylance reported a hard-coded password vulnerability affecting roughly 300 medical devices across approximately 40 vendors.[11] Affected devices included surgical devices, infusion pumps, defibrillators, and others. The ability to access infusion pumps using hardcoded credentials could lead to cases as extreme as murder through patient overdose.

With companies like Neuralink and Google working on next generation technology for products such as brain chips and self-driving cars, it is easy to get swept away with thoughts of technological progress and only consider security as an afterthought. However, due to the lack of consistent adhere to cybersecurity best practices, intense competition, and the simple imperfections of human-created device, the next generation of IoT devices will still be prone to the same issues that have plagued the IoT industry. Nevertheless, the stakes are increasingly becoming life or death.

---

[1] Turner, Vernon, Carrie Macgillivray, and Patrick Gorman. "Connecting the IoT: The Road to Success." IDC Corporate USA, Mar. 2017. Accessed Sep. 2017 <www.idc.com>.

[2] Osborne, Charlie. "Researchers Discover over 170 Million Exposed IoT Devices in Major U.S. Cities." *ZDNet.* 15 Feb. 2017. Accessed Sep. 2017 <www.zdnet.com>.

[3] "Mirai Botnet." New Jersey Cybersecurity & Communications Integration Cell. 28 Dec. 2016. Accessed Sep. 2017 <www.cyber.nj.gov>.

[4] *Medical Device Security: An Industry Under Attack and Unprepared to Defend*. Ponemon Institute. May 2017. Accessed Sep. 2017 <www.synopsys.com>.

[5] Velosa, Alfonso. "Competitive Landscape of IoT Platform Vendors." Gartner. 26 May 2017. Accessed Sep. 2017 <www.gartner.com>.

[6] Grisham, Preston. "U.S. Tech Industry Employment Surpasses 6.7 Million Workers." CompTIA. 29 Feb. 2016. Accessed Sep. 2017 <www.comptia.org>. 23 May 2017.

[7] Kushner, David. "The Real Story of Stuxnet." IEEE Spectrum. 26 Feb. 2013. Accessed Sep. 2017 <www.spectrum.ieee.org>.

[8] Kelley, Michael B. "The Stuxnet Attack On Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought." *Business Insider*. 20 Nov. 2013. Accessed Sep. 2017 <www.businessinsider.com>.

[9] *Budget of the U.S. Government Fiscal Year 2018*. Office of Management and Budget. Accessed Sep. 2017 <www.whitehouse.gov>.

[10] Petit, Jonathan. "How We Attacked Autonomous Cars at Security Innovation, Security Innovation." OnBoard Security. 4 Nov. 2015. Accessed Sep. 2017 <blog.onboardsecurity.com>.

[11] "Alert (ICS-ALERT-13-164-01): Medical Devices Hard-Coded Passwords." Industrial Control Systems Cyber Emergency Response Team, U.S. Department of Homeland Security. 29 Oct. 2013. Accessed Sep. 2017 <www.ics-cert.us-cert.gov>.