Security organizational software

As new and more sophisticated technology involving computers and software develop every year, human lives become more entangled and attached with it. This means that the frequency and percentage of humans using these systems are rapidly increasing.

This equates to more information being processed, transferred, and viewed over vast computer systems across international networks. This pertains largely to everyday browsing of the internet, which may include commonly used information such as reading today’s weather, the news, or the personalized horoscope of the day; to the more sensitive information which can be confidential and requires to be protected, such as checking email messages or accessing your bank accounts, which may include sensitive processes such as transferring of funds. Development of new technologies like wireless connections and networks such as the bluetooth and wifi technology may have brought convenience to most computer users, but these also introduces new flaws that computer security experts are not yet even familiar of. These technologies create new vulnerabilities that attackers may exploit, and thus steps on how to improve security are continuously researched on.

Security becomes more and more complex and costly each year as new additions create more aspects to be exploited. The number of people connected through the internet makes every computer connected to it a potential target of malicious attacks that aim not simply to disrupt processes, but also to steal money and most importantly, information, which can be disturbing as most of the information available in our computers are supposed to be private. The top three security concerns in the internet are

viruses, which includes worms and trojans, spyware and malware, and spam. These problems had cost the most amount of both loses and investments. This paper details the vulnerabilities that computer network architecture has, and what attacks are currently existing and are commonly used today, and how these attacks are executed.

This paper also discusses the role that we humans play in computer security as the users of these systems. Humans are also said to be the weakest aspect of computer security as we are the ones using the computers, and we are the one in control. Tricking someone to do something potentially harmful to a machine had been a popular way into spreading malicious computer code. This paper details those tricks employed by determined hackers and attackers. In addition, online trends such as social networking sites and blogs which are becoming popular nowadays also introduce a new arena in which virus writers can attempt to steal information and spread malicious code through widgets and software loaded through these popular websites.

In the paper entitled “ The Coolest Hacks of 2007”, Kelly Jackson Higgins had discussed some of the exploits made by hackers that are deemed to be the best, as these attacks, after having been proven possible, makes a lot of people to rethink their security. There had been cases that wireless hacking had been used to change the message to traffic signs in Sydney, Australia, a process which was even documented on a You Tube video. Another wireless attack documented there was not done through a computer, but rather with a conventional toaster. Also notable is the developed bluetooth sniffing through a USB stick. This hack makes bluetooth hacking easier and quite

affordable, as it used to cost around $10, 000 just to acquire equiments needed to make the sniffing work.

Now it can be done with a cheap USB stick costing only around $30 dollars. Also found to be vulnerable are the wireless headsets that are really common nowadays. Through radio scanners, hackers are able to listen to conversations over these headsets and even succeeded in recording them digitally. Computer security has grown into a complex science that takes time to be digested and understood. It is constantly changing due to the developments of new technologies, which means that no one can really master everything and knows everything, although grasping the basic ideas may give a user a good grasp on how things work. Cybersecurity There are a lot of software security suites available in the market which are basically anti-virus programs designed to find and obliterate files that pose a threat to a system.

Some of these softwares can be downloaded for free and some can be bought then upgraded with a subscription plan, allowing the user to update the security software with the latest virus definitions from their database. This makes the computer immune to all the known virus patterns in its database, as the program will automatically prompt the user on what to do when it detects a suspicious file, action, or process existing in your computer. Usually, the virus definition of anti-virus software should be updated every few days because new threats arise fast in the span of mere days, rendering your computer unprotected to these new variants of harmful code. Aside from anti-virus software, another vital software for the security of a machine is installing good firewall software on it. The firewall, as the

name suggests, acts like a barrier around your machine. This means that even if you’re connected to the internet, people using remote computers cannot easily access your computer because they have to pass through the firewall, and this can be modified as to what connections to allow and not.

Although not all firewall are guaranteed to stop and filter all kinds of attacks, in the same way that anti-virus sofwares cannot detect a hundred percent of all existing viruses, it is always better to have one running especially when the machine is connected to the internet 24 hours a day. Anti-virus sofware often has options on what way the information flow should be allowed, which means user may restrict connections from the outside to access a machine. Not all hacking or trying to break into a computer or computer network is done in a malicious intent to steal something or infect it with a virus. Hackers also do hack into systems to expose its vulnerable spots and find ways that real attackers may use to break in. This way, the system may be prepared or adjusted to theoretical attacks to be done in the future. Companies invest in securing their information because this information is crucial to the company’s integrity and may result to bigger lose when not attended to.

A single security breach, according to coresecurity. com, a website about computer security, may cost a company around $350, 000 worth of lose. Penetration testing is a process in which a system is tested if it can be entered from the outside. This should be performed regularly to ensure the tightness of the security of the system, especially when the network has grown complex already, or when something was changed in the network, like adding new nodes or applications, or moving to another location physically, or when new security software was installed.

This is important if the organization is to avoid the loses whenever a network goes down when a break-in has been successful. Cybercrime Cybercrime pertains to a wide range of acts that are commited through electronic devices that are considered to be crime. The definition of cybercrime is rather vague and ambiguous because not all countries have passed laws concerning these acts, and what would be a crime to one country can pass as something without any penalty from the law in another. Some countries, especially poor and developing countries, lack the facilities and equipments in investigating these crimes, such that they can be commited and the citizens concerned are not given protection their laws. As was said, cybercrime can pertain to a lot of acts, and can rather be vague.

Stealing can now be done electronically since bank networks are now employing transactions done through their networks or the internet. When one gains remote access to a bank’s resources and servers, bank accounts may be compromised since funds can be transferred with just clicks of a button. Although most banks employ a tight security with their systems, these systems are still prone to have unnoticed security holes that can be exploited by a clever attacker. Before, unauthorized use of credit cards are made possible when credit card numbers have been cracked by software writers across the internet.

As an added security feature, an additional pin number was required now when using credit cards which are rather difficult to crack. Cybercrime is not only limtied to stealing money or bank funds. It can also be done through stealing a person’s identity or personal information to be used in an

authorized way. For example, a third person may listen to communications between two parties if their connection is not secure.

A non-secured connection means that the information being sent from a user to another is not encrypted, and someone who tapped into the wire or the path between the two users can easily read the information contained in the packets of data while it is in transit. Information stolen through snooping, the method of listening in between users, can range from personal passwords, or other sensitive data, such as bank accounts, pin numbers and credit card numbers. Another thing to take note is the evolution of botnet armies. Botnets are usually a network of compromised computers that are infected with a certain trojan called a “ Zombie” which was actually a software that connects to an IRC server, allowing its creator to issue it commands from the IRC channel, and thus give access to the compromised PC.

These infected machines, often referred to as Zombies, are often used to launch DDoS attacks, or Distributed Denial of Service Attacks, to certain websites, flooding them with worthless packets of data. When a website’s bandwidth is small compared to that of the flood of packets coming in, the website usually goes out of the internet because it can’t serve the legitimate requests because of the flood of garbage packets. Web Security As the Web 2. 0 is slowly coming into fruition, a lot of security threats through the web are also generated. Online dating websites, social networking websites, and blogs can be a potential venue for virus writers to deploy their code as these websites have valuable information that can be exploited to get profit from. With this malicious software, the privacy of our online activities is now in peril.

These software may be used to collect personal information, and in a way it can be said that the there is no longer privacy when browsing the internet to this attack, since collection of these data can be done secretly. Usually, these data gathering is used to provide the user with relevant advertisements that may be related to the person’s interests. Because of the number users connected in the internet, it is common to target humans the weak point of the computer system, as the users themselves are sometimes easier to trick than the security system. Tricking a user to install or run certain software or visit an intrusive website may gain the attacker access to the computer which would have been secure without the user’s participation. This has been the case of the popular “ I love you” virus, as a lot of people were made to open and run the attached software in thinking that it was a real message for them.

Such is also the case when spam messages through email announces that the user has won a big amount of cash, or other messages that may bring a user to instinctively open and run the accompanying software, which may turn out to be a trojan or virus. Another attack to trick the users of the computer is called phishing. This is a way of getting a user to enter sensitive information and send it to the attacker instead of the legitimate destination. Basically, the attack comprise of a fake website disguised as a real one. For example, a webpage is designed to look like that of the Yahoo homepage where the login page is. When the user is unwary and opens it, he or she may think that it is indeed the real Yahoo page and thus enters the username and password.

This is done not only with passwords and email accounts but also with credit card information, bank accounts, and others. Malware and Spyware Aside from the threat of viruses that increase everyday, malware and spyware are a new annoyance to users. Unlike viruses which can easily be detected my anti-virus programs because of their potentially harmful patterns, these software are disguised as credible programs that does your computer no harm. In truth, this software is monitoring the activities you do in your machine such as your browsing statistics and what softwares are you using most of the time. This software is found to be more difficult to detect and remove than viruses, and there are those variants that cannot be removed without damaging the operating system installation, which in short means that a reformat is necessary to solve the problem.

There had been a wide range of tools available for curing malware and spyware that are not detected by ordinary anti-virus programs. Oftentimes, these solutions are highly specific to a specialized infection, and the tools do not promise to be an ultimate tool that is able to protect the machine from all spyware infections. Most anti-spyware programs cannot detect all of these spywares, so users often employ two or more software to protect their computer. Most malware are simply spam advertisements that force a user into clicking a certain website. This can prove to be more annoying and destructive that usual viruses because even if the malware does not cause direct harm to your computer, it takes up precious system resources and is difficult to remove because of the difficulty in differentiating them from the legitimate software installed. Trojans are programs disguised as legitimate software like games, or other utilities, that we users normally use.

They are called trojans because despite their outside appearance and function, it hides a certain code that does something to your system. This varies from different strains of Trojan viruses, but commonly they can allow a remote computer to have access to a machine, or download or install another virus that can do the damage. Usually trojans are really small files and can be transferred easily over a network. Although anti-virus software can detect most existing trojans, new threats arise and these can cause damage to computer systems undetected.

Security Software ToolsThere are lots of tools out there that promise to offer security to your machine. This software can be free or with a subscription. But because there had been so many claiming to be the most effective, it is important to note the reviews of users who have had experience using the software. Some software online that claims to be security tools are in fact the malware themselves, so installing just any software, and sometimes asked to pay an amount for it, makes the situation much worse.

This paper attempts to detail some of the most common tools that effectively protect your computer. The most popular download on cnet’s download. com is the AVG anti-virus free edition. This free edition offers full time system scanning and virus-protection complete with periodic updates. Usually this software is preferred by most users because it is lightweight, free, and effective.

Unlike security suites that takes up a lot of disk space and RAM that it acts almost like some malwares, this free anti-virus does little in slowing down your computer even if it is scanning your computer. Also having good

reviews from its users is the Kaspersky anti-virus. This was claimed to be more effective in detecting and removing threats, but unlike AVG, it is only available for trial and requires subscription for further updating and use. Aside from that downside, it has been recommended by most users and experts alike. The Secunia Personal Software Inspector is also a free application that can be used on machines running Windows. It is used to determining the missing files and security patches that may be vital to your system.

Another worthy tool is the OpenDNS. It does not need to be installed in your machine but rather; you simply need to change your DNS settings. When using OpenDNS, the user is warned when he or she visits a phishing site, and speeds up your connection as a bonus. This is really handy for users as it provides them warnings and notification when they are visiting websites that are not safe. Anti-malware tools are so diverse and not one of them offers complete protection.

Some infections are detected by some which are not detected by others, so it was said to be good measure to install two or more of these anti-malware softwares if it doesn’t slow down your system. The most commonly used is Ad-aware, one of the most effective spyware detection tool, and also the most popular. Also available is Spybot Search and Destroy, a free tool which effectively blocks thousands of spyware variants. It also guards your registry and prompts the user whenever a certain program attempts to change something important to the registry of your computer. LinkScanner Lite of the Exploit Prevention Labs integrates on the search engine for both Internet Explorer and Firefox.

It warns you of threats that appear in search results including hacked pages that had already been identified in the past. Computer security is an ever-changing process. It is constantly changing and evolving as the underlying technologies of computer networks likewise evolve. As computer users we must be aware of the existence of these threats and keep ourselves informed and educated as to how we can cope with the different developments relating to these threats. We must also be responsible when using new technologies, as embracing something without fully understanding it can prove to be detrimental to us and our organizations.

Being in an on-going learning process of computer security, we must keep our eyes open to emerging threats, as we are also the ones who are going to benefit as a whole when these problems are identified early. I believe that to completely eradicate computer threats, laws should be passed on countries worldwide that makes it possible to take down businesses that employ these people. Spammers promoting a certain website or product are being paid to do what they are doing, and even if security experts and tools are used to block these spam messages, it only removes the symptoms of the problem. To eradicate these threats one must understand why they exist and for what purpose, as these threats did not exist solely for demonstration purposes. This way the actions and efforts can be directed to the root of the problem.

This is important if we, as the users of computers and the internet, are to maintain the internet’s health. A huge amount of bandwidth consumption and online activity can be attributed to spamming, and without taking early measures, the costs may drastically increase as time passes.