The Internet of Attack Vectors

Vulnerabilities in the Internet of Things Pose Special Problems for Security Professionals

Richard Givens
Department of Computer Science
Lewis University
Romeoville, Illinois, USA 60446
richardpgivens@lewisu.edu

***Abstract*— The Oxford Dictionary defines The Internet of Things (IoT) as "The Interconnection via the Internet of computer devices embedded in everyday objects, enabling them to send and receive data," [1] These so called "smart devices" are increasingly commonplace, and found in objects such as Digital Video Recorders (DVR), smart watches, coffee makers, refrigerators, printers, televisions, and home thermostats, to name a few. The novelty of controlling one's garage door via an app on a smartphone is intriguing for many, yet poses particularly difficult problems for Security Professionals and certain enterprise organizations.**

I. The Rise of the Internet of Attack Vectors

On February 28, 2017, a massive Distributed Denial of Service Attack (DDoS) disrupted services at an unnamed college in the United States of America for fifty-four consecutive hours. Using a variant of the Mirai botnet, the attack originated from almost ten thousand unique IP addresses, and generated nearly 3 billion requests. Using known vulnerabilities, the attacker or attackers exploited CCTV cameras, routers, and DVRs, averaging thirty thousand requests per second [2].

Other examples are abundant; on March 24, 2017, a security researcher disclosed a vulnerability in a commercial dishwasher equipped with an Ethernet interface which "enables cable supported communication in the local network," [3] [4]. In October of 2016, Mirai was responsible, using DVRs as per the attack in February of 2017, for crippling a portion of the Internet, as it struck Dyn, provided of Dyn DNS services to most the Internet's connected computers [5].

Most recently, a malicious user successfully gain access to the city of Houston's emergency sirens, causing every single siren in the city to blare for fifteen cycles of a ninety second activation. Though Mirai is not suspected as a tool or culprit in this case, officials have determined that a vulnerability allowed the malicious user to access the system which communicates with all the city's emergency sirens [6].

Full security of any Internet connected device, or of anything, is impossible. There will always be a vulnerability or some sort which will be exploited by a malicious party. Yet, while the risk of attack is impossible to avoid, the increasing number of IoT devices, solutions, and the resultant attacks demands that Security Professionals, enterprises, and agencies take heed, exerting considerable effort at mitigating potential risk.

II. Convenience as a Vulnerability

A. *Full Security is a Myth*

As previously stated, full security of any item, device, service, property, or person is impossible. A well-developed security plan, and proactive security posture, recognizes this fact and seeks not to defend against all attacks or vulnerabilities, but to increase the risk of detection (and hence, inevitable prosecution) for any malicious actors seeking to exploit potential vulnerabilities found within any organization.

As in Physics, computer or network based attacks follow the path of least resistance. Attackers examine the security landscape of an operation or person, and attempt to breach that security through typically common means. Common used against individuals included guessing possible passwords, social engineering, and phishing. In the case of IoT devices, these attacks typically take the form of exploiting commonly known, yet seldom patched flaws in the operating system of such devices. For, while users are typically mindful about updating their computers, such attention usually falls short when considering IoT devices such as routers, smart televisions, and refrigerators.

B. *A Lack of Standards and Accountability*

Though malicious users are a constant source of concern, it is attacks from within that can cause the greatest damage. With IoT, this is no different as there is a lack of comprehensive unifying standards of accountability and construction, or even conduct, that prevents any enterprise from releasing a device to the public with security flaws.

One such example is the Garadget, an IoT based garage door opener with a smartphone app, allowing the owner to dispose of their garage door remotes, and rely solely on their smartphone or tablet. Such a concept is ideal, in appearance, yet its execution leaves much to be desired.

Security concerns with smartphone device based garage door openers abound, yet it is the actions of the inventor of this device that highlights serious flaws in the IoT concept.

On April 1, 2017, a customer who purchased the Garadget left angry comments on the community board, and eventually a negative review of the device on the Amazon.com purchase page. The inventor, Denis Grisak, replied to the customer chiding him for his actions, and informed him that his device "will be denied server connection. [7]

This type of action from a malicious, or in this case vindictive, inside actor is all too easily accomplished. Any inside actor with sufficient motivation and access is capable of disrupting communication between IoT devices and their owners. While the use of a garage door opener, easily returned to the point of sale, is trivial, other attacks such as those possible against medical devices raise the stakes considerably.

"In 2007, when Cheney needed his implanted defibrillator replaced, Dr. Reiner ordered the manufacturer to disable the wireless feature - fearing a terrorist could assassinate the vice president by sending a signal to the device, telling it to shock his heart into cardiac arrest," [8].

III. Challenges for Security professionals

For the Security Professional, or the security-conscious user, IoT devices are troublesome. How to control these devices, as well as both the oblivious and the knowledgeable pose unique challenges.

A. Command and Control

The number of personal wireless devices, laptops, tablets, routers, networked printers, and local desktop workstations in any business may number from a few, to several thousand. For smaller business, those with only a few network-attached devices, maintaining a roster of these items is complex, yet attainable. For those businesses where such devices number in the hundreds or higher, the amount of effort required to maintain control of these devices increases exponentially, eventually reaching a critical mass after which it is impossible.

B. Oblivious Users Are Their Own Worst Enemy

Attacks using routers, network printers, unsecured computers and wireless devices often rely upon the user's own lack of understanding to succeed. Common mistakes such as failing to change the default password on a router or network printer to a custom password leave the proverbial barn door wide open.

Given that many users are unaware of the full capabilities of their IoT devices, and fewer still configure them beyond default settings, introducing them into an enterprise network is a poisoned pill, creating a vulnerability that may cost a company millions of dollars in lost revenue and reputational damage.

C. Knowledgeable Users May Be Your Worst Enemy

Though relatively harmless, an example of how easy it is to introduce a vulnerability through IoT is described in an October 2015 article on Business Insider. The article describes a series of projects on GitHub that were the work of a programmer who automated a substantial portion of his work, often with the point of pulling the wool over the eyes of his employer. In one memorable quote, the article describes a script used to direct the office coffee machine to brew coffee, and then wait a preset amount of time before pouring it.

"And his coworkers didn't even know the coffee machine was on the network and hackable," [9].

D. Common Vulnerabilities for IoT Devices

- Retention of user data, particularly when passing a device from one user to a new user, or in the case of resale.
- Buffer Overflow
- Cross-site request forgery.
- Storage of user data or passwords in plaintext format.
- Open access point connections.
- Lack of network segmentation.
- Password sniffing and replay.
- Easy to guess default administrator passwords.
- Subject to common network attacks, such as brute-forcing passwords.

IV. Forging ahead

These challenges, though considerable, are no different than the challenges faced every day by Information Security Professionals, and by building upon the knowledge already gained in the last few decades, IoT as a platform may become as secure as any information system.

A. Unversal Standards

By opting for unilaterally accepted "best practice" standards, manufacturers and vendors will increase both the security posture of their devices, and the desirability of these products.

a) Naming and Communication: Devices which directly interact with one another require standard naming conventions, while those without communication to other devices are not required to be visible to any other device, other than the direct user's interface.

b) Monitoring and Privacy: Given that IoT devices by nature connect to the Internet, manufacturers must pay close attention to monitoring and privacy issues that will arise. While the devices themselves introduce vulnerabilities, failure on the part of the vendor or manufacturer to adequately secure their own information assets creates a greater risk. Furthermore, vendors must take responsibility for monitoring and tracking their devices in the event of an outage or network based attack,

and taking appropriate measures to mitigate such events. Any vendor failing to take precaution opens their organization to liability.

B. Is It Necessary?

Perhaps the greatest security precaution any organization or individual may take is asking simply if having such a device is necessary.

For many, DVRs and CCTVs are an absolute necessity, particularly when used as part of a corporate security program. Network attached storage and printers are vital to the operations of nearly every business, and are integral parts of home computing.

However, certain IoT devices are not only unnecessary, but inherently lazy. One must wonder at the need for a dishwasher with an Ethernet connection, or a refrigerator that comes standard with a touchscreen and social media apps [10].

In the Information Age, often we find ourselves in information overload, becoming reliant on devices and methods which are increasingly redundant. It is this tendency to desire instant information, or instant feedback, which leads to the manufacture of many devices.

Instead of waking up a few extra minutes early, or using a coffee maker with a timer, we have created app compatible coffee makers, which brew coffee with a tap of our smartphone's screen. Rather than rely on traditional newscasts, or even our personal electronic devices to tell us the weather, we rely on the touchscreen on our refrigerator. And rather than printing or developing our photographs to have a physical album, we store them on the refrigerator's hard drive, or a wireless digital picture frame all with a mere few taps or swipes of our fingers.

What we do not do, however, is ask ourselves if it is necessary to stand in front of the refrigerator and tweet using its touchscreen. We do not ask ourselves why our televisions require an Internet connection, or who else could use the app that we rely upon to open our garages.

More importantly, we do not think about the potential pitfalls of using these devices, the consequences of allowing them into our everyday lives, our homes, and our businesses. We do not take the logical next step in our thinking, beyond the immediate gratification of the device itself, to consider other consequences which suddenly become possible. Quite the opposite, we remain blissfully ignorant, while we tweet our status update from our refrigerator, that it is also harvesting Bitcoin as part of a botnet. We are incapable of understanding how we reach our data caps so rapidly each month.

C. Understanding the New Threat Landscape

Risk Management and Response depends on asking and answering the classic questions of Who, What, Where, When, Why and How. For the security conscious users, and the Security Professionals, answering these questions is the key to understanding and mitigating the potential risk of IoT devices, as well as other risks. Though it may be unlikely that these questions will be answered at any given moment, the effort required to answer as many as possible will result in a stronger security posture.

Ultimately, the challenges and risks posed by IoT are the same as any computerized, network attached device, however it is their relatively new placement in the workplace, and the lack of controls surrounding their use in these environments, to and for which Security Professionals must improvise, plan, and adapt. Applying lessons learned and best practices from the previous years of Information Security to a new avenue of risk is the only way to minimize its potential.

REFERENCES

[1] "English Oxford Living Dictionaries." English Oxford Living Dictionaries, en.oxforddictionaries.com/definition/Internet_of_things. Accessed 7 Apr. 2017.

[2] Bekermin, Dima. "New Mirai Variant Launches 54 Hour DDoS Attack against US College." Incapsula.com, Imperva Incapsula, 30 Mar. 2017, www.incapsula.com/blog/new-mirai-variant-ddos-us-college.html. Accessed 9 Apr. 2017.

[3] Regel, Jens. "Full Disclosure: [CVE-2017-7240] Miele Professional PG 8528 - Web Server Directory Traversal." Full Disclosure: [CVE-2017-7240] Miele Professional PG 8528 - Web Server Directory Traversal, 24 Mar. 2017, www.seclists.org/fulldisclosure/2017/Mar/63. Accessed 9 Apr. 2017.

[4] "PG 8528." PG 8528 Washer-Disinfector - Large Capacity Washer-Disinfectors, www.miele.co.uk/professional/large-capacity-washer-disinfectors-560.htm?mat=10339600&name=PG_8528#item-2-2. Accessed 9 Apr. 2017.

[5] York, Kyle. "Dyn Statement on 10/21/2016 DDoS Attack | Dyn Blog." Dyn Dyn Statement on 10212016 DDoS Attack Comments, 22 Oct. 2016, dyn.com/blog/dyn-statement-on-10212016-ddos-attack/. Accessed 9 Apr. 2017.

[6] Stengle, Jamie. "Not so Silent Night: Dallas Emergency Siren System Hacked." Essential News from The Associated Press, Associated Press, 8 April_2017, hosted2.ap.org/APDEFAULT/495d344a0d10421e9baa8ee77029cfbd/Article_2017-04-08-US--Dallas-Emergency%20Sirens/id-71caa277d54841c6a46885ce18e8aeb0. Accessed 9 Apr. 2017.

[7] Price, Rob. "The Maker of an Internet-Connected Garage Door Disabled a Customer's Device over a Bad Review." Business Insider, Business Insider, 5 Apr. 2017, www.businessinsider.com/iot-garage-door-opener-garadget-kills-customers-device-bad-amazon-review-2017-4. Accessed 9 Apr. 2017.

[8] Gupta, Sanjay. "Dick Cheney's Heart." CBS News, CBS Interactive, 6 Aug. 2014, www.cbsnews.com/news/dick-cheneys-heart/. Accessed 9 Apr. 2017.

[9] Bort, Julie. "A Programmer Wrote Scripts to Secretly Automate a Lot of His Job - and Email His Wife and Make a Latte." Business Insider, Business Insider, 23 Nov. 2015, www.businessinsider.com/programmer-automates-his-job-2015-11. Accessed 9 Apr. 2017.

[10] Crook, Jordan. "Samsung's LCD Fridge With Apps Is A Fridge That Has An LCD And Apps." TechCrunch, TechCrunch, 21 June 2011, techcrunch.com/2011/06/21/samsungs-lcd-fridge-with-apps-is-a-fridge-that-has-an-lcd-and-apps/. Accessed 9 Apr. 2017.