DATA SECURITY: THREAT, CHALLENGE AND PROTECTION

Kr. Ashutosh Manglam[1], Deepak Kumar[2], Indu Khatri3
[1,2]B.tech Student, [3]Assistant Professor
Department of Computer Science Engineering
Bhagwan Mahaveer College of Engineering and Management, Sonipat

Abstract: - This paper discusses the dangers and problems associated with data and how users of a computer can analyses their exposure to data security and threats. It also analyses the different methods and technologies that can be used to protect data on our personal computers and other computing devices, as well as within organizations. Threats on data can emanate from virus attack, hacking, loss of data due to hard disk failure, power failure, deliberate deletion, and visual data theft which can be seen wherever data reside on computers like laptops, desktops, and other related computing devices. The paper recommends that to avoid these threats, the user should choose passwords that are not obvious and also make sure their virus protection subscription is current and updated.

Keywords: - Data Security, Hackers, Cryptography, Backup, Security, Hacking, Virus

1. INTRODUCTION

Data security is a term that describes technologies used for the protection and safeguarding of data. According to Wikipedia [1] data security is defined as a technique used in protecting data from destructive forces, and unsolicited actions of unauthorized users. Denning Dorothy Elizabeth defines data security as the science and study of methods of protecting data in computer and communication systems, from unlawful disclosure and modification [2]. Because data is so essential to the viability of an organization, finding the means to protect and prevent unauthorized access to data and ensure the integrity of data is the topmost priority of both the user and the system administrator that the computer (the physical object that is directly connected to the theory) is not a focus of investigation (not even it he sense of being the cause of certain algorithm proceeding in certain way) but it is rather theory materialized, a tool always capable of changing in order to accommodate even more powerful theoretical concepts.

On June 24, 2014, a newspaper magazine, based in the United States of America (USA), updated a news report on the topic “Key Figures in the Phone Hacking Case” [3]. In that news report which was available on their website, they listed the key figures involved in a widespread phone hacking scandal. Among those accused are; the Chief Executive Officer of News Corporation (Rupert Murdoch), the Prime Minister of the British Government (David Cameron), the Chief Operating Officer in charge of European operations for News Corporation (James Murdoch), and the editor of The News of the World (Andy Coulson). These men and others, directly and indirectly, gained access to the private data of top executives and individuals without their consent and knowledge. What this means Journal of Universal Development Initiative (JUDI) ISSN (print): 2141-6974 Published by Centre for Research and Manpower Development (CREMD) Owerri, Imo State, Nigeria Volume 1, No. 1, December 2014 93 is that they were able to gain access to sensitive information through unauthorized means.

A similar issue came up when the American whistle blower; Edward Snowden, an American computer professional, exposed the secrets of the United States government by revealing details of their surveillance programs (gaining unauthorized access to people’s phone calls, email messages, and any other media through the help of email giants like Yahoo and Google) .

From the above-mentioned cases, it has become very obvious that protection of data should be made a fundamental human right, as it is in the European Union. The Charter of Fundamental Rights of the European Union stipulates that every individual should have the right to the protection of any personal data concerning that individual. It is pertinent to know that the personal data of individuals are processed in many ways and in day-to-day activities - for example, opening a bank account, online registrations, booking a flight, bus or train, issue of credit card, registering for email accounts, signing up for membership of clubs, libraries, etc [5].

2. THREATS AND CHALLENGES TO DATA SECURITY

Threat simply means a person or thing likely to cause damage or danger. There are numerous ways that a computer system and its contents (data) can be attacked. Many of these attacks may include the use of malicious software relatively called malware [6].

- Data may get lost or damaged due to a system crash- especially one affecting the hard disk.
- Data may get corrupted as a result of faulty disks, disk drives, or power failures
- Accidentally deleting or overwriting files
- Computer viruses attack on data can lead to its loss or corruption.
- Hacking into databanks and gaining access to secret information by unauthorized personnel may be altered or deleted.
- It may also be deleted or altered by employees wishing to make money or take revenge on their employer.

No matter how secured or secretive we may be concerning data, there are individuals or things that often with intent or out of curiosity, contest the security of our secured data. Think about the sensitive data you have on your personal computer or other computing devices, and what level of access you can grant your friends to have access to them. You will agree that due to the sensitivity of your data, you may grant little or no access at all to your data. There are many different threats to computer systems and the data stored on them. These threats increased as computers started to be networked not only to local area networks (LANs) but to the internet. Access to the internet has caused data security to be one of the most important considerations in managing a computer system. After all, what is the use of a computer or a computing device, if the sensitive data stored on them cannot be secure?

2.1 Hackers and Crackers

2.1.1 Hackers

In the context of data security, a hacker is a person or group of persons who seek and exploit the weakness in a computer system or computer network. Except the computers and data are protected, they are vulnerable to anyone who wants to modify the files without the consent of the owner. Such individuals or groups who maliciously and illegally seek data in computers are called hackers [7]. Also, Hackers are people who gain unauthorized access to computer or telecommunication systems for the challenge or even the principle of it. For example, Eric Corley, publisher of a magazine called 2600: The Hackers' Quarterly, believes that hackers are merely engaging in "healthy exploration." In fact, by breaking into corporate computer systems and revealing their flaws, he says, they are performing a favour and a public service. Such unauthorised entries show that corporations are involved in the leaks in their security system [8]. Hackers use computerized tools like IP address detectors to search for computers that are connected to the internet. Once found, they attempt break-in and then take control of the computer, this allows them to interrupt service and commit identity theft [9].

2.1.2 Crackers

On the other hand, crackers are hackers who gain unauthorized access to computer information but do so for malicious purposes. Crackers attempt to break into computers deliberately and obtain information for financial gain, shut down hardware, pirate software, or destroy data. [8]

2.2 Virus

A computer virus is software that is designed to interrupt or stop the normal operations of a computer. This software is called a virus just like a biological virus because it is transmitted from one infected computer to another. The most common and possible ways by which a computer virus can infect one's computer are through file downloads from the internet, when attachments are opened from emails, or when USB memory sticks are exchanged from one computer to the other [10]. According to Bill Daley, a computer virus can be seen as a hidden code within a program that may damage or destroy the infected files [11]. Computer viruses pose a serious threat to data security because of their behaviour. When a virus attacks a computer system, the intent is always for destruction. As it replicates itself across a network or from one computer to another (if it is copied through an external storage media), it destroys every relevant data it comes in contact with, even more, it makes the data unreadable and often prevents access to its content. Now when this happens, it has become a threat to the computer user or data owner, who has been denied access to sensitive and classified information. A significant incident of the effect of a computer virus was felt by South Korea in which they suffered a disruption that paralyzed the computer networks of broadcasters and banks. An attack which they seriously believed was caused by a virus. North Korea also suffered a similar attack when Journal of Universal Development Initiative (JUDI) ISSN (print): 2141-6974 Published by centre for Research and Manpower Development (CREMD) Owerri, Imo State, Nigeria Volume 1, No. 1, December 2014 95 they accused the US and its allies of attacks on its internet servers [12

2.3 Trojan horse

Just like the movie "Troy" in which a horse carrying the Greek soldiers in disguise was used to destroy the city of Troy, this same behaviour is exhibited by the computer program known as the Trojan horse. It is a program that disguises itself to be harmless, pretending to help you protect your computer system and data from theft, malicious attacks, and other havocs. But, behind the program is another terrific program executing the exact opposite of the intentions or behaviour of the original program. Trojan horses often hide in games and other small software programs so that when you download it unknowingly, it will be executed on your computer. Unlike viruses, Trojans do not replicate themselves. Rather, they leave behind a program that can be contacted by another computer. Trojans have also been known to destroy files on your hard disk. One example of a Trojan horse is a program that claims to find and delete viruses, but instead, introduces a virus to your computer [9]. Because Trojan horses often arrive in the form of attachments to enticing email messages, the misdeeds of the Trojan horse are activated when the attachment is opened, therefore, email attachments from unknown sources should never be opened [6]. Trojan horses are designed in a way that allows a hacker remote access to a target computer system and once it is installed on the target computer, a hacker can access it remotely and perform several operations. However, these operations are restricted by the user privileges on the target computer system and the design of the Trojan horse [10].

2.4 Worms

A worm is an independent program that transfers itself through a computer network, settling down as an inhabitant in computers and forwarding copies of itself to other computers. As in the case of a virus, a worm can be designed merely to duplicate itself or to perform more dangerous damage. A typical sign of a worm is an explosion of the worm's duplicated copies that reduce the performance of genuine applications and can ultimately overload an entire network or internet [6]. Worms are self-replicating programs that use a computer network to send copies of themselves to computers on the network and they may do so without any user intervention, this is as a result of security weaknesses on the target computer. Worms are different from viruses and Trojan horses because they do not need to attach themselves to existing programs. Typically, worms cause some harm to the network by consuming bandwidth while viruses corrupt or modify files on a targeted computer [10].

2.5 Other threats

In addition to threats to data due to viruses, worms, Trojan horses, and Journal of Universal Development Initiative (JUDI) ISSN (print): 2141-6974 Published by centre for Research and Manpower Development (CREMD) Owerri, Imo State, Nigeria Volume 1, No. 1, December 2014 96 hackers, and crackers, the security of data can also be threatened through other means like spyware, malware, adware, and hoaxes. These software-based threats can be used to monitor your activity on the internet, collect information about what you are doing and transmit it to other computers. These malicious programs can also be used to generate streams of unsolicited advertisements to your computer, usually viewed through pop-up windows [10]. The other threats are human threats which often are deliberate and could also be in error. When computer data is corrupted due to faulty disks, disk drives, or power failures, the integrity and accessibility of that data are threatened. Also, employees wishing to make money or take revenge on their company, due to ill-treatment or being under-appreciated can threaten the security of data in that company by deliberately deleting sensitive information, altering them, or even selling them to another competitive company. All these actions pose big threats to data, however, they can be avoided, limited, or eliminated to ensure proper security of data by implementing data protection measure [6].

3. DATA PROTECTION

It is important to safeguard data against unauthorized access or accidental or deliberate loss or damage. According to online Business Dictionary, data protection is defined as the use of techniques such as file locking and record locking, database shadowing, disk mirroring, to ensure the availability and integrity of data [13].

The question is “How do we protect data from these threats?” The following techniques will ensure that data is properly kept safe from intrusion, theft, deletion, and alteration.

3.1 Antivirus Software

An antivirus program is a computer program developed to secure a computer and the computer user from the threats of viruses, worms, spywares and other malicious programs which pose threats to computer data [13]. Some antivirus software that can be used to protect our computer system are:

- Kaspersky
- MacAfee
- Norton Symantec
- Avira
- ESET
- Dr Web
- Trend Micro
- Avast

3.2 Backup

A bitter experience that almost every computer user has faced at one point is the accidental deletion of data and having no backup copy. If you have had that experience, I am sure it will make you a crusader in backing up data. A backup is a copy of a file or other item of data made in case the original is lost or damaged. It is useful because, in the event of loss or damage, there is always something to fall back on [8].

3.3 Guard against Power Fluctuation

The excess voltage causes damage to electronic gadgets plugged into wall sockets. Electricity is supposed to flow to outlet at a steady voltage level under normal circumstances. However, you have noticed instances when the light in your house suddenly goes dim or brightens momentarily. Such power fluctuations cause havoc to your electronic equipment. To protect your computer and other computing devices and most importantly your data, plug your computer, monitor, laptops, and other devices into a surge protector or surge suppressor [8].

3.4 Cryptography

Cryptography is the analysis and decryption of encrypted texts. It is the science of keeping information secured in computer networking. The processes involved when encoding and decoding information in cryptography are called encryption and decryption respectively [14]. In this model, the message is referred to as plaintext or cleartext and the encrypted text is called ciphertext. The plain text is encrypted by an encryption algorithm and an encryption key. The ciphertext is transmitted over the communication channel. At the receiving side, the ciphertext is decrypted by a decryption algorithm and a decryption key, resulting in plaintext. The encryption and decryption algorithms are called ciphers [14]

3.4.1 Limitations of Encryption

Cryptanalysis is the art of breaking ciphers or decrypting information without having the key [14]. This process of attempting to read the encrypted message without the key is unchallenging with modern computers than with older computers. Modern computers are pretty fast to permit 'brute force' methods of cryptanalysis. If the key is longer, it also takes a longer time to use the 'brute force' method of cryptanalysis which also makes the process of encrypting and decrypting the message slower. The length of the key is very important to the security of the encryption method but the 'safe' key length changes every time manufacturers of CPU produce new processors. Though encryption does not completely make your data secure, however, failure to use encryption means that any data on transit will be simple to read. Encryption ensures that anyone who reads your messages has worked hard on it [15].

3.5 Authentication

To authenticate means to prove or show that something or somebody is true or genuine. With authentication comes authorization. Once the verification process is completed, the computer user is allowed access (authorized) to any information he or she wants from the computer. This process of identifying an individual is usually based on a username and password. The password helps protect the computer user from malicious use of his or her computer and the viewing of his or her display by others when the computer is not attended [16]. As a computer user running a Windows Operating System, it is safer to use the windows combination key Ctrl + L to lock your computer screen when it is unattended. For other mobile devices like your smartphones and tablets, make sure you enforce a password security feature using Sim lock, pattern lock or any other form of security provided by your phone manufacturer, to keep your mobile devices secured from unauthorized access.

4. CONCLUSION

Data security issues are constantly changing. Every day, new threats arise and fresh best practices emerge to keep individuals and organizations at the forefront of protecting sensitive information. However, it will be fruitful to pursue further research on this interesting topic because there are lots of information about this topic that were not conclusively addressed. We believe that to properly address the issue of Threats and Challenges of Data Security, there should be legal approaches in the form of protection acts and penalties for those who engage in the breach of data security. We want to conclude that this is just research; it is not an entire work. Our colleagues in the same discipline are welcomed to improve on the little enlightenment we could offer on this topic.

5. RECOMMENDATIONS

Having looked at the threats on data and possible protection, we further recommend that individuals and organizations should:

- Choose passwords that are not obvious.
- Make sure their virus protection subscription is current and updated.
- Know about the security risks of e-mail attachments.
- Remove employee’s network access immediately after an employee leaves the organization.
- Not run any unnecessary network services.
- Check and delete unwanted browser histories regularly.
- Always log out after every page session.
- Try and password their files with a password that cannot be easily guessed.

REFERENCES

[1] Wikipedia. (2012, February). Data Security. Retrieved August 18, 2014, from Wikipedia the free Encyclopaedia: http://en.wikipedia.org/wiki Data_security

[2] Denning, D. E. (1982). Cryptography and Data Security. Reading: Addison-Wesley Publishing Company.

[3] The New York Times, C. (2014, June 24). 20110708-key-players-inthe-phone-hacking-scandal. Retrieved August 19, 2014, from The New York Times: http://www.nytimes.com/interactive/ 2011/07/08/world/ Europe /20110708- key-players-in-the-phone-hackingscandal.html

[4] Wikipedia. (2013, June). Edward Snowden.