Cyber security and privacy techniques.

In today society almost everyone has some form of computer or phone with internet capacity that are exposed to hackers and those that wish to interrupt the cyber world. It is imperative that we all become better educated to the risks and pitfalls that go along with accessing cyber space from any kind of device with access to the world-wide web. Be it by cell device, laptop, notebook, or home computer.

I would like to take this time to inform others of the current trends being used to secure not only our devices but our privacy and what the future holds for the growing security and privacy problems in the cyber world. CURRENT TRENDS It is difficult to control and protect individual computer users as there are many different ideas of what the concept of privacy means in different countries. However, there are some basic activities that are considered an invasion of privacy no matter where you live in the world.

Examples of these are as follows: * Collecting and analyzing user data without the user’s knowledge/consent or authorization. * Employing user data in a way other than was authorized. * Disclosing or sending user data to others without the user’s knowledge and authorization. These things are considered don’t in cyber space, so even if there are international laws on privacy, [some countries and companies would still be likely to operate in an opprobrious way] (Subramanian, 2008).

In 1991 the president of the Association for Computing Machinery showed his support for the fair information practices, which included the principles of notice, choice, access, and security, which urged all organizations to observe the rights of people they collect personal information about as well as their

online activity. Later, our government asked the commerce department to assist the Federal Trade Commission to encourage organizations to place self-regulatory practices in place, but as of 2002 these approaches were found to be ineffective in rotecting consumer information (Subramanian, 2008).

Right now in cyber space personal information is collected by the use of web cookies, these cookies are digital information sent from a web server and stored on the individual's hard drive by way of the browser or network applications, " Cookies were designed to address the problem of statelessness inherent in the Hypertext Transfer Protocol (HTTP)" (Subramanian, 2008, p. 9). These cookies provided a solution to the statelessness for they allow for continuity between browser and web server.

They have been proven to be the most reliable and network friendly means to provide needed state functionality on the web. However, this function can also be provided by embedding state information in URLs simply using hidden fields in the HTML forms and or using the client's IP address (Subramanian, 2008). There are two types of cookies, the session cookie which last only as long as the browser session with the server and the persistent cookie which remains stored on the hard drive of the individuals computer or other device until it expires or is deleted.

Although persistent cookies can help the user visit websites previously visited, " The persistent cookie also has more significant privacy implications because storage of navigational streams and log-in information could be used to monitor and track user browsing behavior and linked to any other

personal information provided” (Subramanian, 2008, p. 10). These cookies can also be shared by third part web hosts and are likely used to track activities of a specific web-site or can track the user’s moves from web-site to web-site (Subramanian, 2008).

One of the technologies used to protect privacy on the internet is called an Anonymizer. This technology [provide the ability to sanitize packet headers passed from the client to the server] (Subramanian, 2008, p. 11). The early version was software that acted as a proxy server and it intercepted any communications between the browser and the server allowing the removal of any and all personal information about the user. However the current version uses secured socket layers or (SSL) technologies when sending URL requests.

This version acting as a firewall like technology encrypts the communication tunnel between the sender and the anonymizer proxy, routing the traffic through many different proxy servers, which helps to disguise the users IP address (Subramanian, 2008). Another option is a web filter, these software programs block cookies, advertisement’s as well as web bus. But there are some negative things that happen when using a filter. One example is the software fails to think about asking for consent from the user.

It simply blocks all cookies and prevents the user from using the personalized setting they prefer, even if the site is trustworthy, such as government sites, or bank sites. Still, this does not mean that it is impossible to invade the user’s privacy, personal information can still be gotten through the users IP address, how long a user is interacting with the internet, and the

geographical location. Therefor it is wise to use additional privacy protection (Subramanian, 2008).

Next we have “ Evidence Erasers,” these programs delete any and all stored internet activity that might be stored in log files or other hidden file that most people never know about. Some of these programs even exceed the Department of Defenses’ standards when it comes to destroying data. But it also frees up disk space and helps the PC perform better, as well as permanently deleting cookies and others files that clutter up the user computer space (Subramanian, 2008).

FUTURE TRENDS One thing I thought might be good information to have under ones hat of infinite knowledge of cyber security and privacy is that even though Mobile malware has been increasing, “ attackers’ biggest bang for the buck continues to be attacking Windows systems, largely via operating system and application-level vulnerabilities, as well as third-party plug-ins with known bugs.

Even so, expect the ongoing, negative headlines associated with Android smartphone hacking–or “ smacking,” as Bit9’s Sverdlove calls it–to drive more manufacturers to create locked-down Android smartphones, which would be a boon for securing business users”(Schwartz, 2012, para. 5 – 6). So in other words to boost their marketable value and profit’s they made the Android type phones with higher quality security.

If this had not been done and continued to be improved regularly, some companies that do business over the phone, could lose valuable information to competitors with the right types of attacking software, not to mention it

helps to better protect the personal information belonging to individuals as well. “ Up until now IT security has frankly been a niche industry. No one segment has gone much over $5 billion in total spending” (Sans Technology Institute, 2011, para. 4).

One of the things that will change in the future are the Incident response teams, what was once just a virtual response team similar to fire department volunteer teams (Same concept) during the incident, are likely to become a fulltime team people, who are dedicated to responding only to cyber security incidents, that need forensic analysis or reverse engineering malware specialists. The reason for this is that as the threats become more frequent organizations can not pull people from their normal duties to work on security issues.

For most companies the ratio is 13 to 14 fulltime responders to a 100, 000 node network, as a result of this the need for trained responders will rise quickly (Sans Technology Institute, 2011). I believe part of the reason that there are so many problems with glitches; computer freeze ups, server interruption’s and network capacity problems are a result of the IPv4 address space becoming overloaded and out of room to grow.

The IPv6 will allow for more growth but to do this they must add support and enable support for auto configuration mechanisms. The only real hold up is a lack of security tools to be used, and implementing it is a very time consuming and difficult process. If done improperly it can lead to what is called shadow networks of tunnels which will be undetectable by intrusion

detection software and firewalls as well as many other security features (Sans Technology Institute, 2011).

Another step taking us into the future of cyber security would be improvements of secure software development teams. Not all but venders have strived to eliminate software bugs, but the major ones have begun to test their own systems for attacker flaws, Attackers are always looking for weaknesses in security systems which enables them to invade the system and gain personal or company information, they are able to do this because of the lack of hardware development knowledge and practices.

With all the things in today's society having small computers in them an attacker having control of critical hardware systems could greatly affect many things such as electrical generation and even traffic management systems (Sans Technology Institute, 2011). As computer hackers and attackers become smarter and wind up using new technology ideas before our government and large corporations do, the need for improvement's will always be an issue.

It is comforting to know that these organizations are now and will continue to strive for improvements in our cyber technology to secure personal, business, and country's important information from the eyes of those that wish to use these systems to harm others. I learned many things researching this information and have a better understanding of why this is such an important realization for everyone in the world, as we are all interconnected by cyber space.