Securing the Future: Cyber Security Education

Lauren Horton and Maria Heredia
Derek Phanekham
CS 3339

Abstract

Attacks can come at any time from anywhere. With such insecurity on the internet, is it even possible to defend against hackers? Can everyday people prevent or at the very least deter hackers without having to spend hundreds of dollars on cyber security software? In this paper we will take a look at cyber attacks like DOS, MitM, Phishing, and Malware and how educating the public could help prevent the success of these attacks. DOS, or Denial of Service, floods a system's resources with other requests so that the system can't respond to a user's request. In this way, an attacker can handicap a system as a precursor to a larger, more direct attack. MitM, as Man-in-the-Middle attack is known, occurs when an attacker inserts himself in between, or in the middle of, a client and a server. The MitM can then hijack the client's requests and force the client to go through the attacker to connect to the server versus connecting directly to the server. Phishing is another form of a cyber attack commonly seen in emails where an email appears to be sent from a trusted source. However, attackers send attachments and hyperlinks in these emails to access a user's private information such as passwords, bank accounts, and social security. Lastly, malware attacks are unsecured software that is installed without the consent of the computer's user. Two of the most common malware attacks are done via viruses and ransomware. Viruses infect a computer's host files where the virus replicates throughout the computer, whereas ransomware attacks blocks access to a computer system until the money demanded is paid. It is important to be educated about these cyberattacks in order to keep information private and secure, since the world is evolving from hardware to software.

What Is It?

Denial of Service

One of the most common attacks is a Denial of Service (DoS). Even not thinking about that phrase in a cyber security sense, it's very easy to see why that is such a popular attack. People need things on a daily basis. They rely on service to get them what they need, and when someone interrupts that, people are left bereft. They're left with a problem and they still have an unmet need. They become vulnerable. With millions of different kinds of services, it's also easy to see how it can be hard to prevent. DoS is usually instigated by an attacker flooding a network server with traffic. Basically, the attacker overloads the server with faux service requests, but the server doesn't know to ignore the requests, and so it tries to follow through. The server is misled - instead of going to the actual requestor, it goes to the illegitimate return address, but since that address can't be authenticated, the server becomes overwhelmed, trying to process all of the fabricated requests. Distributed Denial of Service (DDoS) takes this attack one step further - it uses multiple machines to attack one target. DDoS attackers use botnets, or a group of compromised devices, to execute a much larger attack. DDoS is more dangerous because it becomes much harder to pinpoint the chief provocateur and the attack's power is increased with many machines infected to carry out the intrusion [1].

Man in the Middle

Like Denial of Service, the name of the attack seems pretty self-explanatory. A "man" is in the middle of two entities - although in cyber security terms, this is a place he is not supposed to be. For instance, say Alice sends a letter to Bob. But Eve, a worker at the post office, intercepts the letters. She can read them and even edit those private letters before sending them on their way to Bob. Thus, Alice thinks she's talking privately to Bob and Bob thinks he's talking to Alice, but in reality, their communications have been hijacked by Eve. This is what a Man-in-the-Middle (MitM) attack does.

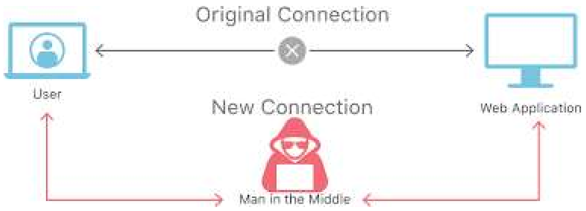

Figure 1: Man in the Middle Attack Diagram
Source: [4]

An attacker can receive a lot of information in this way. Maybe the user is logging into the website - the attacker can get the username and password for that website. The likelihood is also very strong that that username/password combination are reused for many different accounts… say a bank account. Alternatively, an attacker could steal a user's cookies, the pieces of data a website collects and stores on the user's machine. Then later on, the attacker can use that information to impersonate the user and get further information from the website. Usually, this attack happens over public WiFi. A hacker can go to a place where public WiFi is offered and set up his own free WiFi, naming it something to lure people to log on to it (e.g., if the actual WiFi was called "CafeX", the attacker could name his network "CafeX - Guest"). Once a user has logged onto the malicious network, the hacker can sniff the packets processed by the user's computer, essentially looking through everything the user looks through [4].

Phishing

Phishing is one of the most popular cybercrimes being committed nowadays. This cybercrime attack is committed by contacting people through emails, phone calls, text messaging, and other electronic communication ways. The attacker impersonates a trusted source and lures individuals to provide them with their personal information which can include everything from a social security number to a bank account's routing number [6]. Phishing attacks can be seen in 3 different ways: email phishing, vishing and smishing. For email phishing, attackers usually send a link that takes the user to an illegitimate website that downloads malware in order to gain information. Vishing is known as "voice phishing" meaning that attackers impersonate businesses in order to get information via phone calls. This is commonly seen where attackers create a fake caller identification and ask for personal information online. An example of a call may sound like "Your account has been compromised. Please call this number to reset your password" or "Your extended car warranty has been expired. Please call back this number to renew your warranty" [7]. The purpose of these calls is to leave alerting voicemail in order to incite panic to the person being called so they can easily give their personal information. Lastly, smishing is "messaging phishing" which is very similar to vishing. Compared to vishing, smishing is attackers contacting via text messages where they are looking to gain personal information [8]. These phishing text messages often come from numbers that do not look like a real phone number such five digit numbers. Ultimately, attackers practice social engineering in order to successfully take advantage of people. Social engineering focuses on the art of manipulation where attackers try to obtain personal information through technology [9]. In addition, spear phishing is a very popular method for attackers to practice. Spear phishing is just like phishing, but the attackers have a specific target they are trying to steal from [10]. These attackers research the victim and try to send specific websites and links in which the victim is likely to open. Overall, phishing is a cybercrime that involves social engineering and manipulation in order to successfully steal personal information.

Malware

While phishing is the art of manipulation users, malware attacks refers to the actual software being installed in a computer without having the user consent. Malware attacks are seen in the form of different viruses, software, and programs. A computer virus is a type of software that inserts itself in a computer system and replicates itself throughout host files. Every time a host file is executed, the virus is also executed and infects other areas of a computer. This type of self-replicating virus is called a 'worm' where it "spreads without end-user action" [11]. Since worms do not require end-user action, it is easy and fast for the worm to spread fast and corrupt a computer's infrastructure. Another type of malware attack is file infectors. File infectors are viruses that "attach themselves to executable voded such as .exe files" in order to infect a computer [11]. Once the code is loaded and executed by a user, the virus executes as well. In addition, Trojan is another type of malware that is executed accidentally by a user. In this case,Trojans is a program that contains malicious functions that can be taken advantage by attackers. With Trojans, a user can visit a website that instructs the user to download a program that can help clean the computer system. In this case, the user downloads the program and by installing it on a computer, Trojans have access to ports that an attacker can utilize [10]. However, the most important detail about Trojans compared to viruses, is that Trojans do not self-replicate while a virus does self-replicate. Another well-known malware attack is adware. Adware is another type of software that is usually used to gain information. The purpose of adware is to displace computers with malicious marketing materials and advertising (hence where the name comes from). This is usually one of the most common malware seen by users since the software can be automatically downloaded to a computer by simply browsing different websites. On the other hand, spyware is another type of malware that many users might not be as easy to recognize. Spyware is another type of program that attackers utilize in order to gain access to a user's personal information. Through spyware programs, as the name implies, it helps attackers spy on a user's computer and track everything a user does [11]. Lastly, ransomware is a malware attack that many users are unfamiliar with. Ransomware, as the name suggests, blocks users from accessing certain parts of their computers until a ransom is completely paid. Through this, randsomewar usually pops up to a user, encrypts a user's computer, and threatens to publicize or delete information until the ransom is paid [11].

How Can It Be Countered/Mitigated?

Denial of Service

DoS/DDoS is actually fairly difficult to create an effective defense mechanism against. There's

> (a) large number of unwitting participants, (b) no common characteristics of DDoS streams, (c) use of legitimate traffic models by attackers, (d) no administrative domain cooperation, (e) automated tools, (f) hidden identity of participants, (g) persistent security holes on the Internet, (h) lack of attack information, and (i) absence of standardized evaluation and testing approaches [2].

As it is so difficult for professionals to create an effective stratagem against DoS/DDoS, what can ordinary people do to help? Filtering the traffic at edge routers can prevent IP spoofing, but it's not very easy for the average Joe to filter on such a level. But he can **remove unused services**, to give a potential attack less vulnerabilities to exploit, and he can **install security patches and updates**, keeping up with the fast pace of security. Professionals are creating new security measures every day to address these attacks, but people have to help them out by updating their machines [2] People can also **check for detection themselves**: is the network unusually slow? Is a particular website unavailable? Or are any websites inaccessible? A person, as administrator for their own devices, can "**create an alert** upon the detection of anomalous traffic load," that can then also look into where this traffic load is coming from, or even dismiss "network packets that meet a certain criteria," like being unusually large [1]. Once an attack is suspected, the appropriate professionals must be contacted. The sooner a DoS/DDoS attack is detected, the faster professionals can counter and the vulnerability can be shut down to prevent spread to more servers or systems.

Man in the Middle

MitM attacks can be difficult to detect, too. If done properly, and if a user isn't actively searching for such threats, a MitM attack can be highly successful. An easy line of defense a user can adopt is avoiding "**submitting any sensitive information on any public WiFi** network unless they are protected by a secure Virtual Private Network (VPN)" [4]. The VPN secures a user's traffic so that even if "an attacker happens to get on a network that is shared, he will not be able to decipher the traffic in the VPN" [5]. A user can further assist in the prevention of MitM intrusions by **encrypting wireless access points**, a hardware machine that connects WiFi devices to a wired network and **changing the passwords** not only of the WiFi but on the router as well to be stronger and much more difficult to crack. Furthermore, many MitM attacks target HTTP traffic, or insecure connections between users and web services, so that is another easy way a user can prevent the attack: he can install a browser plugin that forces his computer to **block any HTTP connections and prevent cookie theft**. The use of **Public Key Pair Authentication** may sound difficult, but it can be very useful. A public key alone used for encryption cannot safely prevent a MitM attack, since an attacker could substitute his key for the real key. Authentication certificates and hash functions complement the use of public keys, by adding that deeper level of defense, since those certificates and signed hashes are much more difficult for an attacker to spoof. Some of these techniques sound daunting, but a user need only be careful and wary. Choosing strong passwords for WiFi is something everyone knows, but people can easily extend that toward their routers. Being smart enough not to blindly trust any public WiFi is another good habit and requires little effort, as does making sure to only click on HTTPS encrypted sites. As for VPNs and adding keys, it is not terribly difficult to Google how to set one up on the individual's machine, and will not take long to learn to use.

Phishing

When it comes to phishing, it is one of the easiest cybercrimes to avoid getting caught in. In order to protect one from receiving phishing emails, email accounts already come with a spam filter where spam emails automatically go to the spam folder instead of the inbox folder. In addition, if there is a certain email sender that the spam filter does not automatically detect, one can add specific email addresses so that sender is blocked and does not reach the inbox folder. The way the spam folder works is that the algorithm inspects the origin, content and way it was sent to determine if the email is considered spam or not. However, some spam filters are inaccurate and do black emails from trusted senders, so that is something to keep in mind. In addition, if a user finds an email and/or text message to not be safe to open from the beginning, the user should firstly block the sender and then delete said message. There are still multiple ways to prevent phishing attacks. It is very common for people to open an email and text message from an unknown sender. One of the best ways to know if the link the user has received is safe to open is to have the mouse hover over the website's URL. By first doing this, the URL should begin with an "https" which helps identify the link being protected by a Secure Socket Layer (SSL) . This verifies to the user that the link is secure and the user can safely open it. In case that the user ends up opening a link from an untrusted sender, browsers often alert a user that the website they are trying to access is unsafe and proceed with caution. However, that is not simply guaranteed for all unknown websites. Users can change their browser settings and block illegitimate websites, this way next time that website is trying to be accessed, the browser automatically blocks it. A last resource that is also helpful to personal information from being taken, is for users to change their passwords frequently and not re-use the same password for multiple accounts. By doing this, it is harder for personal accounts to be accessed since each password is different and adds an extra layer of security. Even though phishing is one the most popular ways to commit fraud, it is also one of the most easy cybercrimes to take action against. It is up to the user to be educated and use logic to protect their personal information from being stolen.

Malware

Since there are multiple ways for malware attacks to be present in a user's computer, it is important for users to know what they need to do in order to not get taken advantage of. The first most popular way to protect computers from malware attacks is to download antiviruses softwares. These antiviruses softwares are the most common way for businesses and individuals to install their computer systems. Nowadays, the cybersecurity field is booming and companies keep creating and updating their antivirus softwares in order to keep up with malware attacks. In addition, antivirus softwares is proven to be effective in catching malware used by attackers [12]. Another easy way to be prepared for malware attacks is for a user to think logically and not open any software or website that they think is sketchy. Although this method of thinking logically might seem obvious, is actually really not that obvious since people are curious and tend to click on links they do not realize are malicious. Lastly, another simple method to counteract these malware attacks is to simply run software updates. It is important to run these updates since by having the latest version of a software it makes sure that computers are secured. For example, if a user has a software that has not been updated in 5 years, it is likely that an attacker can find a vulnerability in that software and gain access to personal information. If a user periodically updates their software, then the vulnerability that an attacker found in an older software is most likely not found in the new update of that software. Overall, these simple methods of updating software and installing antiviruses can prevent people from having their personal information stolen.

So What?

Denial of Service

Thinking about DoS/DDoS attacks, it soon becomes evident that there's not a clear motive for initiating such an attack. Alone, a DoS/DDoS attack doesn't give much reward to the attacker. Why, then, is it so important to counter such an attack? While some hackers may simply initiate it simply for the satisfaction of denying service to people, others are much more likely to instead use the attack as a stepping stone for another, greater attack. DoS/DDoS can take servers offline, or shut down a system because the flood of requests is too much for it to bear, and that leaves people in a very vulnerable state [3]. Other attacks can quickly follow, if DoS/DDoS is not countered and addressed as quickly as possible.

Man in the Middle

Since an attacker can see what information a user is trying to access, the attacker can then edit or copy that information. This can lead to all sorts of disastrous events. It can lead to identity fraud, blackmail, and setups for more invasive attacks. A hacker could use DoS/DDoS as a hook to lure a user into a MitM attack, and if a user is not careful, he could be completely vulnerable before he knows it. A user has to be very aware of what's going on at all times, to take ownership and responsibility for his actions, to do his part in a digital age. Cyber crimes are more and more deadly, and professionals need all the help they can get to counter them. Everyday people can help, by simply learning and taking steps to fulfill their end.

Phishing

Since phishing is one of the most popular ways of personal information being stolen online, it is important for everyone to be educated on this matter. In addition, it is simple for people to prevent these attacks because it is one of the easiest cybercrimes to protect identities from being stolen. This means that users do not have to go through the process of paying and installing security software. Through simple education of informing people to not open unknown websites and block sketchy senders, identities and personal information can be easily protected. However, there are people that are not aware of the consequences of successful phishing. If an attacker is trumphiant in his attack, phishing can lead to problems such as breaching data can cause a company to lose credibility and suffer immensely from financial loss. In addition, if an individual is a victim of phishing, this may cause that individual to completely delete and change all of their personal information and even be victims of their social security being compromised. Nowadays, children from a young age have easy access to technology. Through this, phishing takes advantage of ignorance and ends up accidentally having children clicking on illegitimate websites. Although their parents might be well aware of these scams, children are not old enough to think logically about these scenarios and can lead to their parents' identities and financial accounts to be stolen. Therefore, it is essential for society to be aware of the severity of phishing emails and take them seriously. It only takes less than a minute for a user to block someone on their smartphone, so if a user can do that so quickly, it also only takes a minute to explain the ways people can prevent their identities being stolen.

Malware

Malware is also one of the easiest ways for hackers to get access to a computer and then steal important information from the computer. It is important to educate the public about all of these different types of malware since an individual who is not tech-savvy might not be aware that malware attacks are happening frequently. Often, many users do not frequently update their software in being afraid that the update might make their device run slower. While this may be true, it is important to know that the purpose of software updates is to secure a user's personal information. In most cases, in each software update, bugs that are not fixed are bugs that were considered a vulnerability in the previous version of that software. Therefore, it is essential for users, specifically for users who use computers and devices owned by a company, to update their software frequently. Just by getting access to a computer's system, attackers can easily find ways to exploit important information.

Conclusion

The dangers of cyber security are quickly becoming more and more relevant to daily life. But professionals can only do so much themselves. Everyone can do their part, and can actually make a difference. By being aware and educated, people can detect and prevent attacks, and then even deter future ones. Some of it may seem very daunting, but with a few measures implemented per each of the security risks described above, people can deter and even stop attackers. It doesn't take much to be a well informed, proactive member of society, and all the small things add up to create a harder-to-hack community. Risk will never truly be eliminated, as human error is and always will be an unsolved problem, but by remaining vigilant, a society can succeed in protecting information to secure a bright new future for its children.

References

[1] CISA, “Understanding Denial-of-Service Attacks | CISA”, *Us-cert.gov*, 2009. [Online]. Available: https://www.us-cert.gov/ncas/tips/ST04-015. [Accessed: 10- Apr- 2020].

[2] B. Gupta, R. Joshi and M. Misra, “Defending against Distributed Denial of Service Attacks: Issues and Challenges”, *Information Security Journal: A Global Perspective*, vol. 18, no. 5, pp. 224-247, 2009. Available: http://proxy.libraries.smu.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=cph&AN=49232880&site=ehost-live&scope=site. [Accessed 10 April 2020].

[3] J. Melnick, “Top 10 Most Common Types of Cyber Attacks”, *Blog.netwrix.com*, 2018. [Online]. Available: https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/#Denial-of-service%20(DoS)%20and%20distributed%20denial-of-service%20(DDoS)%20attacks. [Accessed: 10- Apr- 2020].

[4] “What is a Man-In-The-Middle Attack?”, *Cloudflare*, 2020. [Online]. Available: https://www.cloudflare.com/learning/security/threats/man-in-the-middle-attack/. [Accessed: 10- Apr- 2020].

[5] “Man-in-the-Middle (MITM) Attacks: Techniques and Prevention”, *Rapid7*, 2020. [Online]. Available: https://www.rapid7.com/fundamentals/man-in-the-middle-attacks/. [Accessed: 10- Apr- 2020].

[6] “Phishing | What Is Phishing?”, *Phishing.org*, 2020. [Online]. Available: https://www.phishing.org/what-is-phishing. [Accessed: 28- Apr- 2020]

[7] "What is Vishing? Voice Phishing Scams Explained & How to Prevent Them", *FraudWatch International*, 2020. [Online]. Available: https://fraudwatchinternational.com/vishing/what-is-vishing/. [Accessed: 30- Apr- 2020].

[8] "What is Vishing? How to Recognize Voice Phishing Phone Calls - Hashed Out by The SSL Store™", *Hashed Out by The SSL Store™*, 2020. [Online]. Available: https://www.thesslstore.com/blog/what-is-vishing-how-to-recognize-voice-phishing-phone-calls/. [Accessed: 30- Apr- 2020].

[9] "What Is Smishing?", Us.norton.com, 2020. [Online]. Available: https://us.norton.com/internetsecurity-emerging-threats-what-is-smishing.html. [Accessed: 30- Apr- 2020].

[10] J. Melnick, "Top 10 Most Common Types of Cyber Attacks", *Blog.netwrix.com*, 2020. [Online]. Available: https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/. [Accessed: 30- Apr- 2020].

[11] J. Sowells, "8 Different Types of Malware | United States Cybersecurity Magazine", *United States Cybersecurity Magazine*, 2020. [Online]. Available: https://www.uscybersecurity.net/malware/. [Accessed: 30- Apr- 2020].

[12] "How Do I Protect Myself Against Malware?", *Surveillance Self-Defense*, 2020. [Online]. Available: https://ssd.eff.org/en/module/how-do-i-protect-myself-against-malware. [Accessed: 30- Apr- 2020].