The Internet of Things

Kayla McGill

Executive Summary

The Internet of Things (IoT) is made up of everyday devices with computing capabilities - essentially any device that can download or upload information from the internet. For example: pacemakers, biochip transponders for animals, 'smart home' hardware like a thermostat, lights, or home security system, things like Google Home/Alexa/other home automation, and vehicles using GPS with other features and preferences.

With so many access points to upload or download information there are many vulnerabilities in these IoT devices which experts warn pose a threat to national and global cyber security[1]. In an unclassified report, the U.S. National Intelligence Committee maintains it would be hard to deny "access to networks of sensors and remotely-controlled objects by enemies of the United States, criminals, and mischief makers[2]". On the other hand, the U.S. Intelligence Community views the IoT as a rich source in Open Source data gathering. Regardless of the benefits, costs are associated with non-secure access to the IoT. With the IoT expected to include over 20 billion devices by 2020, steps are needed to ensure security[3].

Context and Need for IoT Security

While the IoT uses advances in technology and to create better lives, there are threats to using unsecured or un-encrypted devices since any hacking or

---

[1] Reuters Staff, U.S. Senators to Introduce a Bill to Secure the Internet of Things. August 2017. https://www.reuters.com/article/us-usa-cyber-congress/u-s-senators-to-introduce-bill-to-secure-internet-of-things-idUSKBN1AH474

[2] National Intelligence Council. Conference Report CR 2008-07, April 2008. "Disruptive Civil Technologies: Six Technologies with Potential Impacts on U.S. Interests Out to 2025." https://fas.org/irp/nic/disruptive.pdf

[3] Senators Introduce Bipartisan Legislation to Improve Cybersecurity of Internet of Things (IoT) Devices. August 2017 https://www.warner.senate.gov/public/index.cfm/2017/8/enators-introduce-bipartisan-legislation-to-improve-cybersecurity-of-internet-of-things-iot-devices

accessing of the IoT can easily go undetected. Because many devices come with a factory-set, or hardcoded passwords (i.e. passwords that are unable to be changed), these devices are unable to be updated or 'patched' creating a weak point in network security. (A patch is a small update to a software or firmware that typically solves a problem – i.e. a patch can be added to windows to improve a newly discovered security vulnerability (also called a hotfix)). Most of IoT devices download and upload information. For example, devices such as Google Home and Alexa store all requests on 'the cloud', including audio recordings from vocal request by individual uses, patterns of speech, and colloquialisms. This data, if in the wrong hands, can be used to commit identity fraud and theft.

Further dangers include Data Mining, Information Hacking, and Bot Networks or Zombie Networks (botnets or zombienets) creation and use. Data mining is a primary danger of IoT, especially in-home automation, because the information gathered is not only used for making the product more efficient, but could also be used for advertising purposes to persuade individuals to potentially invest in scams[4].

As mentioned, personal information can be hacked as well. Simple methods like monitoring traffic on a network can reveal many pieces of information. If security defenses are used on any websites or home devices, and they are penetrated, all the convenient information about the primary user is available to the hackers. This information could be personal (i.e. credit, social security, etc.) and enable hackers to commit identity fraud.

[4] The Botnet that Broke the Internet Isn't Going Away. https://www.wired.com/2016/12/botnet-broke-internet-isnt-going-away/

Unregulated IoT use could lead to the creation of botnets or zombienets. These 'networks' are essentially an army of computers or IoT devices which have been hacked and are manipulated to continuously 'ping' servers and create a steady flow of traffic to the server. With millions of IoT devices available, if a large number were used to ping the same server at the same time, it would cause a Distributed Denial of Service (DDoS) attack. A DDoS attack can disable servers and restrict access by legitimate authorities attempting to access the server because of the influx of traffic from IoT devices.

Throughout the past year, IoT devices have been used by actors to launch devastating DDoS attacks. These attacks are usually on internet infrastructure such as websites, web-hosting servers, and internet providers[5]. In August 2016 a (still currently active) botnet called Mirai overwhelmed Dyn (a company that provides a significant portion of the U.S. internet's backbone) with traffic from zombienet IoT devices to knock some web services (such as Twitter, PayPal, and Spotify) offline[6]. Mirai is, "A type of malware that automatically finds IoT devices to infect and conscripts them into a botnet…this IoT army can be used to mount DDoS attacks in which a firehose of junk traffic floods a target's servers with malicious traffic" often shutting down the site and servers[7]. Mirai is one of many attacks meant to control and exploit. While Mirai is meant to disrupt internet infrastructure, if the proper penetration tools and methods were used to create an opening in cybersecurity

[5] Senators Introduce Bipartisan Legislation to Improve Cybersecurity of Internet of Things (IoT) Devices. August 2017 https://www.warner.senate.gov/public/index.cfm/2017/8/enators-introduce-bipartisan-legislation-to-improve-cybersecurity-of-internet-of-things-iot-devices
[6] The Botnet that Broke the Internet Isn't Going Away. https://www.wired.com/2016/12/botnet-broke-internet-isnt-going-away/
[7] Ibid

protocols and firewalls, then important government database servers could essentially be shut down, removing all access to information held inside.

Current Efforts

The Federal Trade Commission FTC has made recommendations for companies to ensure data collection, storage, and processing would be secure and encrypt data when IoT devices are created, allow users the choice of what data they share with IoT companies or when their data is exposed, and that data collected through pulling from IoT can only be retained for a limited time[8]. The issue is that these are simply recommendations and not enforceable by law.

There are a few policies in place now. In secure areas, devices with wireless network connection capabilities are not allowed in, additionally restricted are devices with hardware or software that could prevent or disrupt connections. However, this protocol does not address a large concern: an IoT botnet does not need to be inside of a secure network to perform a DDoS attack. Because manufacturers do not often have security in mind, IoT devices are easily hacked and can be used to infiltrate networks and cause devastating loss of services.

There is currently a bipartisan effort made in the Senate to improve the cybersecurity of IoT devices[9]. Under the terms of the bill, vendors of IoT devices who provide internet connectable equipment to the U.S. government, would need to ensure their devices are “patchable, do not include hard-coded passwords that

[8] FTC Report. March 2012. “Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers.” https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf

[9] S.1691 – Internet of Things (IoT) Cybersecurity Improvement Act of 2017. 115th Congress (2017-2018). Introduced 08/01/2017. https://www.congress.gov/bill/115th-congress/senate-bill/1691

cannot be changed, and are free to known security vulnerabilities"[10]. The bill is sponsored by two Republicans Cory Gardner and Steve Dines, and two Democrats Mark Warner and Ron Wyden.

Policy Recommendations

- Pass the bipartisan Senate bill. This will ensure that measures are put in place to equip the U.S. government with the ability to detect and avoid known security vulnerabilities. Under this bill[11]:
    - Require vendors of Internet-connected devices purchased by the federal government ensure their devices are patchable, rely on industry standard protocols, do not use hard-coded passwords, and do not contain known security vulnerabilities.
    - Exempt cybersecurity researchers engaging in good-faith research from liability…when engaged in research pursuant to adopted coordinated vulnerability disclosure guidelines.
- Require, not just recommend, that companies improve security measures on these devices to ensure external control is only accessible by the intended user.
- Restrict the ability to store customer information by minimizing the duration of data storage, what data is stored, and improve the security of that data.

[10] Reuters Staff, U.S. Senators to Introduce a Bill to Secure the Internet of Things. August 2017. https://www.reuters.com/article/us-usa-cyber-congress/u-s-senators-to-introduce-bill-to-secure-internet-of-things-idUSKBN1AH474

[11] Senators Introduce Bipartisan Legislation to Improve Cybersecurity of Internet of Things (IoT) Devices. August 2017 https://www.warner.senate.gov/public/index.cfm/2017/8/enators-introduce-bipartisan-legislation-to-improve-cybersecurity-of-internet-of-things-iot-devices