November 7, 2019

Caden Johnson, Collin Stiller, & tyler Lovato

CNA425

Group 3

Network Security and Vulnerabilities

|  |  |  |  |
| --- | --- | --- | --- |
| Chapter | Author | Page | |
|  |  | |  |
| Title Page | Tyler Lovato | | 1 |
| Table of Contents | Caden / Tyler | | 2 |
| Introduction | Caden Johnson | | 3 |
| Passwords | Caden Johnson | | 3 |
| Multi-Factor Authentication | Caden Johnson | | 3 |
| Virtual Private Networks | Collin Stiller | | 3-5 |
| Motives | Caden Johnson | | 5 |
| Types of Networks | Collin Stiller | | 5-7 |
| Firewalls | Collin Stiller | | 7-8 |
| Basic Prevention | Collin Stiller | | 8-9 |
| Access Privileges | Caden Johnson | | 9-10 |
| OSI Layers | Caden Johnson | | 10-11 |
| Malware | Caden Johnson | | 11-12 |
| Points of Entry | Caden Johnson | | 12-13 |
| Attacks | Tyler Lovato | | 13 |
| Cross-Site Scripting | Tyler Lovato | | 13 |
| Denial of Service | Tyler Lovato | | 14-15 |
| Man-in-the-Middle | Tyler Lovato | | 15 |
| Social Engineering | Tyler Lovato | | 15-16 |
| Conclusion | Caden Johnson | | 17 |
| Bibliography | Caden, Collin, & Tyler | | 18 |

**Introduction:**

When it comes to a society surrounded and immersed in technology, security and safety are the foundation on which we rely. Without a knowledge of possible vulnerabilities and safeguards to protect against such, networks and the devices they connect would become useless and even dangerous. It is our job as up-and-coming Cyber Security students to analyze and predict the acts of hostile forces before they act. This includes designing networks that are available to those they are meant for, finding exploits and loopholes to fix/patch, and many more preventive measures necessary for safe operability through the use of technology.

In the following content, we will describe the basic fundamentals of network security, and how they help prevent unallowed access. We will then progress towards how an antagonist may attempt to access, destroy, or manipulate networks using various attacks. These attacks all have preventive measures, and these will be briefly summarized. Due to the immense complexity and continuous growth of technology, there will always be new vulnerabilities and issues, but there will also always be new preventive measures and techniques used to keep networks and devices safe.

**Passwords:**

The very most simple practice used to keep networks and the devices connected safe is the use of passwords and security keys. Most services and devices now require certain standards for personal passwords such as a minimum of 8 characters, symbols and numbers, etc., but work related passwords are often much more regulated and often cannot contain whole words or anything related to personal life. Most often, these are the object that malicious actors are after when they attempt to access or scam personal devices.

Security keys, however, are very much like passwords but are used by the devices rather than the users. These keys are often much longer (24 digits/characters or more) and are often encrypted and/or hidden deep within the device using them. They are used for access to specific software, networks, and many other services. These keys are by far more important than regular passwords and can lead to drastic and possibly irreversible effects if someone other than the intended device or user obtains them.

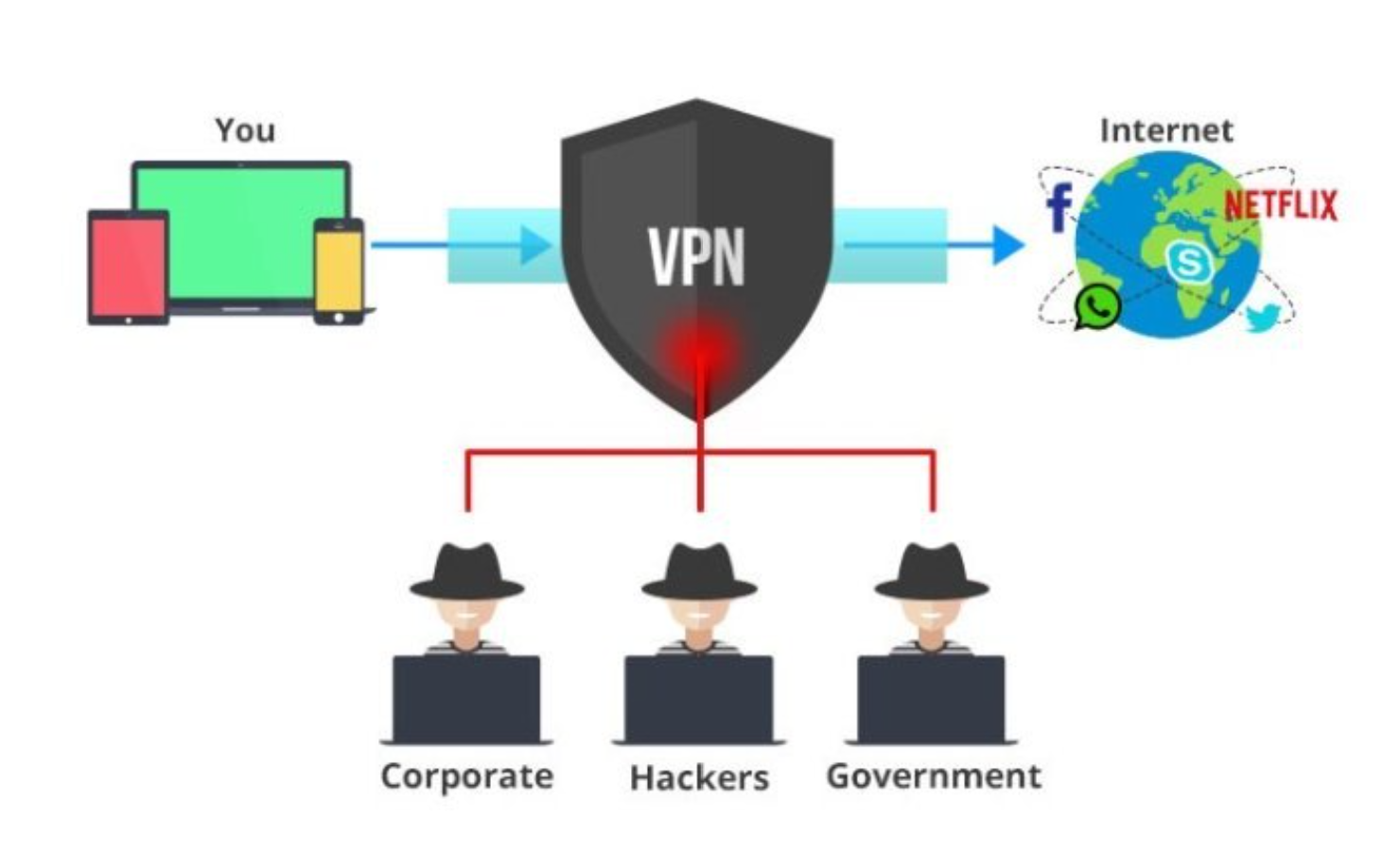
**Multi-Factor Authentication:**

When it comes to basic security, multi-factor authentication is a modern day necessity. There are many levels of security with the easiest requiring the person logging in to insert a code sent to their phone or email. They can also require a person to answer security questions that they have previously set up. The more complicated authentications can require a person to also have a corresponding application that provides codes that reset every 60 seconds that you must also enter. These methods can make it, although not impossible, very difficult for a malicious actor to gain access to a network, service, or device.

**VPNs:**

Virtual Private Networks are used to extend private networks across public networks. This allows users to swap data back and forth as if their devices where connected directly to a private network. This allows users to securely send data between devices without much chance from cyber-attacks or threats. It is a virtual point-to point. It creates this connection through the use of dedicated circuits or with tunneling protocols. Using a VPN can greatly help you from hackers and can be beneficial when trying to practice good network security skills. VPNs don’t make online connections 100% anonymous but are still pretty secure because typically allow only authenticated remote access using tunneling protocols and encryption techniques. This means without direct access it is pretty hard to get on a VPN.

VPNs are used on basically any device that can connect to a network. This means you computer, laptop and even your mobile device can use VPNs. Mobile VPNs are what allows us to roam from multiple WI-FI access points to different cellular providers without dropping our applications or VPN sessions. Mobile security is a recent development because mobile devices have just recently been able to access the internet so easily and send so much sensitive data. People now online shop from their phone. There are a lot of newer technological devices we have to start protecting. It is even common now to put a VPN on your router to protect your smart TV or gaming console. A lot of people don’t realize how a gaming console or a smart TV could be in harm of cyber attacks but they could be. If someone got into an unprotected router they could get access to them and it is really common to have sensitive information on them such as a credit card number. It is smart to set up a VPN to help protect any network you can. Of course if you are dealing with really sensitive data it is smart to encrypt it even before you send it through a VPN tunnel.

****

The diagram above gives a quick idea of what a VPN does. You send data and it stops people from accessing it. It is a fairly simple concept that can greatly help your data from getting stolen or misused.

A handful of VPN services to consider are Hotspot Shield, Norton Secure VPN, Cyber Ghost, and Ultra VPN. These are some of the most used and most reliable VPN services and should work well if you need wish to set one up for your devices.

VPNs and even allow you to access data and content from places you normally might not be able to. Since the server you are connecting to is over the internet then you could potentially access one in a different country. This could allow you to access region locked content. In video games sometimes a game will be locked in certain countries due to rules or regulations blocking it. This would allow you to bypass that. Not saying you should just saying that a VPN has a lot of protection and can allow you to roam the internet freely without fear of attackers or to many restrictions. In a lot of cases people that move countries but their device is region locked to the original country could use it to get access to their new home countries internet. This is also a great way to secure yourself if you are using public WI-FI. Hackers target public WI-FI because it is unsecured so they wait and collect your data when for logon to it. With a VPN you could use the WI-FI with little to no risk of getting attacked. VPNs are also useful for travel. You could be halfway around the world and you could access your own network.

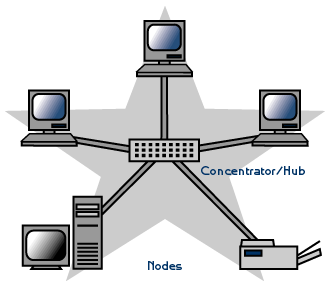
**Motives:**

There are many motivations for people to want to gain unwanted access to a network’s or device’s traffic. These motivations can give you an idea of what to protect, and what aspect or vulnerability they may focus on attacking. First off, sniffing is the act of intercepting someone’s traffic in order to gain access to any details about the device or what the device is doing. This can become dangerous if the device is accessing secure content such as online bank accounts, confidential documents, or anything else not meant for the public. As described above, VPN’s can help prevent against this, but also the additional use of further encryption or using certain proxy servers can help prevent this. Spoofing is often used when sending false information through traffic in order to gain access. With the amount of traffic being sent and received by hosts and clients, creating fake packets and sending them while pretending to be someone else can result in traffic being redirected or sent to the wrong person.

Gaining access to manipulate or change files and privileges is much harder to carry out, but definitely possible. This can be prevented by having strong passwords and by using multi-factor authentication as much as possible. However, most often it is the weakest link that hackers will attack. This means that a well-rounded security set up is most often the best situation. The methods of attacks, and how to specifically prevent against them will be further described later on. All in all, it is always a good idea to understand what someone might want to access and how they might access it. It doesn't necessarily matter if someone is sniffing your traffic if your main security concern are sensitive documents safely stored on your device and never sent over the link/internet.

**Types of Networks:**

LAN or Local Area Network is a group of devices, usually computers, connected together usually to a single server. This could be wirelessly to a server or directly connected. This is done with most commonly through ethernet or WI-FI. The best way to secure a LAN is threw the router. Passwords and keeping the software as up to date as possible. If someone gets into the LAN they could get access to all the devices connected to that LAN so protection is important. This means you should have as strong of a password as you can and keep up on updates. The LAN example you see below is an example of a star. You can see the server in the middle and you computers connecting to it.

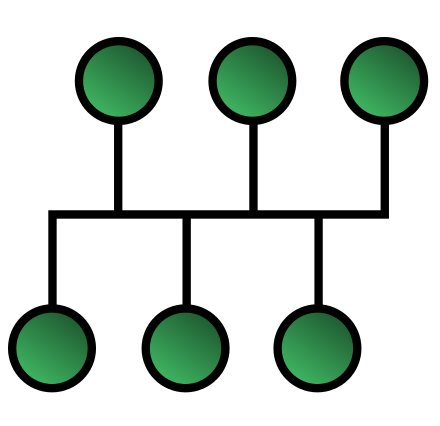


Wan or Wide Area Network is basically a collection of computers and devices connected over a network with a geographic area. This is a large scale LAN. LAN is much more local as for a WAN spans over a large area geographically. The Internet is the largest WAN in the world. To protect a WAN from security attacks it is wise to use things like encryptions, firewalls and VPNs. Your data can travel long distances over a WAN and to prevent attacks it is useful to encrypt your data so no one can open it. It is also smart to have a VPN so no one can collect the data either. These two prevention tactics should stop most attackers.

The main network type topologies are Point-To-Point, Bus, Star, Mesh, Ring and Hybrid. These all have different strengths and weaknesses to consider when being set up. Here we are going to specifically look into their strengths and weaknesses regarding network security.

A point-to-point is good if you need to get information between two devices fast, but in the case if security it isn’t great, if either device gets attacked then they both go down. These quickly shuts down the whole system.

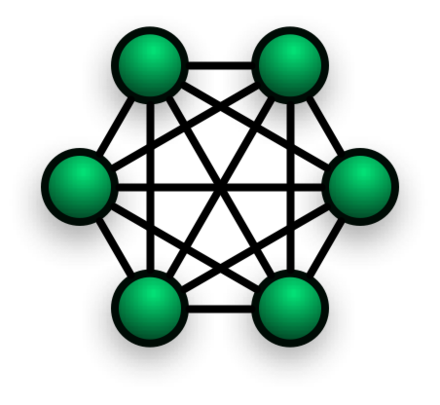
A bus is a collection of computers and devices that connect one by one to a common cable. This is effective in sending information down the line to each device. In the case of an attack depending where it starts you could potentially save some devices. If an attacker went down the line, they may have only made it a little way down. This means a large percent of your data could be saved.



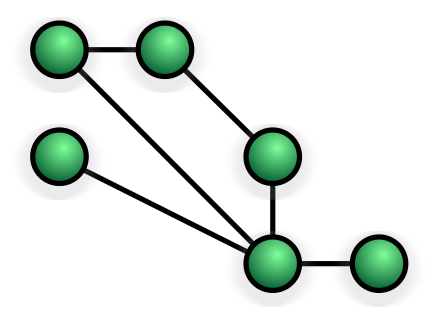
Star is a common network topology because it is easy to set up. All the devices to one place. You just all hook up on one system, usually a server. This is extremely easy to set up and works well. It's not super safe against an attack. The path from the server goes straight to all the devices so if anything gets attacked then it's not too hard to move around and shut the system down. This makes it a vulnerable topology to have. You will want to have good preventions in place with this one.

A ring is easy to set up but can be slow if you are sending data to the device all the way at the other end. This can mean the same for attacks. If it starts on one end and is caught soon enough for could save some of the devices because the ring is one big circle of connections. This topology could help save data in an attack but could also slow down your data transfers overall.

Next is a mesh topology. This method connects every computer or server on the system to one another. Data moves incredibly because it goes straight to its destination. There is a bunch of cables you have to deal with but you will have great data transfer speed. It isn’t the safest system though. With everything being connected if a hacker gets into any system it can move pretty fast into any device it wants. This can be dangerous for any sensitive data you may have on the network.



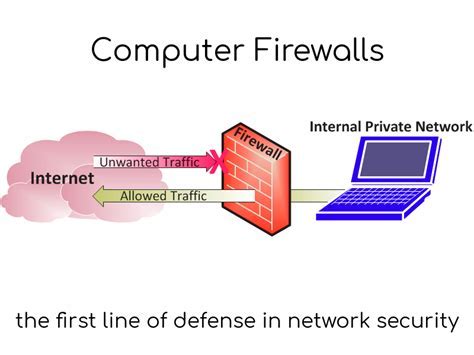
The last topology network we will look at is the hybrid. This is a combination of the previous topologies in a way that it doesn't necessarily resemble anyone topology. This is the best option for security. You can arrange the connections in a way to make it harder for sensitive data to be captured and less important data a little more at risk. With the ability to arrange your network in a way that isolates sensitive data hybrid is the best form of protection.



**Firewalls:**

Firewalls play a huge role in network security. They are a barrier that controls and monitors the ingoing and outgoing traffic between a trusted internal network and an untrusted external network like the internet. They are designed to protect devices and from dangerous data that may contain things like viruses. The most common firewall is the application layer firewall. It works by determining whether a process should accept any given connection. Application firewalls hook into socket calls to filter the connections between the application layer and the lower layers of the OSI model. They apply rules on every piece of data that goes through to determine if it is safe to use or not. One common function of a firewall is to hide the true address of a device to help stop harmful attacks from getting to it.

There are many kinds of firewalls such as Packet, Stateful Inspection, Web Application, Proxy, Undefined Threat Management and Next Generation. The earliest is Packet firewall. This was done by inspecting each packet between computers and the internet. Any packets not allowed would be dropped. A stateful inspection firewall allows or blocks traffic based on state, port, and protocol. It filters based on the administer rules and context by looking at previous connections made on the same port. A web application firewall is a hardware appliance, server plug-in, or some other software filter that applies a set of rules to an HTTP, FTP, and DNS conversation. In return the attackers are identified and blocked. Proxy accepts all traffic that comes in and pretends to be the destination address. It then goes through it and if it deems it acceptable will pass it to the true address. The Undefined Threat Management is really just a loose version of the Stateful inspection. Next Generation is what we mostly use today. Now that applications are so sophisticated simple packet checking doesn’t cut it. It acts as a platform for network security and network traffic inspection. Next generation is a deep inspection done at the application layer that looks for dangerous traffic.

Firewalls are either host-based or network-based. Host-based means they are on the host devices itself and network-based means they are attached to LANs and WANs. Host-based would be a firewall on one individual computer setup to protect that one computer. Network-based are set up to a network and are used to protect the whole network it is assigned to. Firewalls are known as the first line of defense in network security. Firewalls can come in both hardware and software and sometimes they can even be both. This gives you many different ways to access firewalls and that can be helpful when trying to set up a good prevention tactics. Today you don’t always need to go out of your way to install one because a basic version is commonly put on your device when you by it, but it is important to look into which ones are better and getting one of the better ones installed if you are going to commonly have sensitive data on your device. It might be worth the upgrade. Below is a diagram of how a firewall works. As you can see the unwanted traffic from the internet is stopped and the wanted traffic is allowed to pass through the firewall freely.

**Basic Preventions:**

There are plenty of easy basic ways to keep yourself safe from cyber attacks and in a time where technology is so dominant in our lives it is important to know what you can do to keep your stuff safe. We already covered VPNs which are really helpful in keeping your devices protect when accessing the internet. Another form we talked about is passwords and how having something as simple as a password on your devices and networks can protect it. Easy and effective. The stronger the password the better, 1234 won't stop a hacker from getting into your device. We also covered firewalls. These are software or hardware you install that have a set of rules and laws that it applies to all the data that comes thru and determines if the data is harmful in any way or not. They are the first form of defense that your device or network has in protecting its data. These are incredibly helpful to have and are easy to get a hold of so you should try and have some for a firewall set up. It is really common for computers to come preloaded with some kind of firewall installed.

One way of preventing attacks is to simply keep your devices up to date. A lot of attackers go after out of date devices software because the security is often relaxed and easier to get into. It is important to have your device or software pretty regularly updated. That being said, sometimes it is good to give an update a week or two just to see if people are reporting bugs in the system. But overall you should update sooner than later.

Another good idea is to actively manage users’ access. Hand picking which users have access gives you the control over who to trust. Plus, if something goes wrong it is easier to narrow it down. This isn’t always easy to do but in many businesses, it is common for employers to be manually put into the system so that they can be monitored and have as much control as the business wants them to.

It can also be smart to get rid of any old unused accounts. This could be a gateway for past employers or for a hacker to get into your data unnoticed. It is smart to go thru every once in a while and clean them out so that no one can get their hands on them. This isn’t a very common method of getting into systems, it is more common with angry past employees and is usually easily traceable, but it never hurts to be a little extra cautious when it comes to protecting your data.

In a business setting you can control getting you systems hacked by making sure they are only permitted to download software that is chosen. If you keep a list of all the software that is deemed safe and only let those devices us those software then you can greatly minimize the chances of them getting attacked. This isn’t a guaranteed fix but it can help minimize and if you add a couple other prevention methods they should stay pretty safe.

The last prevention method you should practice is to constantly check the network traffic. This is where you will notice the attacks happening. If your fast enough you can stop it or at least recover some data. If your not checking it is possible to not even notice an intruder. This means the more often you check the more you can know for sure if your data is safe or not. It can seem redundant to constantly check but it could save you.

These are the top basic prevention methods to secure your data. Most of these prevention practices that where covered are fairly easy to set up and it doesn’t take too much knowledge of computers and networks to set up. For the most part one of these on their own won't guarantee you won't be attacked but if you combine a handful of these, your data should be pretty secure. The more you preventions you have set up the better your data will be protected from cyber attacks.

**Access Privileges:**

Often in businesses or schools, each node on the network is given specific privileges to allow that device to what it needs and nothing more. This is also seen in cloud computing such as AWS (Amazon Web Services). It is always good practice to never give anyone but the administrator (Admin) full access to everything. This makes it more difficult for a disgruntled employee, student, or random stranger to hop onto a machine and have their way with the devices on a network or a service like AWS.

This can be done by creating specific user profiles and accounts for each person involved, and only allowing them as much as necessary. This will help restrict their access to sensitive materials and/or abilities that could drastically change or damage the network and the devices on it. The major problem with this can occur when an employee or student leaves. Their account, if not removed, can leave an opening for a possible attack. In the best case scenario, even if no attacks occur, these accounts can add up and cause unnecessary complexity and clutter. However, if properly maintained and set up wisely, setting up access privileges go a long way in your efforts to maintain a secure system.

**Each Level of OSI:**

The OSI model, commonly used when dealing with network traffic, is a 7 layer model that incorporates all of the steps from user interface all the way to physical transmission over electrical signals. Theses layers, from the top-down include:

* Layer 7 - Application
* Layer 6 - Presentation
* Layer 5 - Session
* Layer 4 - Transport
* Layer 3 - Network
* Layer 2 - Data-Link
* Layer 1 - Physical

All of these layers use software except for the Physical Layer, Physical, Data-Link, and Network Layers use Hardware, and the Data-Link and Network Layers use both. The Application Layer is the closest layer to the user interface. It is the first layer to receive outgoing traffic and the last layer to receive incoming traffic. It’s services include web browsers, basic email, file transfer, etc.. Vulnerabilities at this layer are often due to loopholes or unseen exploits in software. SQL injection is an example of this, where you can input a partial line of code into a search bar or URL and receive data that should not be accessible. Problems like these can be prevented mainly by the creator of the software and are the main reason that patches and new versions of software come out every now and then.

Next up is the Presentation Layer. This layer not only separates the rest from the application layer, but also plays a huge role in monitoring and changing the format of incoming and outgoing traffic. It is responsible for translation into bits, and also assists in encoding the data. The Session Layer is responsible for providing structure between applications and helps establish, manage, and terminate connections. In the very well-known TCP/IP model, these two layers (Presentation and Session) are not included but are combined into the Application Layer.

The Transport Layer is very important and plays a huge role in the transmission of data. It provides end to end recovery and assists in flow control. Additionally, it checks quality of service, and helps with segmentation and reassembly. The protocols it uses are TCP, UDP, ARP, and RARP. A major vulnerability at this layer includes port scanning, where a hacker tries to find out what ports are open to connections and can then use that to connect to that device. This can mainly be prevented by using a firewall and making sure that your ports are well managed and open only when necessary.

The Network Layer is the layer that separates the upper layers from the lower layers not only used in client and host machines, but also used in switching devices such as ATM switches and routers. This layer, like the Session Layer is also responsible for establishing, managing, and termination connections. It uses protocols that include IP, ICMP, ARP, and RARP. This layer is prone to sniffing, DOS attacks, and ping attacks. The only way to prevent this is to make sure your routers are filtering the traffic and setting up further protocols within the routers.

The Data-Link Layer is responsible for reliably transferring the data over to the physical link. It makes sure that the “frames” are checked for synchronization, error control, and flow control. It is most important and seen in bridges, switches, intelligent hubs, and NICs. Security concerns in this layer are mostly within the physical network layout, and primarily switches and hubs. We will discuss this later in the Points of Entry chapter in respect to ethernet.

Lastly the Physical Layer is the layer associated with actual transmission over a physical medium. It manages mechanical, electrical, functional, and procedural operations, and is seen in every device but also including repeaters, hubs, and multiplexers. It uses the addresses of nodes distinguished by the LAN or the WAN also known as link addresses. These addresses have authority over the entire network, and the size and format depend on what network is using them. The main concern with the Physical Layer is the integrity of the physical connections. If a wire is unplugged or cut, it would cause loss of data and/or connection.

**Malware:**

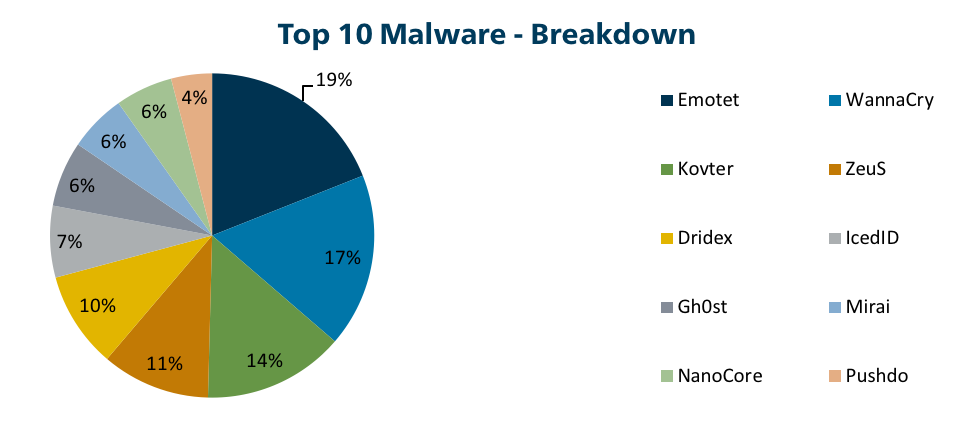
When it comes to malware, all kinds use networks as either a means of transportation or point of attack. There have been various designs and implementations, but they more or less fit into one of the following categories:

-Worms -Virus -Bots/Botnets

-Trojan Horses -Ransomware -Scam

-Spam -Spyware

Worms are mostly known for their ability to replicate quickly and infect anything within reach. They can be designed to do many things including, but not limited to stealing data, modifying/deleting files, and installing trojan horses. The mostly use loopholes in software or are spread using phishing attacks. Viruses, however, need to be activated and are commonly seen in executable files such as a fake ad or unwanted file. They require an already infected machine or network, but once activated can lead to drastic consequences.



As of January 2019

Bots are often used to carry out activities that the malicious actor does not want linked to themselves. However, they can be very powerful when in large quantities, such as botnets, working towards the same goal. With large numbers of devices infected to carry out a determined task, it can become easy to shut down servers by overloading them, mine bitcoin without the user’s consent, or carry out any other actions predetermined by the hacker.

Trojan Horses (also known as rootkits) are very popular due to the access they have and the danger of having one in your device. These are either downloaded directly by the user, or downloaded by a virus, worm, etc.. Trojan Horses are disguised as a regular or necessary file hidden deep in a device’s files. These “files” can then spy on the system, manipulate files, gain access to the network that the device is connected to, and much more. Due to how hard they are to find and how much control they have, they are by far the most important malware to look out for and prepare against. This can be prevented by making sure all downloads are closely monitored and all incoming traffic is only for safe and approved sources.

Ransomware is spread in the same way as Trojan Horses but serves a very different purpose. These files, when activated, will prevent your access to your files, network, or even basic computing tasks. The motivation behind this is the hope that the user will pay the hacker to regain control of their device/network. If not paid, which they usually aren't, it can cost the school, business, or user a lot of money due to the cost of a new device or setup. These can be prevented by always patching software that isn’t up to date, as there may be a vulnerability. Also, backing up your files and data offline, such as on a separate hard drive, large-quantity USB drive, or on the cloud can prevent the loss of important materials.

Scams most often correlate with Adware, and will most often slow your computer, or in the most common case just annoy the user. Worst case scenario, the ads will not only clutter your machine, but often contain dangerous download links that may contain any of the previously listed malware. There isn’t a lot you can do to prevent these, other than an ad-blocking software, but it is always safest to never click on anything suspicious. Spyware is a lot like a Trojan Horse and are known to monitor a user’s activity or traffic. Most often they are trying to collect sensitive information such as passwords, bank information, etc.. Lastly, Phishing and spam are often more for personal information rather than device/network access. They are used in emails, calls, and texts disguised as someone who you might know. The purpose of these messages is to hopefully trick the user into releasing confidential information such as personal information, passwords, etc..

In response to all of these kinds of malware, It is always best to maintain good judgment when sent or downloading content. In respect to actual network changes to increase security and prevent accidental infection from malware, you should make sure to only connect to secure networks and use a firewall for either your network or device.

**Points of Entry:**

Networks can be connected by many means, and these connection methods can provide a vulnerability open to exploitation by an outside source. If connections are not secure, they can be the weakest link in your security plan. These connections include, but are not limited to ethernet (wire), wifi (wireless), and phone (dial-up). The methods of securing your connections can be very complicated, and often incorporate network structure and layout, router protocols, and VPNs.

Through ethernet or wire connection, it is possible for an outside source to attempt to attack your devices or entire network from anywhere in the world. However, it is extremely dangerous if the malicious actor has access to any of the devices or ethernet ports within the physical layout of your network. If any of your switches have a mirror port, which sends out all of the traffic that travels through the switch, this can be very vulnerable to sniffing. The same applies to any hubs. The main precaution in this circumstance would be a well thought out physical network layout in order to protect and monitor your devices.

Wifi is very similar to ethernet, since the wireless signals are intercepted by a WAP (wireless access point) and are then transported over ethernet like all of the other traffic. Wifi also adds the vulnerability of having the wireless signals intercepted before they even reach the WAP. Someone within range of the wireless devices could possibly intercept traffic, spoof traffic, or carry out many other attacks. Although there are a lot of exploits on the different types of wireless protocols, it is always safest to use the newest, patched Wireless protocols and make sure your wifi is protected with a strong password.

Dial-up connection isn’t as common in today’s technology, but was very popular in the early years of the internet. This method combine your phone traffic and internet traffic on the same connection. In recent years, it has been replaced with broadband. A common problem with dial up internet was the number of attacks where hackers would repeatedly try to connect to phones until they got a connection. They could then install wiretaps, guess the passwords for the user and various other things. Another huge exploit was using certain sounds through a phone call to manipulate the device on the other side of the connection. This sound could convince the other side that the call was over, but would leave the connection open so the hacker could gain access to the device or the network it was connected to. These problems have now been solved due to broadband, but are still dangerous if you use dial-up.

**Attacks:**

There are a variety of network attack types, such as denial of service, man in the middle attacks, phishing, and remote code execution attacks.

One of the most well-known types of vulnerabilities is the denial of service attack. A denial of service attack (DoS) aims to bring down a service so it is not accessible for legitimate users. Denial of service attacks are often a Distributed Denial of service attacks (DDoS), where the attack is distributed across multiple malicious machines. Often, these malicious machines are a part of a botnet. A botnet is a device that has malware installed and can be controlled to some extent by a malicious hacker. Other Types of attacks we will discuss are Man in the Middle attacks and phishing.

According to the White House in 2018, Cyber Attacks cost the economy between $57 billion and $107 Billion in 2016.

**Cross-Site Scripting**

Cross-Site Scripting, or XSS, is a vulnerability where an attacker is able to inject scripts (Typicall Javascript) into webpages. Cross-site Scripting is one of the most common attacks in the internet, with Symantec claiming about 84% of Security vulnerabilities in 2007. While Security has improved in the last decade or so, cross-site scripting is still a threat today/

Cross-Site Scripting may be persistent or non-persistent. A non-persistent XSS attack attacks at the time a victim browses a webpage. A persistent XSS attack utilizes cookies or other files to stay on the victim’s computer longer.

Cross-Site Scripts can be used to steal cookies, which are often used as a login credential. They can also be used to Hijack a session and redirect the victim to another site. They can also be used as a botnet, or often as a way to show advertisements, generating income for the attacker. Advertisements are often an avenue for an attacker, for both cross site scripting and other attacks.

**Denial of Service Attacks.**

A common Denial of service attack is known the SYN flood. A SYN flood exploits TCPs 3-way handshake, where an attacker attempts to open many possible sessions by sending SYN packets. and then never responding to the servers SYN-ACK requests. A SYN packet is a special type of TCP packet used to establish a TCP connection. A SYN packet is sent from, which is then Replied to with a SYN-ACK packet. That Packet is then acknowledged by the original sender with an AWK packet, and the connection has been established. By not replying to the SYN Packets, the victim server has to keep many connections open at once waiting for SYN-AWK packets that never come, until the connection times out. This causes the target device to hold onto many active connections at once, overloading the system.

There are a variety of ways this attack can be minimized or avoided. One is to reduce the time that a SYN-Received timer stays open. Another is to filter the Incoming SYN packets, often through firewalls. However, this becomes more difficult if the attacker spoofs its IP address. You could also recycle the half open TCP Connections instead of opening new ones.

A simple variation of this attack is the ping flood, which is simply overloading the victim’s bandwidth with ICMP “ping” packets. While easier, this attack only really works if the attacker has equal or more bandwidth than is available to the victim. A savvier attacker can instead use what is affectionately called the ping of death. The ping of death is a malformed ping packet. Normal ping packets are only 56 or 64 bytes. However, the normal maximum size of an IPv4 packet is 65,535 bytes. Because many systems were never designed to handle such a large ping packet, a buffer overflow can occur, which can bring down a system. An extra savvy attacker can use some of those 65,535 bytes to inject malicious code into the victim machine.

Another variation of the ping attack is the Smurf attack. Like the ping attack, it works by overloading the network with Ping Packets. However, instead of simply having that attacker send a bunch of ping requests, the packets are modified so the source IP address is the broadcast address. Many devices on the network by default will reply to this ping request, overloading it with its replies. This attack is very effective on networks with many host devices that will reply to a ping from a broadcast address. To avoid this type of attack, each end device needs to check to see if the host IP address is valid before sending a reply. Another option is to ensure that routers are not sending ping packets that have a broadcast IP address.

A related attack is the Fraggle

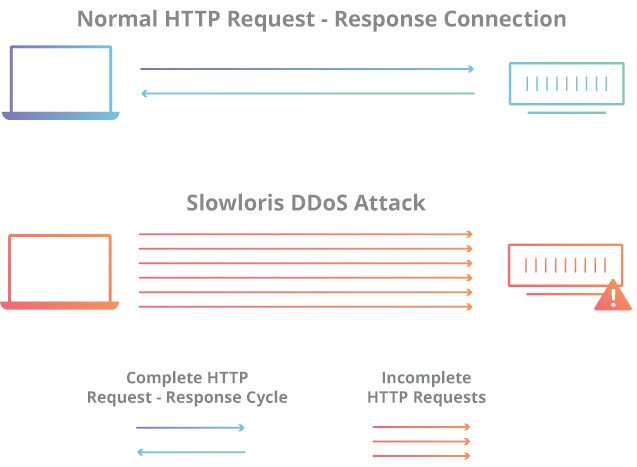
Attack. Instead of using ICMP like the

Diagram of the SlowLoris Attack

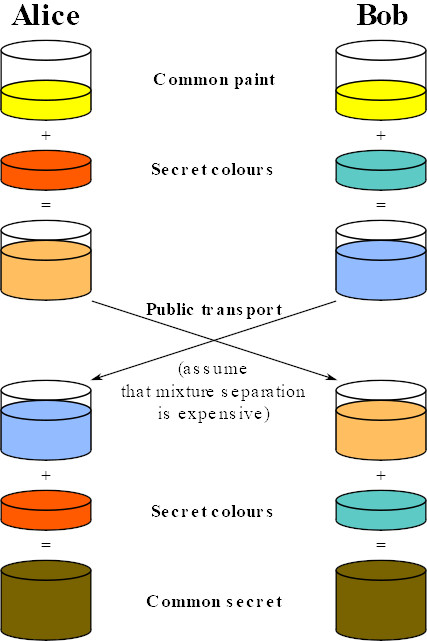
Smurf attack, Fraggle uses UDP, and sends packets to the broadcast address with the source IP address spoofed to the victims IP address. As a result, many to

all devices will begin to reply, sending their replies to the victim.

The above attacks often require a lot of bandwidth on the attacker’s end. Often, that means that the attack must be

a DDoS attack. A lonely attacker with limited bandwidth would be smart to choose a low bandwidth attack like the slow Loris attack. The Slow Loris attack mainly attacks HTTP web servers like Apache. It works by opening connections and then periodically sending the victim incomplete http headers, but never completing the request. Thus, the victim server will keep the connection open. Unlike the above SYN Flood attack, the slow loris keeps and maintains a complete TCP connection, but it will still overload the system by having too many active connections open. This attack can be mitigated by limiting the maximum number of open connections per IP address, or by setting a minimum transfer speed. However, there is no way to completely prevent the attack.

**Man-in-the Middle and Encryption**

 The above attacks all aim to bring down a service and make it inaccessible to legitimate users. A more common, and possibly a more damaging form of attack is the Man-in-the-middle attack, or MitM. A man in the middle attack is where an attacker eardrops and potentially alters communications between two parties. A common and easy man-in-the-middle attack is an attacker listening in on unencrypted Wifi traffic.

Encryption is the most common and best defense against MitM attacks. The Diffie-Hellman key exchange is often used for two parties to exchange keys without ever sending that key over the network. Diffie-Hellman used modular Arithmetic on large primes for its key. It works by having two parties each create a key with public and private values. Each party sends their public values to the other, then combine them with their private vales. Thus each end up with the same key without ever having to send that key over the network.

Another option is to use RSA Encryption. In RSA, each party creates a public and private key, and shares their public key with everyone. Data sent over the network is then encrypted with that devices public key, where it can only be decrypted with the private key. RSA is often used in tandem with a Certificate Authority (CA). A Certificate Authority is a trusted third party that verifies that a public key is legitimately owned. Certificate Authorities are mainly used on the

The Diffie-Hellman Key Exchange

World Wide Web, and are the foundation of HTTPS. Public Key encryption is also the bases of protocols such as SSH.

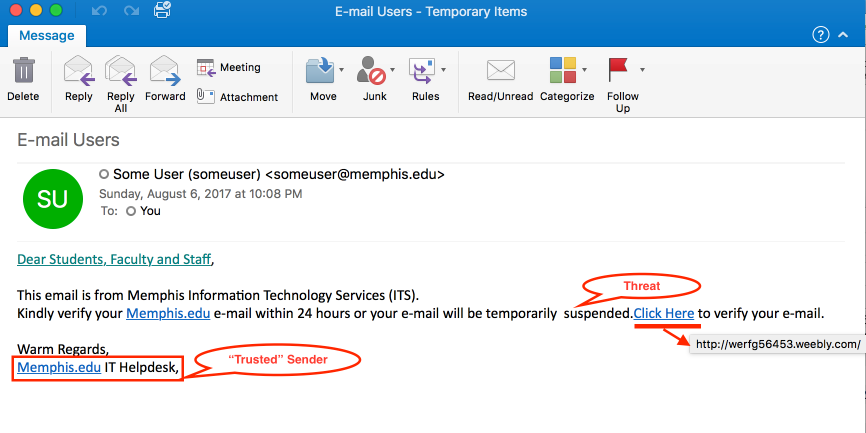
**Social Engineering**

A less technical but still dangerous form of attack is Phishing. Phishing is a form of social engineering where an attacker pretends to be a legitimate organizations or persons in order to get information from users. A common example is sending emails to users that look legitimate in hopes of extracting information. Often, these attacks happen by sending massive amounts of emails in hopes of getting one or more users to take the bait. By contrast, spear Phishing is the targeting of specific users in order to extract specific information. The term wailing may be used when the spear phishing attack is aimed at a high-profile target.

The primary aim of phishing attacks is to extract valuable information from its victims. Often times that information is login credentials for services, or personal information such as credit card numbers, social security numbers, or bank routing numbers. Phishing attacks have also been used in corporate and government espionage.

Phishing attacks often use link manipulation. For Example, if a phishing attack was pretending to be *fooBarBand.com* the attackers may send a link like *FoobarBand.legitsite.com* . Other Times, an attacker may instead try and redirect a user from a legitimate site to one that the attacker owns.

Technical Defenses against phishing attacks are firewall and email filtering, using Trusted Certificates, and being smart with your information. Using 2-factor authentication can limit exposure if login credentials are leaked. Using key based login, such as RFID or a yubi key can also prevent phishing attacks since a login credential is only useable once, for a very limited time. SMS based two factor authentications can help, but is susceptible to sim card jacking, where an attacker pretends to be a phone company customer and gets a sim card with the victim’s phone number on it. Sim Jacking is another example of a social engineering attack.

The best defense against Phishing attacks is by educating users on how to recognize phishing attempts, and to be careful with the information they give out. While phishing can be reduced with technical solutions, the most effective solutions useless if ignorant or indifferent users ignore them.

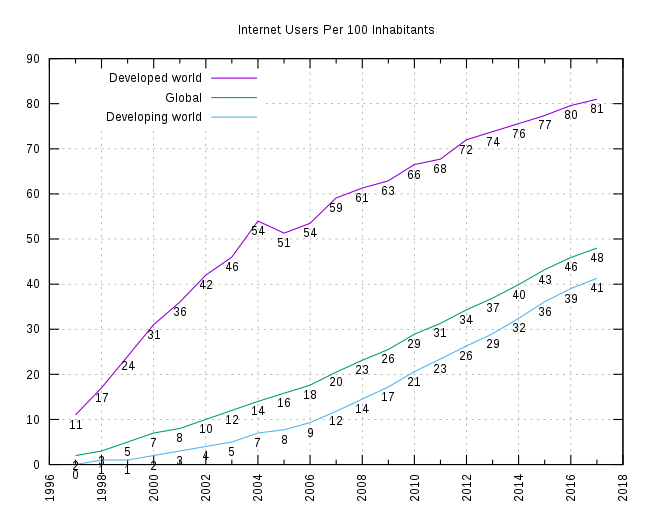
An actual Example of a phishing attack

**Conclusion:**

Network security is a very broad topic, and with the amount of technology and brilliant minds in the world, the complexity of each aspect can be overbearing. The main components to keep in mind are points of entry, basic preventions, physical network layout, and keeping your software/hardware up to date. Depending on the severity and importance of your network, it may require extra precautions such as firewalls, VPNs, and specific access privileges.

Despite the extreme specifics of it all, it is always best to never access or download content from an unknown source, and never give out information about passwords, network details, or even personal information. Malicious actors will always search for the weakest link in your system, and that can even involve the people using it. Separation of network, devices, and materials related from your personal life can help protect the integrity and confidentiality of important content. And lastly, it is always wise to ask a professional or consult with someone more experienced when in doubt.

On a final note, and like stated before, technology use in the 21st century has grown immensely, and will continue to grow. With the vast connections of networks across the world, security has become a valued necessity. This safety is crucial to the amazing experience that everyday users invest their time and money. With the help of cyber security professionals across the globe, the Internet, everything connected, and anything in between will continue to be the keystone of business, education, and social interaction everywhere.



**Work Cited**

**“What Is a VPN? How Does It Work?” *Latest Hacking News*, 29 Jan. 2018, latesthackingnews.com/2017/05/10/what-is-a-vpn-how-does-it-work/.**

**Hoffman, Chris. “What Is a VPN, and Why Would I Need One?” *How*, How-To Geek, 18 June 2019,** [**www.howtogeek.com/133680/htg-explains-what-is-a-vpn/**](http://www.howtogeek.com/133680/htg-explains-what-is-a-vpn/)**.**

**Berry, Megan. “Network Security: Top 5 Fundamentals.” *IT Manager Daily*, 16 Apr. 2012,** [**www.itmanagerdaily.com/network-security-fundamentals/**](http://www.itmanagerdaily.com/network-security-fundamentals/)**.**

**Rouse, Margaret, and Diana Hwang. “What Is a LAN? - Definition from WhatIs.com.” *SearchNetworking*, searchnetworking.techtarget.com/definition/local-area-network-LAN.**

**“Chapter 5: Topology.” *Florida Center for Instructional Technology*, fcit.usf.edu/network/chap5/chap5.htm.**

**Talari. “Tips For Securing Your WAN.” *Talari Networks*, 16 Apr. 2019,** [**www.talari.com/blog/tips-for-securing-your-wan/**](http://www.talari.com/blog/tips-for-securing-your-wan/)**.**

**“What Is a Firewall?” *Cisco*, Cisco, 25 Oct. 2019,** [**www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html**](http://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html)**.**

**Geekboots. “What Is Firewall in Computer?” *Geekboots*, 21 Feb. 2019, www.geekboots.com/story/what-is-firewall-in-computer.**

**Shaw, Keith. “The OSI Model Explained: How to Understand (and Remember) the 7 Layer Network Model.” *Network World*, Network World, 22 Oct. 2018,** [**https://www.networkworld.com/article/3239677/the-osi-model-explained-how-to-understand-and-remember-the-7-layer-network-model.html**](https://www.networkworld.com/article/3239677/the-osi-model-explained-how-to-understand-and-remember-the-7-layer-network-model.html)

**Comtact. “What Are the Different Types of Malware?” *What Are the Different Types of Malware?*,** [**https://www.comtact.co.uk/blog/what-are-the-different-types-of-malware**](https://www.comtact.co.uk/blog/what-are-the-different-types-of-malware)

**“Phreaking.” *Wikipedia*, Wikimedia Foundation, 31 Oct. 2019,** [**https://en.wikipedia.org/wiki/Phreaking**](https://en.wikipedia.org/wiki/Phreaking)

**The Cost of Maliucious Cyber Activity to the U.S. Economy 04 Nov, 19**

<https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf>

“Global Internet Usage.” *Wikiwand*, www.wikiwand.com/en/Global\_Internet\_usage.