DDoS and IoT:
How You Could Have Contributed to Breaking the Internet

Timothy Ho
Introduction to Computer Security
Fall 2016

Mentor: Ming Chow

Abstract

Distributed denial-of-service (DDoS) attacks have been increasingly common in recent years and are frequently used to target businesses, financial institutions, and other services to block and disrupt communications and normal everyday operations. This paper covers and explains basic concepts how using Internet of Things (IoT) devices to perform such DDoS attacks can be used to take down large target servers, as evidenced by the attack on Dyn in October of 2016. While knowledge and awareness of DDoS and IoT has been rising, an encompassing goal of this paper is to increase and promote awareness of these issues, vulnerabilities, and computer security as a whole.

Introduction

On October 21, 2016, a large cyberattack was directed towards servers owned by Domain Name Service (DNS) provider Dyn. As a result, many major websites and services were made unavailable to a large number of users across North America and Europe. Some of the services that were affected included major well-known companies and social media and news platforms such as Amazon, BBC, CNN, GitHub, Reddit, SoundCloud, Spotify, and Twitter. The massive Internet outage lasted for hours and it was later discovered that hacked cameras and other Internet of Things (IoT) devices were used to perform a large distributed denial-of-service (DDoS) attack against the Dyn servers. Many found themselves asking these questions afterwards: How did this happen? Who was behind this? And how could a single cyberattack result in damage that affected millions of users?

To the Community

This paper is not merely directed towards those who are involved with computer security or careers in computer science; it is *especially* directed towards members of the general public. For those who are not aware, DDoS attacks and even the specific networked program to control IoT devices, Mirai, are not new occurances. In fact, it was just one month earlier that the website of well-known security journalist Brian Krebs, *krebsonsecurity.com*, was targeted by the very same malware.

This topic was chosen because after many years of repeated and similar cyberattacks over the Internet, things have not changed to prevent more of the like in the future from happening again. This topic is important for all users to know because computer security is the responsibility of everyone, not just

those in charge of information and computer security. From software developers and web engineers to everyday users of the Internet and its connected devices, it is imperative that everyone understands the risks of security breaches in hopes of creating a safer environment as the world inevitably becomes more dependent on technology.

One of the major goals of this paper is to educate and promote awareness of issues surrounding the security of IoT and its vulnerabilities that can be exploited for DDoS. The first few sections will delve into basic concepts and explain what DNS is, outline the structure of a DDoS attack, and illustrate the increasing prevalence and potential dangers of IoT devices in order to build a basic understanding of what happened to the Dyn servers last October. The paper will then offer several action items and defense strategies to the developer and everyday user alike so that future attacks can at least be somewhat mitigated or have less strength to draw upon. Finally, the conclusion will wrap up the discussion by questioning our world's increasing reliance on wireless technologies and ask whether trading convenience for security is truly worth it.

What is DNS?

DNS, or Domain Name Service, is an underlying application service that millions of users utilize each day and probably don't even realize it. Webpages, internet applications, and other services are stored on various servers around the world that contain, or host, the data that we want. Each of these servers has an IP address, traditionally a set of four numbers between 0 and 255, which acts very much like an actual mailing address. All computers, devices, and routers/access points are addressed in a similar fashion as well. But when a user types an address like *www.google.com* or *amazon.com*, these names are actually translated by DNS underneath the web browser to the actual IP address of a Google or Amazon server, usually something like <139.130.4.5>. This allows humans to recognize and remember servers and websites with an English-sounding name more easily than a set of seemingly four random numbers that computers are able to recognize.

DNS as a service plays a critical role for almost the entire Internet to function and without it, many websites and services would be inaccessible without prior knowledge a server's IP address that can move around and change over time. This was the case for the Dyn attacks because their servers provide DNS for all of the websites listed in the introduction (and many more). There are hosts of DNS servers

around the world organized geographically and are presumably expected to handle high traffic loads because DNS is such a widely and frequently used service. If this is the case, how could such a large and important set of these servers get taken out so easily? The answer is a distributed denial-of-service attack or DDoS.

What is DDoS?

In order to explain DDoS, it would be best to illustrate the concept of denial-of-service with an analogy. According to a Cisco paper, a denial-of-service attack is "a malicious attempt by a single person or a group of people to cause the victim, site, or [access point] to deny service to its customers." This is typically done by exhausting the computing resources of the target in order to block others from accessing it. Imagine a long line at a fast food restaurant where customers line up and wait for a few workers that can process orders and deliver the correct food. From the mindset of an attacker, how would someone, a competitor or malicious person, devise a strategy to stop others from going to this restaurant? Using this analogy, a typical denial-of-service would involve methods such as getting enough people to fill the line to block others from entering the restaurant or hiring people to complain to the cashiers and waste as much time as possible to frustrate others in line to the point of giving up and being denied their service.

Computer servers work very much the same way – each one has limited resources where queues and bandwidth act as the line length and restaurant space to process orders. An attacker can overwhelm the server by flooding it with network packets and requests. What makes a denial-of-service attack so effective is that an attacker can hide behind a fake IP address or a proxy to conceal where the attack is truly coming from. However, there is seemingly only so much one person or one computer can do against a target. This is where the idea of a *distributed* denial-of-service comes in. Going back to the analogy, each person is probably limited in how many people they can know or hire to block the restaurant lines. But what if someone had the ability to hire a network of people or mercenaries to control hundreds or thousands of others that would take orders without question? This leads into Cisco's exact definition of a DDoS attack, one that "takes place when many compromised machines infected by the malicious code act simultaneously and are coordinated under the control of a single attacker in order to break into the victim's system, exhaust its resources, and force it to deny service to its customers." A visualization of this concept is shown in the figure below.

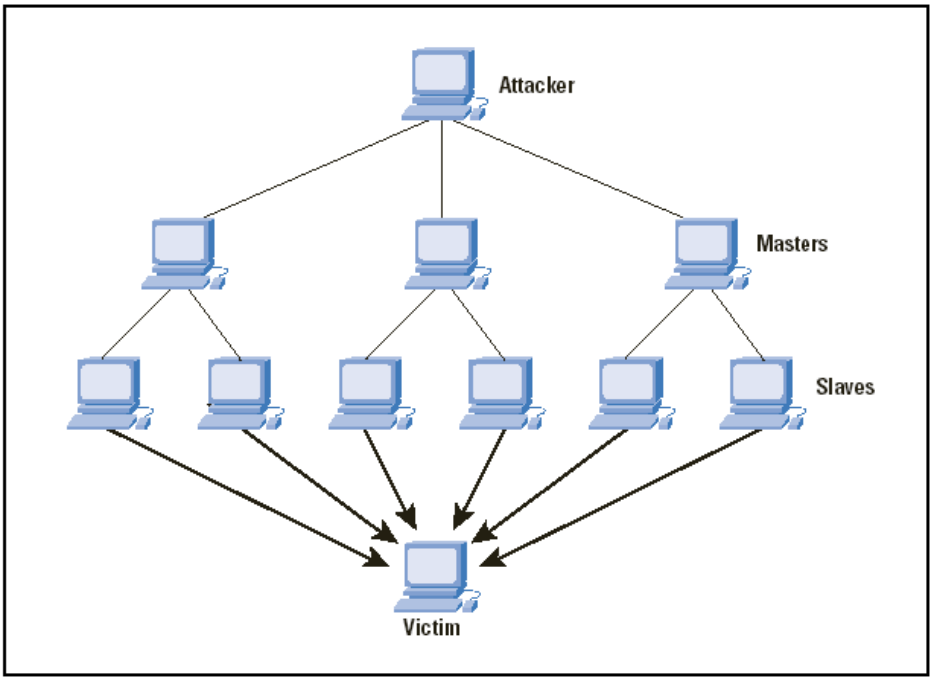

Figure 1: Illustrating the visual concept of a DDoS attack

Unfortunately, the concept of a DDoS attack is nothing new – the Cisco paper was written at the end of 2004 and many such attacks have occurred long before and after its publication. Defense strategies against these attacks have continued to prove challenging although many large companies can simply throw more resources at the problem such as larger servers and more bandwidth. This leads back to the original question: How could large-scale and important DNS servers like Dyn be susceptible to a DDoS attack? This leads to the final part of the equation, the Internet of Things or IoT.

What is IoT?

The Internet Society published a comprehensive document in October 2015 about the Internet of Things and its expected massive growth within the next decade and beyond. While the term is relatively new, the concept is fairly basic. IoT has become "a popular term for describing scenarios in which Internet connectivity and computing capability extend to a variety of objects, devices, sensors, and everyday items" (Rose, et al, 14). In other words, it describes the increasing movement to have more devices connected to the Internet for improved service and usability. Rose predicts that over 100 billion devices will be connected to the internet by 2025 and Cisco points out that almost 70% of internet traffic will be generated by non-PC devices by 2019. Such statistics are understandable given the explosion and growth of phones, tablets, and other devices to access websites and services over the last decade.

Proponents of IoT point out that connected devices can offer better services and more convenience for customers. Examples of IoT include internet-connected medical devices, security cameras, retail devices, vehicles, and many more. NBC News recently published a story that car companies are looking to transmit wirelessly to each other to prevent accidents and other incidents too quick for a human to react to. While many of these benefits sound promising, we have unfortunately traded away security and privacy for convenience and a reliance on technology. What if someone was able to break in and compromise even a fraction of these billions of devices? Stealing data is already enough of a crime but what if someone put them to use for malicious purposes, perhaps using them for DDoS attack?

Following the attack of the Dyn servers, investigations pointed out that a coordinated attack from thousands of devices such as cameras, printers, baby monitors, and many others was used to deliver the DDoS attacks. Specifically, a piece of malware called Mirai was used to infect IoT devices and coordinate an effort that delivered roughly 1.2 terabits per second to overwhelm servers. The code for Mirai was released prior to the October incident and Incapsula published a detailed analysis of it and its ramifications. According to the analysis, Mirai's two main objectives are to "locate and compromise IoT devices to further grow the botnet" and "launch DDoS attacks based on instructions received from a remote command and control." What is probably most concerning about the analysis is that Mirai was able to break into these devices because many of them contained passwords that had not been changed from their original factory settings or were simply given "easily guessable" passwords that could be broken by a brute force dictionary attack. In other words, if someone uses a common English word for a password, a computer can use a dictionary to check every possibility and break in with relative ease. It this major flaw in our devices and usage that leads to action items and defense steps that should be taken seriously.

Action Items & Defenses

What are steps that can be taken to prevent large-scale DDoS attacks in the future? As stated earlier, DDoS has been around for some time and is likely here to stay unless major changes to current Internet architecture is changed. Gu *et al* points out in their 2007 paper many techniques that have been used to stop DDoS such as implementing firewalls, filters, and tweaks with router and packet implementation. For those in the networking and security fields, this area of research must continue to be pursued and perhaps a taking a long look at our current but aging IP/TCP networking structure is necessary to cope with the new demands and high loads of web traffic that are coming from billions of small devices. For

those in software development, an emphasis on security and liability for products must be stressed. Too often these days and especially with the growing IoT appetite, companies rush out more and more products in attempts to corner a new market and fail to take time to address flaws, defects, and security concerns. This applies to anyone involved with computer science and CS education – it must be the responsibility of everyone in the field to help increase awareness of security flaws and the lack of this emphasis in our current computer science curriculums across high schools and colleges across the world.

There are also simple action items for the everyday person not involved with computers or software development at all. *Welivesecurity* and *Incapsula* both published a small list of steps everyone can take after analyzing the October Dyn attacks. The easiest step most commonly suggested is for users of home routers and IoT devices is to use secure passwords and not be lazy by simply leaving the factory set password or using common passwords like “password”, “admin”, and “12345.” Many websites enforce the use of mixing characters and numbers with non-English words but this must be carried over to devices as they become more prevalent. Other practical steps include disconnecting devices when not in use or making sure IoT devices are bought “from companies with a reputation for providing secure devices” (Incapsula). These seem like small, insignificant steps but with billions of vulnerable devices that can potentially be broken into, the sum of these small action items can make a big difference. Continuing to make users and the general public more aware of security vulnerabilities should be the highest priority moving forward. Again, as evidenced by the IoT flaws exploited for the use of DDoS against DNS servers, security is the responsibility of everyone. If we can all work together instead of blaming or passing on the responsibility to others, perhaps things can improve on the security front for the future.

```
root     12345
user     user
admin    (none)
root     pass
admin    admin1234
root     1111
admin    smcadmin
admin    1111
root     666666
root     password
root     1234
```

Figure 2: A portion of a small list of passwords that Mirai used to break into thousands of devices

Conclusion

In conclusion, this paper has shown basic principles and concepts of security vulnerabilities and what practical steps can be taken to prevent such occurrences in the future. However, the deeper issue that should be raised from all these concerns is looking at our evolving world and how we as a society continue to rely more on technology. IoT spawned out of a need to synchronize and use devices in a way that make our lives more convenient. Technology has many benefits and the use of customized data can help provide better services to people. But at what cost are we all paying for comfort and convenience? The topic of information privacy was not touched at all in this paper but very much applies to all the issues tied to IoT. DDoS attacks currently provide a relatively minor hindrance and inconvenience to the services we use. However, as technology moves forward where cars, airplanes, power plants, and other devices that affect life and death are involved, how much damage could one cause with security vulnerabilities in those areas? It would be naïve to suggest the world to stop connecting devices or stunt the growth of technology. At the same time, it would be wise to take a step back and question how much convenience, customization, or comfort we truly want in our devices and services before realizing how dangerous desiring these things can really be.

Citations & References

Charalampos Patrikakis et al, 2004 “Distributed Denial of Service Attacks - The Internet Protocol Journal - Volume 7, Number 4” Cisco
http://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-30/dos-attacks.html

Stephen Cobb, 2016 “10 things to know about the October 21 IoT DDoS attacks” WeLiveSecurity
http://www.welivesecurity.com/2016/10/24/10-things-know-october-21-iot-ddos-attacks/

Qijun Gu et al, 2007 “Denial of Service Attacks”
https://s2.ist.psu.edu/paper/ddos-chap-gu-june-07.pdf

Karen Rose et al, 2015 “The Internet of Things: An Overview” Internet Society
https://www.internetsociety.org/sites/default/files/ISOC-IoT-Overview-20151221-en.pdf

Ben Herzberg et al, 2016 “Breaking Down Mirai: An IoT DDoS Botnet Analysis” Incapsula
https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html