Jamil Gafur

Fall 2016

Computer Security

In this age of technology are we still secure? Many companies ask themselves this question; are their computers, software, and computer systems safe from external and internal threats. How vulnerable is the system they are using? The answer is simple… No. Since the internet or other untrusted network are used to transport information, it is common to expect attacks from the lower level infrastructure; These attacks can come in many forms, and are not only aimed at the company's network, but also the resources and information that the network provides. Some ways that people get in are by target the companies staff, try to guess the company’s passwords, or attacking the Operating system and its bugs.

Computer security has been a growing industry for the past few years. This is due to a circular growth argument that allows a non-limiting growth for a company’s growth and its security. In essence, a company use different technological devices to become more efficient. As the company’s efficiency increases it saves money, and becomes more successful. When a company becomes successful it is subjected to attacks on their network for sensitive information. Therefore, the company increases its security, and expands because of its success. When the company expands it takes up resources, and to manage their resources, they obtain more technological devices. Now we are in a circular growth where companies are becoming more successful and more devices are being used. It is only a matter of time before people realized that others would want to steal information from them. To prove this if we look at the statistics from the “Computer Security Institute” in which they interviewed five hundred and thirty-eight companies.

* 64% reported a financial loss due to computer breaches
* 84% admitted to detecting a security breach within the last year
* And 70% stated that a majority of their attacks came from internet connections

However, this is based off of computer vulnerabilities, another problem is the actual computer, a computer insurance company stated that in 2000 over five hundred sixty-seven million dollars’ worth of equipment were stolen. From there it would be very simple to remove the data by swapping out the hard drive or by other means.

How do people with malicious intent cause damage to our computers? From Social engineering to viruses, DoS and IP Spoofing, to even the theft of an actual device are just a few ways for a company’s security to be compromised. A security breach that changes data can have a significant impact on a company. For example, a fraudulent transaction that can result in the monetary holdings of a company to be altered, or stolen files off a personal computer can be used as blackmail. These are a few things that someone can do once they get on to a network. One way they get in is as simple as lying and taking advantage of a person, this is called Social Engineering. In this digital age many people put their personal information online, and without knowing it they put themselves in danger, or a person is exploited by their need to want to feel helpful. An example of each is as follows:

* Someone goes on your Facebook profile and learns about your friends, pets and family. Then they call your bank and pretend to be you by giving the information they learned about you. Thus gaining access to your financial information and more personal information.
* An aggressor calls your phone and pretends to work for your company’s IT department, they inform you that they need to access your computer to solve a problem. Then they prompt you to download a malicious software so that they can access all your company secrets from your account.

Another way attackers can try to hinder/exploit a company’s devices is by uploading a Virus/Trojan Horse onto their system. This is when malicious code goes into the OS and re writes code, the most common way of doing this is by having the code placed into legitimate software and activated when it is downloaded and runs. It is highly difficult for security software to detect this because most times the code is hidden in the binary; Binary is the computer language that breaks down our program so the computer will understand it. It is done by taking the programmer's code and transferring it into a sequence of 0’s and 1’s that is interpreted by the computer's OS. This is a good way of destroying a computer system from the inside. This however might not be what the aggressor wants.

By contrast maybe a competitor wants your customers to have a bad experience with your company. How do they go about doing it? They won’t take down your whole system, because then it would be too obvious. One thing they can do is a DOS (Denial Of Service) attack; This is an attack that targets the resources in a network, while the virus targets the network itself. In doing so legitimate users can’t access the resources because they are being used by the DOS attack. One form of a DOS attack is called SYN; when a computer connects to a server beforehand it sends information to the server so it can reserve space for the computer. A SYN attack is when a computer pretends to be a large number of computers (by changing its IP) and then having all the computers request access to the server. In turn the server will hold space waiting for the computers to connect but that actually will never happen. Because of this many people who actually need to access the server can’t because they the SYN attack is using the server’s resources for nothing.

Earlier we mentioned that in DOS attacks the computer changes IP addresses. What is an Ip address? The most basic explanation is that an Ip address is a way for a network to recognize the devices connected to it. To show how this works imagine you are connected to a Wi-Fi network at your company; you have been assigned a specific IP that is special for everyone in the company who is connected to the Wi-Fi. To access information, you connect to the server and send it your special IP address and are given access. If your Ip does not have the special “code” you cannot access the server. For attackers to get around security precaution they need to send an IP that is recognizable to the server, commonly known as IP Spoofing.

These are all different ways of attacking a company’s devices and using it to hinder the company’s success. In order to protect against these different types of attacks there are different security policies and standard to allow for easy transition of data between places and increase the difficulty of obtaining access to data you aren’t allowed to have. The first step was to create an infrastructure that obeys the same protocols and standards inside a company; this can be as simple as having a class once a year that all employees must attend to inform them not to give out their information to anyone. After making sure everyone is following the same security ethics we move on to the actual devices. It is good to imagine this part as sending a package though UPS; suppose you send someone a package containing something valuable. First you make sure you are sending the correct thing, the address is correct and you are sending it using a reliable source of transportation (UPS). Then it goes out and you call the person you sent it to so you can make sure that it reached the correct person and also that no one stole the valuables that you sent.