Securing the Internet of Things

By Tomer Shapira, ECE '17

The Rise of the Internet of Things

The Internet of Things (IoT) generally refers to a system of devices other than traditional computers that are able to send and receive data over computer communication networks, such as WiFi, and are ultimately connected to the internet. A "thing" can be used for a variety of applications; smart home systems and many industrial sensor networks are composed of IoT devices. Their purpose is to allow for remote monitoring or operation over a network without the need for manual input.

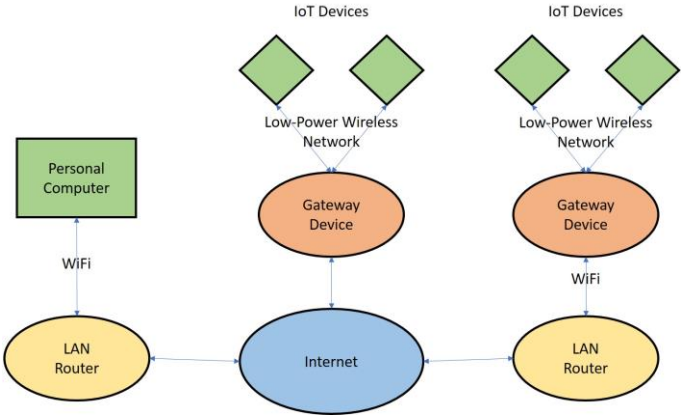

Figure 1. An example of a network of devices featuring IoT devices.

In the last 5 years, the IoT field has grown and is projected to continue growing rapidly; according to a report done by Business Insider, 34 billion devices will be connected to the internet by the year 2020. Of those 34 billion devices, 24 billion of them will be appliances or Internet of Things devices other than standard computers, smartphones, and tablets [7].

The Internet and its Design Flaws

The internet was originally designed as a system that relied on mutual trust; its architects assumed that users would be respectful of each other's data and privacy. As a result, security is not inherent to the internet. One effect caused by the principle of mutual trust is the lack of authentication for IP addresses. This leads to an opening for a hack called spoofing, where a hacker "pretends" to be another computer by using its IP address. Due to the design of the web, Internet-connected devices are designed to ignore any information that is not sent to their IP address. However, they have the ability to *packet sniff*, where one could still read the information sent to and from a device. A hacker can have the ability to potentially alter that data. In addition to the lack of built-in security, older computers and systems still connected to the internet can serve as easy openings for a malicious attack; they are "unpatched".

The Need for Securing IoT

Adding IoT systems, which tend to be composed of devices with either minimal computing power or very dedicated computing functionality (embedded systems) only exacerbates the flaws of the internet. These devices, being connected through communication networks, are subject to the same problems as other connected computing devices. They provide another place for a hacker to exploit system vulnerabilities for their own gain,

and potential harm of others.

All internet connected devices have an IP address, which includes small IoT devices, such as WiFi cameras and internet-connected baby monitors. The IP addresses allow every connected device to be able to be discovered from any location. If the device is "open", as it has no level of security, hackers can use exploits, such as Shodan.io, to gain access. As reported by ZDNet in an article about Shodan:

> *A quick scan either through paid or free membership using terms such as* port:554 has_screenshot:true *reveals cameras installed in places ranging from car parks in Japan to bars in France, private lounges in Korea to rabbit cages in Germany* [12].

Shodan works by taking advantage of devices that stream data without any sort of protection. Once finding an open stream, it takes a "snapshot" of the current stream. Devices like WiFi security cameras (ironically) and baby monitors are vulnerable to such exploits.

Unprotected devices connected to the web are a major security risk. It has been reported so far that hackers have managed to break into devices namely Google's Nest, the Belkin Smart Plug, Cayla Doll, LG refrigerators, Lifx light bulbs, and Smart TVs [6].

Attacks on these "things" and IoT systems as a whole can come through a number of ways due to lacking security. One notable method takes advantage of poor authentication credentials, such as a factory-default combination. A hacker is able to access the device, detectable due to an available IP address. Due to the weak credentials, the hacker is then able to gain control of the device. One now infamous example of an attack made possible due to this type of exploitation was the October 2016 DDoS (Distributed Denial-of-Service) attack:

> *On October 21, 2016, a major cyber attack took place that brought the internet to a halt. The hackers targeted the DNS (Domain Name System) provider Dyn by installing malicious software on WiFi cameras and other IoT devices. Everything from social media sites to news organizations was affected by the attack* [9][10].

This attack was made possible due to the use of the Mirai malware. Mirai works by tasking a computer to search the net for IoT devices and gain access to them by testing them against a list of default passwords and other credentials. Once in, the malware infects the IoT device to perform the same task. In the end, the hacker, who initially installed the malware, has the ability to control a large network of internet-connected devices without the awareness of their respective users. The hacker can then turn these into "zombies" to form a botnet; their IP addresses can be used to launch attacks, usually of the DoS/DDoS type. The October 2016 DDoS attack was done by a massive botnet composed of "things" created with the Mirai malware.

Mirai is not unique; there are similar malware out there that work in a similar manner. The fact that these infiltrate devices by using a table holding a collection of default username/password combinations points to a glaring vulnerability with current IoT devices: the user.

Mitigating the Problem

The simplest solution to fix most security problems is to change the username/password combinations once setting up a new device. This solution thus would rest on the users; it is their responsibility to change the passwords to something more unique. However, this is not unknown information; knowledge about the danger of keeping default passwords and/or using weak combinations (for example: using "password" as a password) is commonplace among tech-savvy people. With them, the issue is laziness. Ultimately, for those who are unaware of the risks, education is necessary; however, being aware is not enough to mitigate the problem. User action is required, and many would either forget to or just never change the credentials.

Instead, security can be implemented within the hardware and other parts of the software. For data security, encryption algorithms can be used. Most IoT devices tend to be low power systems running on very basic hardware. As a result, they have limited memory and computing power. Encryption algorithms have to be modified to be able to work with the limited resources while not sacrificing key functionality (secure, easily adaptable, etc). These "Lightweight Encryption Algorithms" are designed to be condensed versions of normal algorithms that still manage to provide the same outcome.

Encryption helps add data security, but for exploits such as Mirai, all that is needed is the IP address of the device. Once a hacker has access, all that is needed is to install the malware. One type of solution to prevent IoT devices from becoming part of a botnet involves implementing a degree of isolation; the local network on which the IoT devices are connected would need to be secured so that only certain requests could be routed to the devices. These devices would need to sit behind a firewall. Another possible solution would be to maintain the integrity of the firmware on the device; the "thing" would need to be able to detect and prevent attempts at rewriting what should be protected code.

The field of IoT is diverse; there are many systems that vary greatly in terms of specifications and purpose. There is no uniform hardware platform or software platform or other development platform that all IoT products confine themselves to use. Ultimately, solutions to the security problems with the Internet of Things would need to cater to specific products. Securing the Internet of Things requires much research and also rests on the need to educate the public about the dangers of factory-default passwords.

References

1. Arseni, S., Mitoi, M., & Vulpe, A. (2016). Pass-IoT: A platform for studying security, privacy and trust in IoT. Paper presented at the , *2016*- 261-266. doi:10.1109/ICComm.2016.7528258

2. Ray, S., Bhunia, S., Jin, Y., & Tehranipoor, M. (2016). Security validation in IoT space. Paper presented at the , *2016*- 1-1. doi:10.1109/VTS.2016.7477288

3. Schurgot, M. R., Shinberg, D. A., & Greenwald, L. G. (2015). Experiments with security and privacy in IoT networks. Paper presented at the doi:10.1109/WoWMoM.2015.7158207

4. Sitnikova, E., & Asgarkhani, M. (2014). A strategic framework for managing internet security. Paper presented at the 947-955. doi:10.1109/FSKD.2014.6980967

5. Voas, J. (2016). Demystifying the internet of things. *Computer, 49*(6), 80-83. doi:10.1109/MC.2016.162

6. http://ieeexplore.ieee.org.ezproxy.library.tufts.edu/document/7815675/authors

7. Greenough, J. (2016, July 18). How the 'Internet of Things' will impact consumers, businesses, and governments in 2016 and beyond. Retrieved September 15, 2016, from http://www.businessinsider.com/

8. Newman, L. H. (2016, October 21). What We Know About Friday's Massive East Coast Internet Outage. Retrieved November 04, 2016, from https://www.wired.com/

9. Woolf, N. (2016). DDoS attack that disrupted internet was largest of its kind in history, experts say. Retrieved November 04, 2016, from https://www.theguardian.com/technology/

10. Bonderud, D. (2016, October 4). Leaked Mirai Malware Boosts IoT Insecurity Threat Level. Retrieved January 8, 2017.

11. Wellers, D. (2015, November 27). Is this the future of the Internet of Things? Retrieved January 8, 2017.

12. Osborne, C. (2016, January 26). Shodan: The IoT search engine for watching sleeping kids and bedroom antics. Retrieved January 8, 2017.