Internet Security

Khaled Alotaibi

Abstract- Today, people are more dependent on the internet in order to complete their tasks and live their lives. Many more people use the internet not just for e-mailing but for filing their taxes, using to complete their homework, communicate with their friends and family, buy and sell goods, etc. However, this would also lead into more and more people using the internet to do malicious things to innocence. Computer networks hold valuable information such as credit card information, financial data, technical, trade, and government secrets, mailing lists, medical records, etc. (Darney). The Internet, as a connector between computer systems, is also a highway of access to valuable data stores. The issue is that it is even easier to perform these malicious tasks than ever before. To prevent these issues from happening, internet security was developed over time to be the primary defense.

Introduction

Today, people are more dependent on the internet in order to complete their tasks and live their lives. Many more people use the internet not just for e-mailing but for filing their taxes, using to complete their homework, communicate with their friends and family, buy and sell goods, etc. However, this would also lead into more and more people using the internet to do malicious things to innocence. Computer networks hold valuable information such as credit card information, financial data, technical, trade, and government secrets, mailing lists, medical records, etc. (Darney). The Internet, as a connector between computer systems, is also a highway of access to valuable data stores. The issue is that it is even easier to perform these malicious tasks than ever before. To prevent these issues from happening, internet security was developed over time to be the primary defense.

Internet security is a term for a very broad list of issues covering security for transactions made over the Internet. It generally encompasses browser security, the security of data entered through a Web form, and overall authentication and protection of data sent via Internet Protocol. Internet security relies on specific resources and standards for protecting data that gets sent through the Internet, which includes the use of encryption such as Pretty Good Privacy (PGP). Other aspects of a secure Web setup includes firewalls to block unwanted traffic, strong passwords to prevent hackers from accessing sensitive information, and anti-malware, anti-spyware and anti-virus programs to monitor Internet traffic for dangerous attachments (Janssen).

Internet security is generally becoming a top priority for both businesses and governments because good Internet security protects financial details and everything else handled by a business or agency's servers and network hardware. Insufficient Internet security, however, threatens to collapse an e-commerce business or any other operation where data gets routed over the Web (Janssen). Most people would think that Internet security is a relatively recent issue, but it is actually older than the average person thinks it is.

History:

Even though the e-mail system was conceived in 1969, the information security history during the 1970s was largely untouched by digital calamity (Pillai, Symantec). It was marked, however, by the exploration of emerging telecommunications technology. The first modern day hackers appeared as they attempted to circumvent the system and make free phone calls, a practice called "phreaking." Perhaps the most publicly well know phreaker was John Draper, alias Captain Crunch, who helped pioneer the practice. He was later arrested and convicted on charges related to his nefarious phreaking activities multiple times (Symantec). It wasn't until the 1980s that the security issues we would know today came into light.

The world was made familiar with the term 'computer virus' for the first time in 1983 by Fred Cohen. The first PC virus, called "Brain", was created in Pakistan in 1985 and by 1987, with the growing number of Internet hosts and the personal computer industry, more people gained access to Internet, making it no longer safe. Privacy and security concerns started mushrooming and the terms "hacker", "cracker" and "electronic break-in" were coined, when Robert Morris launched the Internet worm, called the Morris Worm, which spread across 1/10th of the Internet hosts. He was then sentenced to three years of probation, 400 hours of community service and $10,000 fine (Pillai, Symantec, Miller). These issues became so severe that the Computer Fraud and Abuse Act was instituted in 1986 and a computer hacker named Kevin Poulsen, was featured on America's Most Wanted; and arrested in 1991, after spending several years as a fugitive (Symantec). In 1988, the Computer Emergency Response Team (CERT) was formed and acted as the focal point of computer security concerns for Internet users (Pillai, Symantec).

The 1990s is where the dawn of the modern information security industry began (Symantec). The restriction on the commercial use of Internet was lifted by the National Science Foundation in 1990 and many companies, organizations and individuals hosted their own websites. By 1992, the numbers of Internet users increased by 341%, but hackers started working widely around 1995 and caused a lot of trouble (Pillai). Notable threats witnessed during this decade included: the Michelangelo virus, Melissa, and Concept, the alteration of the websites of the U.S. Justice Department, the CIA and the U.S. Air Force, distributed denial of service attacks and the bots that made them possible were also born, such as Trin00, Tribal Flood network and Stacheldracht (Pillai, Symantec). Among other things, AOL suffered through the first real phishing attacks as fraudsters aimed their efforts at stealing users' credentials. Privacy watchdogs called out in concern as tracking cookies were born, allowing ad networks to monitor user surfing behaviors in a rudimentary fashion (Symantec). Despite efforts to prevent these issues, Internet systems today still cannot be deemed foolproof, and always need a security back-up to save the computer systems (Pillai).

The first decade of the 21st Century was when malicious Internet activity turn into a major criminal enterprise aimed at monetary gain. Adware and spyware entered the scene with such programs as Conducent TimeSink, Aureate/Radiate and Comet Cursor. Perhaps even more visible than adware and spyware, self-propagating malware also appeared. Big name threats such as Code Red, Nimda, Welchia, Slammer and Conficker all took advantage of unpatched machines. Phishing attacks also became commonly used as well, targeting both online banking and social networking sites. Zero day attacks, rootkits, rogue antispyware, SPIM, clickfraud and other attacks also all made their mainstream debut in this decade, as well (Symantec).

Key logger: (Keystroke logging):
Keystroke logging, frequently alluded to as key logging or keyboard capturing, is the activity of recording (or logging) the keys struck on a keyboard, commonly in a secretive way so that the individual utilizing the keyboard is ignorant that their activities are being monitored. It has utilizes as a part of the investigation of human–computer association. There are various key logging systems, running from hardware and software-based ways to deal with acoustic investigation.

Software-based Key Logger:
These are programs intended to work on the target's PC software. Key loggers are utilized as a part of IT organizations to investigate specialized issues with PCs and business networks. Other legitimate uses incorporate family or specialists utilizing them to monitor the network utilization without their clients' direct information. Software Key Loggers have advantages of invisibility to human eye, possibility of remote installation; can record your information using your cameras and microphones. But as there are advantages there are disadvantages too that Software-based Key Logger can be detected by some malware detection software and removed immediately, as in transmission can be intercepted by others and if you're caught it can be used as an evidence against you in court and can cause you a lot of problems.

From a specialized point of view there are a few categories:

- Hypervisor based
- Kernel based
- API based
- Form Grabbing based
- Memory Injection based
- Packet analyzers
- Remote Access Key loggers

Hardware-based Key Logger:
Hardware key loggers are utilized for keystroke logging too and they can be implemented via BIOS-level firmware, or alternatively, via a device plugged in line between a computer keyboard and a computer. They log all keyboard activity to their internal memory. Hardware key loggers have an advantage over software key loggers as they can begin capturing the user's data from the moment a computer is turned on (and are therefore able to intercept passwords for the BIOS or disk encryption software).

All hardware key logger devices have following:

- **A microcontroller:** this translates the information stream between the keyboard and PC, forms it, and passes it to the non-volatile memory
- **A non-volatile memory device:** for example, streak memory - this stores the recorded information, helps in retrieving data when power is lost.

From a specialized point of view there are a few categories:

- A Regular Hardware Key logger
- Wireless Key logger sniffers

- Firmware
- Keyboard overlays
- Acoustic key loggers
- Electromagnetic emissions
- Optical surveillance
- Smartphone sensors

An early key logger was written by Perry Kivolowitz and posted to the Usenet news group net.unix-wizards, net.sources on November 17, 1983.[27] The posting seems to be a motivating factor in restricting access to /dev/kmem on Unix systems. The user-mode program was operated by locating and dumping character lists (c lists) as they were assembled in the UNIX kernel.

In the 1970s, spies installed keystroke loggers in the US Embassy and Consulate buildings in Moscow and St Petersburg. They installed the bugs in Selectric II and Selectric III electric typewriters. Soviet embassies used manual typewriters, rather than electric typewriters, for classified information—apparently because they are immune to such bugs. As of 2013, Russian special services still use typewriters. (WIKI)

Other Features:

- **Clipboard Logging:** It captures what is copied on clipboard.
- **Screen Logging:** It captures the screenshots and reveals the information of user to the logger.
- **Recording** of every file you're opening, screenshots of every file you've opened for a while.

Legitimate Use:
Key Loggers can be used by IT companies to detect the problems in their customers PC's and business networks and troubleshoot it for them automatically, families use this technique to monitor their children activities and data usage by them without their knowing also business companies utilize it in a same way to monitor their customers' data usage. Other legitimate uses include it as a suitable research tool to analyze the writing tests, other hourly jobs. For example Odesk uses their application to capture the screenshots of user to check if he is working or not during hourly jobs and keep a track of you without knowing.

Illegal Use:
Key Loggers can be used in numerous illegal ways. When we hear about a Key Logger first thing comes to our mind is illegitimate use or theft of someone's information without their knowledge. It can be used to capture passwords, your emails, your visa card information and even your assignments. It can be used by Federal agencies to steal your information without your knowing. And believe me they are stealing our information without our knowledge and we cannot do a thing. So basically there are more bad ways to use key loggers than the good ways.

From all the discussion above we now know the difference between software and hardware key loggers and their advantages and disadvantages too. We know legitimate ways to use these key loggers and illegitimate too and we can conclude from this discussion is that there will always be a theft of information even if it is being used in legitimate way, your information is being leaked to someone without your knowledge and it can be used to harm you so basically we should be aware of these key loggers and scan our computers regularly for these type of malicious software and in this way we can avoid the stealth of our information.

Identity theft definition:

The short answer is that identity theft is a crime. Identity theft and identity fraud are terms used to refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain.

Methods of stealing Identity:

Shoulder surfing

Many people do not realize how easily criminals can obtain our personal data without having to break into our homes. In public places, for example, criminals may engage in "shoulder surfing" watching you from a nearby location as you punch in your telephone calling card number or credit card number or listen in on your conversation if you give your credit-card number over the telephone to a hotel or rental car company.

Trash or mail box

If you receive applications for "pre-approved" credit cards in the mail, but discard them without tearing up the enclosed materials, criminals may retrieve them and try to activate the cards for their use without your knowledge. (Some credit card companies, when sending credit cards, have adopted security measures that allow a card recipient to activate the card only from his or her home telephone number but this is not yet a universal practice.) Also, if your mail is delivered to a place where others have ready access to it, criminals may simply intercept and redirect your mail to another location.

Internet

In recent years, the Internet has become an appealing place for criminals to obtain identifying data, such as passwords or even banking information. In their haste to explore the exciting features of the Internet, many people respond to "spam" unsolicited E-mail that promises them some benefit but requests identifying data, without realizing that in many cases, the requester has no intention of keeping his promise. In some cases, criminals reportedly have used computer technology to obtain large amounts of personal data.

Type and Purpose of Identity theft:

Identity cloning and concealment

When a person impersonates someone else in order to conceal their own true identity. Examples might be illegal immigrants, people hiding from creditors or other individuals, or those who simply want to become "anonymous" for personal reasons. Another example are posers, a label given to people who use somebody else's photos and information through social networking sites. Mostly, posers create believable stories involving friends of the real person they are imitating. Unlike identity theft used to obtain credit which usually comes to light when the debts mount, concealment may continue indefinitely without being detected, particularly if the identity thief is able to obtain false credentials in order to pass various authentication tests in everyday life.

Criminal identity theft

When a criminal fraudulently identifies himself to police as another individual at the point of arrest, it is sometimes referred to as "Criminal Identity Theft." In some cases criminals have previously obtained state-issued identity documents using credentials stolen from others, or have simply presented fake ID. Provided the subterfuge works, charges may be placed under the victim's name, letting the criminal off the hook. Victims might only learn of such incidents by chance, for example by receiving court summons, discovering their drivers licenses are suspended when stopped for minor traffic violations, or through checks performed for employment purposes.

It can be difficult for the victim of a criminal identity theft to clear their record. The steps required to clear the victim's incorrect criminal record depend in which jurisdiction the crime occurred and whether the true identity of the criminal can be determined. The victim might need to locate the original arresting officers and prove their own identity by some reliable means such as fingerprinting or DNA testing, and may need to go to a court hearing to be cleared of the charges.

Synthetic identity theft

A variation of identity theft which has recently become more common is synthetic identity theft, in which identities are completely or partially fabricated. The most common technique involves combining a real social security number with a name and birthdate other than the ones associated with the number. Synthetic identity theft is more difficult to track as it doesn't show on either person's credit report directly, but may appear as an entirely new file in the credit bureau or as a sub file on one of the victim's credit reports. Synthetic identity theft primarily harms the creditors who unwittingly grant the fraudsters credit. Individual victims can be affected if their names become confused with the synthetic identities, or if negative information in their sub files impacts their credit ratings.

Medical identity theft

The report's definition of the crime is that medical identity theft occurs when someone seeks medical care under the identity of another person. In addition to risks of financial harm common to all forms of identity theft, the thief's medical history may be added to the victim's medical records. Inaccurate information in the victim's records is difficult to correct and may affect future insurability or cause doctors relying on the misinformation to deliver inappropriate medical care. After the publication of the report, which contained a recommendation that consumers receive notifications of medical data breach incidents, California passed a law requiring this, and then finally HIPAA was expanded to also require medical breach notification when breaches affect 500 or more people.

Child identity theft

Child identity theft occurs when a minor's identity is used by another person for the impostor's personal gain. The impostor can be a family member, a friend, or even a stranger who targets children. The Social Security numbers of children are valued because they do not have any information associated with them. Thieves can establish lines of credit, obtain driver's licenses, or even buy a house using a child's identity. This fraud can go undetected for years, as most children do not discover the problem until years later. Child identity theft is fairly common, and studies have shown that the problem is growing. The largest study on child identity theft, as reported by Richard Power of the Carnegie Mellon Cylab with data supplied

by All Clear ID, found that of 40,000 children 10.2% were victims of identity theft.

Financial identity theft

The most common type is financial identity theft, where someone wants to gain economic benefits in someone else's name. This includes getting credits, loans, goods and services, claiming to be someone else.

How companies protect the client

Often when discussing security measures, only mentioned purely technical, such as firewalls, antivirus or backup systems. However, the most effective measures are usually management measures raised medium and long term from a strategic and tactical point of view.

We will briefly mention the measures and security systems frequently grouped under two aspects: Management measures and technical measures. The first should be implemented by the managers of the organizations as part of the strategic and tactical plans, while the latter correspond to tools and technical systems designed to prevent, control or recover damages that can undergo the systems by the appearance of certain security threats.

Management Measures

Emanating from the strategic aspect of information and corporate systems, two management tools are often generated: security policies and contingency plan. Security policies of an organization are internal rules and procedures to be followed by members of the organization to comply with the security requirements that wish to preserve. It should describe the criticality of information systems and the roles of each job and the mechanics of access to systems, tools, documentation and any other component of the information system. It often break down security policies in detailed procedures for each system component individually, so for example, you can create documents describing emails treatment policies, Internet use polices, backup, virus treatment and other malicious logic, training policies for staff safety, etc. It should be noted that security policies must emanate from the corporate strategy and that it should document all members of staff. For its part, the contingency plan describes the procedures to be followed by the appearance of significant contingencies that could cause serious consequences for the organization. You must be detailed the steps, for example in case of total destruction of the systems by flood, fire, etc. Often the simple preparation of the plan discover defects in the systems that can be alleviated with relative ease. For example, you may find that no backup of crucial information for the company remain physically safe places, or at least distant to the location of the systems susceptible to damage sites.

Technical Measures

Among the more established techniques are backups, anti-virus, firewall, authentication mechanisms and cryptography. Backups and in general any form of redundancy, are aimed at ensuring the availability of the systems against any eventuality. The antivirus intended to prevent the appearance of malicious logic in case of infection and try to remove it from the system. Among the antivirus it should be noted that inspect those emails preventing infection of the recipients. For its part, the firewall try to reduce the number of potential routes of access to corporate systems from outside, establishing limitations on the number of equipment and services visible. Another essential techniques throughout the organization are authentication mechanisms. These mechanisms can range from simple peer-based schemes password to complex distributed systems based on credentials or biometric authentication systems based on the recognition machining physical characteristics of individuals. Finally, all security scheme should include in one way or another encryption of sensitive information. Sometimes it may be enough encryption passwords, while other communications encryption and databases is essential. As more advanced measures, we can mention the stenography, exploit detection and intrusion detection. Stenographic techniques try to hide information. Unlike cryptography, which tries to make the information unreadable, steganography tries to prevent even notice its existence. Ex: enterprises engaged in producing digital documents, may be interested in include certain invisible mark in a way that is demonstrably his own and can be pursued illegal copies. The vulnerability detection tools are often as auditing tools that can show ways most likely would use intruders to access the systems. Finally, intrusion detection systems try to discover, often in real time, unauthorized access to systems, both from outside the organization, and from within the facilities of the company.

Conclusion:

The goal of computer security is to protect valuable computer resources of the organization, such as information, hardware or software. Through the adoption of appropriate measures, the IT security helps the organization accomplish its objectives, protecting its financial resources, its systems, their reputation, their legal status, and

other both tangible and intangible assets. Unfortunately, sometimes it sees computer security as something that hinders the achievement of the very objectives of the organization, imposing rigid rules and procedures to users and systems administrators. But it should look to computer security, not as a goal in itself but as a means of supporting the achievement of the objectives of the organization.

References

Borglund, Josh. "Internet Security: Defining the Threats - TopTenREVIEWS." *TopTenREVIEWS*. TopTenREVIEWS.com, n.d. Web. 21 Apr. 2015. http://internet-security-suite-review.toptenreviews.com/internet-security-defining-the-threats.html

"A Brief History of Internet Security." *SC Magazine*. Symantec, 24 Sept. 2009. Web. 21 Apr. 2015. http://www.scmagazine.com/a-brief-history-of-internet-security/article/149611/

Darney. "Internet Security Law & Legal Definition." *Internet Security Law & Legal Definition*. ECDI, n.d. Web. 21 Apr. 2015. http://definitions.uslegal.com/i/internet-security/

Janssen, Cory. "What Is Internet Security? - Definition from Techopedia." *Techopedias*. N.p., n.d. Web. 21 Apr. 2015. http://www.techopedia.com/definition/23548/internet-security

Miller, Gabriel. "A History of Internet Security." *Life123*. Life 123 Inc, n.d. Web. 21 Apr. 2015. http://www.life123.com/technology/internet/internet-history/history-of-internet-security.shtml

Pillai, Prabhakar. "History of Internet Security." *Buzzle*. Buzzle.com, 10 July 2012. Web. 21 Apr. 2015. http://www.buzzle.com/articles/history-of-internet-security.html

"What Is Internet Security?" *BBC News*. BBC, 06 June 2013. Web. 21 Apr. 2015. http://www.bbc.co.uk/webwise/0/22717881

USDOJ: CRM: About the Criminal Division (USDOJ: CRM: About the Criminal Division)

http://www.justice.gov/criminal/fraud/websites/idtheft.html

"Privacy Rights Clearinghouse". Archived from the original on 2012-09-21. - "Fact Sheet 17g: Criminal Identity Theft: What to Do if It Happens to You "

In re Marie A. COLOKATHIS, Catherine Bauer, M.D., Plaintiff v. Marie Colokathis, 417 B.R. 150 (2009)

McFadden, Leslie (2007-05-16). "Detecting synthetic identity fraud". *Bankrate.com*. pp. 1–2. Archived from the original on 2012-07-18. Retrieved 2008-09-21.

"The Medical Identity Theft Information Page"World Privacy Forum. Retrieved 26 November 2012.

"Correcting Misinformation on Medical Records"Identity Theft Resource Center.