Anatomy of an IoT DDoS Attack and Potential Policy Responses

In recent years, the impact and frequency of cyberattacks have significantly increased, from millions of personal records compromised to hundreds of millions and even a billion records in the case of Yahoo.[1] This has put both personal wealth (e.g., in the case of bank accounts, insurance information) and potentially human life (in the case of the US Office of Personnel Management hack, where personal information—including that of secret agents—was compromised, putting them at physical risk)[2] at risk on an unprecedented scale.

Meanwhile, the threat vector in the form of Internet-connected devices (Internet of Things [IoT]) has been utilized by hackers more extensively to direct extremely large distributed denial-of-service (DDoS) attacks at targeted companies to bring down their services. The strong emergence of the IoT threat vector needs to be properly understood in deliberations on the right type of policy and technology response to create defenses to protect data and systems. This article discusses popular definitions of IoT; current and future proliferation levels; a high-level anatomy of an IoT attack—in this case, the DYN attack; the business case for legislation; and the level and type of organized government intervention that may (unfortunately) be required.

What Is IoT and How Big Will It Get?

An interesting definition of IoT comes from the European Telecommunications Standards Institute (ETSI). It refers to IoT as "a dynamic global network infrastructure with self-configuring capabilities, where physical and virtual 'things' have identities, physical attributes and virtual personalities, and use intelligent interfaces to connect both between themselves and to data networks."[3] Additionally, the International Telecommunication Union (ITU) definition of IoT can be found in its recommendation ITU Y.2060. It states that an IoT "is an object of the physical world (physical things) or the information world (virtual things), which is capable of being identified and integrated into communication networks."[4]

Some examples of IoT devices include smart home applications such as Internet-connected thermostats, smoke alarms, Wi-Fi and electric bulbs. Internet-connected automobiles (e.g., the Tesla car) is another popular example.

Virtually every appliance and device can potentially be connected to the Internet. PricewaterhouseCoopers (PwC) research predicts that by the year 2020, anywhere between 30 to 50 billion devices will be connected to the Internet.[5] Such high levels of Internet proliferation can be incredibly beneficial to individuals, businesses and society at large by automating mundane jobs or making jobs more efficient and safe. It also provides a platform for innovation when combined with advancements such as cloud computing, robotics and smart grids, which renders the number of innovation permutations infinite. By 2020, the

Do you have something to say about this article?
Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

http://bit.ly/2vf0bNz

Hari Mukundhan, CISA, CISSP
Has 15 years of extensive cyber security, IT audit, IT operations, project and program management experience across a wide range of clients and businesses. He is currently a cyber security manager in a leading private organization. He can be reached at harimukundhan@yahoo.com.

global annual economic potential realized through productivity and innovation from machine and machine communication across all sectors will range from US $1.4 trillion to US $14.4 trillion.[6]

> “With great proliferation comes greater concerns about whether these devices can be leveraged to expose behavior patterns, compromise physical safety and security, or even launch an Internet attack on a given target.”

With great proliferation comes greater concerns about whether these devices can be leveraged to expose behavior patterns, compromise physical safety and security, or even launch an Internet attack on a given target. For example, an innocuous-looking Wi-Fi-connected light bulb can be made to talk to another connected light bulb and both can be enslaved to launch a DDoS attack. One such attack that happened in 2016 almost brought down the Internet.

Anatomy of a Recent Cyberattack Using IoT Devices

On 21 October 2016, at approximately 6:00 am CST (UTC -6), Internet users in the eastern portion of the United States were unable to access some of the top and most visited sites such as Twitter, PayPal and Amazon. This was due to a coordinated DDoS attack[7] on DYN, a domain name service (DNS) company. At a high level, DNS resolves website names to IP addresses at the back end, while hiding the complexities from the end user. Without DNS, users would have to remember the IP address for a website instead of the website name itself (a much more difficult prospect).

While DDoS attacks have been happening for a long time, what was peculiar about the attack on DYN was the size of the attack (which was unprecedented in its scale and seriousness), how it was attacked and, more importantly, why it was attacked.

A typical denial-of-service (DoS) attack overwhelms the web server resources with so many requests from one computer connected to the Internet—for example, a flood of Internet Control Message Protocol (ICMP) ping requests—that the server is so busy responding to the pings that it does not have enough resources to respond to legitimate requests from users and, thus, returns an error message (e.g., 404 Page Not Found). This may make an organization unable to offer its services to its customers, leading to potentially significant financial, operational, reputational and legal risk.

On a larger scale, if the attacker uses not just one computer, but thousands of unique IP addresses, it is considered to be a distributed DoS, or DDoS, attack. In terms of numbers, an average DDoS attack size, according to an Arbor Networks study, was 986 Mbps in the first half of 2016, with the largest attack clocking in at 579 Gbps.[8] It is worthwhile to note that an attack of one Gbps is considered large enough to take most organizations offline. At such high volumes, it is also quite difficult to discern which IP address is legitimate and which is not, making it that much more difficult to fend off.

TCP SYN Flooding

So, what is a DDoS attack? One of the more common types of DDoS attack is TCP SYN flooding,[9] which exploits an inherent vulnerability in the Transmission Control Protocol (TCP),[10] a set of rules to establish and maintain a reliable conversation between two computers over the Internet.

When one computer (a client, e.g., a laptop), attempts to connect to another computer (a server, e.g., a website), a series of messages, or data packets, is first exchanged between the two to establish reliable connectivity over the Internet.

First, the client requests a connection to the server via a SYN message. The server then acknowledges the request via the SYN-ACK message back to the client. The client then responds back with an ACK message, thereby establishing a connection between the client and the server, i.e., a laptop and a website. This is called a TCP three-way handshake (**figure 1**).[11]

In the case of TCP SYN flooding, the client sends the SYN message and receives a SYN-ACK from the server, but does not respond back to the server with an ACK message. The server waits for the ACK message for some time before moving on. However, precious server resources are consumed during this process and, during that time, while it waits for the ACK message, it cannot respond to legitimate requests from other clients. If the number of such client requests exceeds a server's capacity to process them, the server is overwhelmed and will become unavailable, i.e., it denies service to the users (DoS).

Another variant of this attack is the client falsifying its IP address (also known as IP spoofing) so that the server sends a SYN-ACK to the spoofed IP address in the original SYN message it received, and the spoofed IP address never responds with an ACK message because it never sent a SYN message to the server in the first place. In the case of the DYN attack, it is not entirely clear what type of DDoS attack was launched, but the Mirai botnet, a cluster of 100,000 or so compromised and enslaved IoT devices, was configurable to deliver different types of DDoS attacks, including TCP SYN flooding.[12]

Attack Delivery Model—Mirai Botnet

As defined by Kaspersky Labs, "The word Botnet is formed from the words 'robot' and 'network.' Cybercriminals use special Trojan viruses to breach the security of several users' computers, take control of each computer and organize all of the infected machines into a network of 'bots' that the criminal can remotely manage."[13]

The key features of the Mirai botnet are that the source code was designed to recruit hundreds and thousands of IoT devices and the source code was released[14] a few days before it was used[15] for the DYN attack. DYN disclosed that probably 100,000 IoT devices[16] (scaled down from tens of millions), such as digital video recorders and closed circuit television cameras, were used for the attack. Moreover, it was simplified to a point that script kiddies launched the attack, not advanced persistent threats, such as state actors, that people usually tend to imagine.

DDoS as a Service: Threat Capability, Motives and Likely Frequency

So, what does the DYN attack mean to the Internet? What were the attackers' motives? How capable is the botnet/IoT DDoS threat, and how frequent and large can it become?

The Mirai botnet's source code is now being incorporated into 12 other botnets since the

Figure 1—A Typical TCP Three-way Handshake

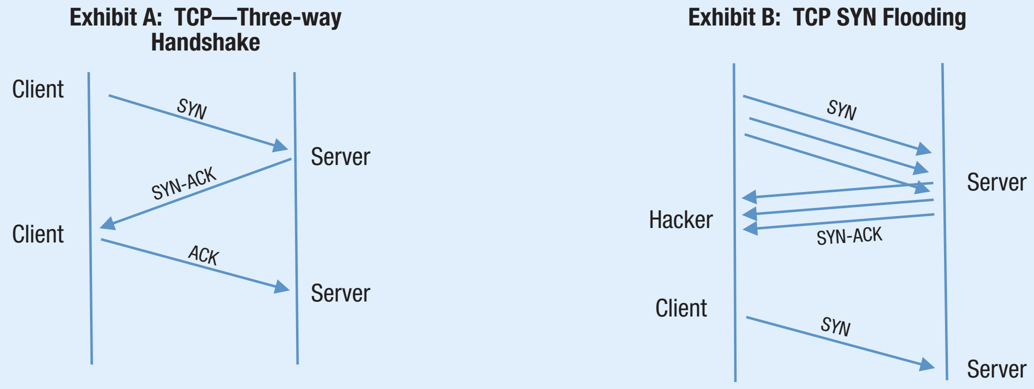
Exhibit A: TCP—Three-way Handshake

Exhibit B: TCP SYN Flooding

Enjoying this article?

- **Read *Internet of Things: Risk and Value Considerations*.** *www.isaca.org/internet-of-things*
- **Learn more about, discuss and collaborate on information security policies and procedures in the Knowledge Center.** *www.isaca.org/information-security-policies-and-procedures*

code was released. Botnets will now be readily available to provide DDoS services for customers with malicious intent.[17] As the number of available IoT devices increases, perpetrators will have that many more devices to enslave via readily available botnets[18] or DDoS services with which they can launch unprecedented attacks.

The motivations to launch an attack are numerous. They can range from an enemy country launching an attack for political reasons to a competitor or an angry employee launching an attack against a company to a cybercriminal trying to extract ransom from a wealthy company. It could even be a political or cyberwar situation, wherein a state or a nonstate actor with advanced capabilities can carry out a large-scale coordinated attack to bring down access to the Internet for a large number of people.

“As the number of available IoT devices increases, perpetrators will have that many more devices to enslave via readily available botnets or DDoS services with which they can launch unprecedented attacks.”

Market Failure—A Key Cause

IoT products are widely believed to be weak on security, with easily guessable passwords and unsecured ports. Security journalist Brian Krebs reports being able to identify many of the IoT vendors using easily guessable usernames and passwords.[19] Moreover, many vendors do not provide an interface to change passwords nor do they update the firmware, leaving these devices highly vulnerable to attack.

Since there are no statutory or market requirements for IoT vendors to develop secure devices, and since such an effort will surely increase the manufacturing cost, vendors are not competing to create secure products. This can, therefore, be considered a market failure that calls for some level of government intervention to ensure that baseline security for the device is present. To quote the well-respected Bruce Schneier:

> *The market can’t fix this because neither the buyer nor the seller cares. Think of all the CCTV cameras and DVRs used in the attack.... The owners of those devices don’t care. Their devices were cheap to buy, they still work.… The sellers of those devices don’t care: They’re now selling newer and better models, and the original buyers only cared about price and features. There is no market solution because the insecurity is what economists call an externality: It’s an effect of the purchasing decision that affects other people. Think of it kind of like invisible pollution.*[20]

Smart Regulations

The success of the Internet is largely due to its openness to collaboration and innovation without government intervention. In the United States, there were no Internet regulations up until 2015, when lawmakers decided to address net neutrality.[21] Therefore, careful thought has to be given to the type and level of government intervention that now appears to be warranted in the IoT space to overcome a market failure while at the same time not stifling innovation.

Following are some of the key aspects to consider when drafting the regulations:

IoT security standards
A minimum baseline of IoT security standards should be introduced, along with a mechanism for vendors to demonstrate compliance with the standard, i.e., certification of compliance. The standards should be internationally applicable and involve all the stakeholders, e.g., government, civil society, IoT vendors, academia and other private companies. But it should also be noted that while having a few security standards would probably raise

the overall security bar, it is definitely not a guarantee against getting hacked. In the United States, active discussions seemed to have kicked off with the US Department of Commerce soliciting feedback[22] on formulating an approach to betterment of IoT. The US Federal Trade Commission (FTC) has basic security guidelines for IoT products.[23]

A few IoT standards and guidelines are emerging:

- IoT Security Guidance by the Open Web Application Security Project (OWASP) provides guidance to help manufacturers build more secure products in the IoT space.[24]
- Strategic Principles for Securing the Internet of Things (IoT), from the US Department of Homeland Security, provides a set of nonbinding principles and suggested best practices to build responsible levels of security in the IoT space.[25]
- Security Solutions, One M2M Technical Specification, defines security specifications in the IoT space.[26]
- The Alliance for Internet of Things Innovation by the European Commission addresses standardization, interoperability and policy issues in the IoT space.[27]
- The Institute of Electrical and Electronics Engineers (IEEE) "has created a number of standards, projects, and events that are directly related to creating the environment needed for a vibrant IoT."[28]

Legal Foundational Components

For standards to be effective, the following legal foundation components need to be established consistently across both buyer and seller markets:

- **Market access laws**—Countries should enact laws that will allow market access only to security-certified products that are in compliance with globally acceptable IoT baseline security standards. However, this has the risk of increasing the cost of the product and putting it out of reach of some or many consumers.

- **Enforcement**—A compromised IoT has the potential to directly impact day-to-day life not only by disrupting routine, but also by posing significant safety risk. Examples include a remotely disabled carbon monoxide detector or a device taking control of a car. In 2015, researchers were able to take complete control of a Jeep Cherokee remotely while it was driving at a high speed.[29] In fact, the DEF CON Hacking Conference has a dedicated section just for car hacking.[30] Given such heightened concerns, the role of enforcing existing and new laws and standards needs to be thought through. Will consumers buy only devices they know are secure? Would they care enough to result in vendors that create unsecure devices being driven out of the market? Will standards, legislation and enforcement be effective to reduce the number of unsecured products in the market? Or will compliant products actually attract the determined hacker who would like to delegitimize the regulations? Only time will provide the answer as the market matures.

- **Product recalls**—After the Jeep Cherokee hack was demonstrated by researchers in *Wired*,[31] Chrysler recalled 1.4 million vehicles to update their software since it posed a significant risk to human lives.[32] That raises questions about what would require a product recall. Would a recall apply to only the products that threaten human safety or health, or should it also apply to products that threaten privacy, national security, etc.? Should product recalls be applied retroactively? For example, if an individual bought an Internet-connected thermostat two years ago and it is not compliant with a newly released regulation, can the person get the product

> **"Since there are no statutory or market requirements for IoT vendors to develop secure devices, and since such an effort will surely increase the manufacturing cost, vendors are not competing to create secure products."**

updated? And if the product's firmware cannot be updated, are there technological solutions available to block such devices from the Internet—and is it even fair and legal to do so? By the way, the complexities of recall may increase as the number of devices multiplies into millions and billions. Many complex concepts need to be taken into consideration while formulating policies.

- **Globally coordinated efforts**—Whatever form the regulation takes, one thing is certain: It has to be a globally coordinated effort. A country can create draconian laws or simply decide to keep IoT open for all, but the threat posed may come from the outside as long as the country decides to stay connected to the Internet in some form. For example, IoT devices may be produced in country A, consumed in country B, enslaved by hackers in country C and used for attacking DNS servers in country D. Therefore, major consumer and producer countries and all major countries that are connected to the Internet should be at the table to create a global framework to define operation in this space.

> **“Major consumer and producer countries and all major countries that are connected to the Internet should be at the table to create a global framework to define operation in this space.”**

Conclusion

This is an age in which machine-to-machine communication is expanding significantly, creating new types of cyberrisk or exacerbating existing risk, thus impacting not only privacy and wealth, but also human safety. Such a transformation of the environment requires IS professionals to maintain a solid understanding of the technologies and risk involved so that appropriate levels of controls can be built not only at the IoT product level, to ensure that the product meets an internationally acceptable standard, but also at the organizational network level, to protect against attacks that can be launched by these devices. In addition, global coordination by nation states, professional organizations, standards bodies, corporations, academia and civil society would be required to craft the right level of policy responses to safeguard against this newly emerging attack vector.

Endnotes

1 Goel, V.; N. Perlroth; “Yahoo Says 1 Billion User Accounts Were Hacked,” *The New York Times*, 14 December 2016, *https://www.nytimes.com/2016/12/14/technology/yahoo-hack.html?_r=1*

2 Hirschfeld Davis, J.; “Hacking of Government Computers Exposed 21.5 Million People,” *The New York Times*, 9 July 2015, *https://www.nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html?_r=0*

3 ETSI, “Standards for an Internet of Things: A Workshop Co-organized by EC DG Connect and ETSI,” 3-4 July 2014, *www.etsi.org/news-events/events/771-2014-etsi-ec-dg-connect-iot*

4 International Telecommunication Union, “Y.2060: Overview of the Internet of Things,” 15 June 2012, *www.itu.int/rec/T-REC-Y.2060-201206-I*

5 Chitkara et al.; “The Internet of Things: The Next Growth Engine for the Semiconductor Industry,” PricewaterhouseCoopers, May 2015, *www.pwc.com/gx/en/technology/publications/assets/pwc-iot-semicon-paper-may-2015.pdf*

6 Schindler, H.R., *et al*.; *Europe's Policy Options for a Dynamic and Trustworthy Development of the Internet of Things*, RAND Europe, 2013

7 York, K.; “Dyn Statement on 10/21/2016 DDoS Attack,” Vantage Point, 22 October 2016, *http://dyn.com/blog/dyn-statement-on-10212016-ddos-attack/*

8 Arbor Networks, “Arbor Networks Releases Global DDoS Attack Data for 1H 2016,” press release, 19 July 2016, *https://www.arbornetworks.com/arbor-networks-releases-global-ddos-attack-data-for-1h-2016*

9 CERT Software Engineering Institute, "TCP SYN Flooding and IP Spoofing Attacks," 19 September 1996, *https://www.cert.org/historical/advisories/CA-1996-21.cfm?*

10 TechTarget, "TCP (Transmission Control Protocol)," *http://searchnetworking.techtarget.com/definition/TCP*

11 Techopedia, "Three-way Handshake," *https://www.techopedia.com/definition/10339/three-way-handshake*

12 Symantec, "Mirai: What You Need to Know About the Botnet Behind Recent Major DDoS Attacks," 27 October 2016, *https://www.symantec.com/connect/blogs/mirai-what-you-need-know-about-botnet-behind-recent-major-ddos-attacks*

13 Kaspersky Lab, What is a Botnet?, *https://usa.kaspersky.com/resource-center/threats/botnet-attacks*

14 Krebs, B.; "Source Code for IoT Botnet 'Mirai' Released," Krebs on Security, 1 October 2016, *https://krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released/*

15 Woolf, N.; "DDoS Attack That Disrupted Internet Was Largest of Its Kind in History, Experts Say," *The Guardian*, 26 October 2016, *https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet*

16 Hilton, S.; "Dyn Analysis Summary of Friday October 21 Attack," Vantage Point, 26 October 2016, *http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/*

17 Krebs, B.; "Alleged vDOS Proprietors Arrested in Israel," Krebs on Security, 10 September 2016, *http://krebsonsecurity.com/2016/09/alleged-vdos-proprietors-arrested-in-israel/*

18 Mathews, L.; "World's Biggest Mirai Botnet Is Being Rented Out for DDoS Attacks," *Forbes*, 29 November 2016, *https://www.forbes.com/sites/leemathews/2016/11/29/worlds-biggest-mirai-botnet-is-being-rented-out-for-ddos-attacks/#32473c2f58ad*

19 Krebs, B.; "Who Makes the IoT Things Under Attack," Krebs on Security, 3 October 2016, *https://krebsonsecurity.com/2016/10/who-makes-the-iot-things-under-attack/*

20 Schneier, B.; "Lessons From the Dyn DDoS Attack," Schneier on Security, 8 November 2016, *https://www.schneier.com/blog/archives/2016/11/lessons_from_th_5.html*

21 Pagliery, J.; "FCC Adopts Historic Internet Rules," CNNMoney, 26 February 2015, *http://money.cnn.com/2015/02/26/technology/fcc-rules-net-neutrality/index.html*

22 National Telecommunications and Information Administration, *Fostering the Advancement of the Internet of Things*, USA, 12 January 2017, *https://www.ntia.doc.gov/other-publication/2017/green-paper-fostering-advancement-internet-things*

23 Federal Trade Commission, *Careful Connections: Building Security in the Internet of Things*, USA, January 2015, *https://www.bulkorder.ftc.gov/system/files/publications/pdf0199-carefulconnections-buildingsecurityinternetofthings.pdf*

24 Open Web Application Security Project, IoT Security Guidance, *https://www.owasp.org/index.php/IoT_Security_Guidance*

25 Department of Homeland Security, *Strategic Principles for Securing the Internet of Things (IoT)*, USA, November 2016, *https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf*

26 OneM2M, *OneM2M Security Solutions*, 1 August 2014, *http://onem2m.org/images/files/deliverables/TS-0003-Security_Solutions-V-2014-08.pdf*

27 Alliance for Internet of Things Innovation, *https://aioti-space.org/*

28 Institute of Electrical and Electronics Engineers Standards Association, "Internet of Things," *http://standards.ieee.org/innovate/iot/*

29 Greenberg, A.; "Hackers Remotely Kill a Jeep on the Highway—With Me in It," *Wired*, 21 July 2015, *https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/*

30 Hern, A.; "Car Hacking Is the Future—and Sooner or Later You'll Be Hit," *The Guardian*, 28 August 2016, *https://www.theguardian.com/technology/2016/aug/28/car-hacking-future-self-driving-security*

31 *Op cit,* Greenberg

32 Goldman, D.; "Chrysler Recalls 1.4 Million Hackable Cars," CNNMoney, 24 July 2015, *http://money.cnn.com/2015/07/24/technology/chrysler-hack-recall/*