A Study of Data and System Security in Modern Times

Mayuresh Kulkarni[1]

[1]*Computer Engineering (Pursuing), Department of Computer Engineering, Bharati Vidyapeeth College of Engineering, Navi Mumbai, Maharashtra, India*

---***---

Abstract - *System security is the fundamental right an individual can demand in these digital times. While there are various measures taken at different levels to protect the user from online threats, updated knowledge of the topic should be available to all. Hence, this research was undertaken. The text begins with a brief introduction for the topic and defines the background knowledge necessary. Then, the various parameters and frequently observes security threats are discussed in detail under the title of 'system protection necessities', followed by a discussion of different 'security breaches' that one might encounter in his/her secured machine. Post of which, 'worms' are explained and their functions and how they damage the system is discussed, followed by the most important topic of 'encryption'. An example of BitLocker is used to further understand the latest security standard at hardware level using the technology built by Microsoft.*

Key Words: system, security, threat, encryption, bitlocker

1. INTRODUCTION

One may be able to protect their house from thieves but protecting the bits and bytes in this digital world is difficult. While the current security standards do protect from majority of threats, a considerable amount of protection is still very much necessary. To have an idea of the severity of the threat, check the trend of number of viruses, malwares and trojans known since the year 2000. In 2000, around 50,000 viruses were identified, in 2002 the number rose to 60,000 and currently, more than 1,00,000 variations of virus, trojans and malwares are known [1]. But, known does not mean there is a solution or protection available from them. There are still thousands which propose a serious threat to the digital world around us.

Softwares, be it any type and variation, are always vulnerable to some or the other forms of attacks. Some softwares made by companies which are well versed in software-making are better and more secure as compared to those made by unexperienced ones. And this security factor is much more relevant if the software is made for banking, government or military use. These also include system softwares. The systems that the entire digital world relies on should be protected from such known and even unknown viruses. It is thus essential to understand the factors from which the systems should be protected.

This text deals with different types of protection our operating systems and computers need, at software and hardware level respectively, the different types of security breaches that can take place (in different situations). Then a brief study of 'worms' is given to connect the gap between software and hardware protection measures. And finally, a comprehensive study of encryption and most powerful data protection techniques is given to complete the text.

2. System Protection Necessities

Systems need to be protected at hardware and software levels, which has been discussed before. The systems which help run this multi-trillion-dollar internet world is full of threats and security breaches. The following are brief descriptions of threats and vulnerabilities which our systems should be protected from:

1. Security Beaches
   a. Backdoor Attack: Any software or code made has to meet certain security protocols and standards. These standards define the quality of the program and the code written to make it. International standards mandate removal of backdoors or highly secure backdoors (if necessary) to any code which will be publicly available and/or deal with sensitive and personal information. These standards are commonly verified by getting security certificates that prove the program satisfies the legal standards and protocols set in those countries. These standards are increased to alarming levels in certain critical conditions like banking websites, payment gateways, government non-public websites (and servers), and military usage programs. But, since nothing can be 100% perfect, some of the other flaws remain in the programs. To be fair, some backdoor attacks are *generated* in the future. Meaning, a programmer cannot protect its software from something which hasn't been discovered yet and these new-found, and yet to be found, variations of cyber-attack make their way to millions of users' systems.
      A backdoor attack is using these system vulnerabilities to exploit the target system and available target system data. It is an illegal act that is severely punishable under cybercrime laws. Small businesses are more vulnerable to backdoor attacks as the available protection resources and measures are limited to (generally) publicly used and in rare cases a

more advanced version of that. It is only the large and rich organizations that have access to some of the really powerful security as the amount of invested money is well worth the protection it gives. Additionally, backdoors are getting increasingly difficult to detect as protect as the way of getting into the systems is becoming easier, thanks to the rise in demand for 'seamless connectivity'. Increased user comfort definitely comes at a cost, which many are paying heavy prices for.

b. DOS/DDOS attack: DOS, standing for Denial of Service, attacks are more sophisticated and toughened versions of backdoor attacks. They are very difficult to detect and generally come as genuine requests to get service. The main intention of a DOS attack is to overload the system with infinite requests to the immediate attention of the system and deprive other tasks of resources and system attention. In operating systems, DOS attacks at kernel level are generally false system-interrupts which direct to some cycling void functions. In banking systems, requests are in the form of OTP request or empty transaction requests. After a lot of research in DOS attacks, the source was detected using some programming techniques, but by then the DOS was converted into DDOS attacks which make it near to impossible to detect the actual source.

DDOS stands for Distributed Denial of Service. The main difference between them is DOS attacks come from a single source, while DDOS attacks change their source of request after EACH request, making every single ping seem genuine. DDOS and DOS attacks do not aim to steal data or have unauthorized access but want to simply crash the system making it inaccessible to others. DDOS attacks are also called Infrastructure Take-Down attacks (as they make the costly servers and systems unusable).

c. Malware Attack: Malware is something that gets into systems without authorized permission of the system administrator. It comes hidden under some layer of 'genuine' software and once inside the system, it starts its job, something which in cyber-security terms, is called 'system decay'. Other similarly used words for malware are spyware, ransomware, etc. Many a times, these 3 words are used interchangeably and in general purpose communication, make negligible difference.

Malware can get into one system through almost anything these days. Earlier, the famous ILOVEYOU virus (in the year 2000) started by being a simple letter sent as an attachment through emails. The letter seemed to be a simple word file and when clicked, the script used to get executed in the clients' machine, making and doing the damage intended. Almost all of the currently available antiviruses provide a strong safety wall from 99% of known malwares, but some malwares are simply unstoppable. In a recent incident, a tech giant released one of their biggest software updates to millions of people and unfortunately the update came with a lot of bugs, some doing irreversible changes to networking device drivers. The problem was, the security features which the company claimed to provide were tied to the device drivers and a change in them simply failed to provide the necessary protection, making almost 100 million computers vulnerable to almost everything on the internet. Such blunders happen very rarely, but they do set an example of how important and necessary these measures are for the safety and security of the systems.

2. Memory Access Violation: Everything that is done on computers needs memory to run. Even CPU instructions delivered using special registers are first verified through RAM and then enter CPU for processing. Thus, accessing memory is essential for every program to execute. But this permission to Read from and Write to memory may be used for illegal purposes also. In most cases, some memory cells are reserved only for system kernel to access. Meaning, regular (non-system) programs, generally consisting of 3rd party softwares, cannot access these cells at any cost. Programmers who wrote the software have to keep this limitation in mind while designing the software. This may be a continuation to backdoor attack, but even after taking several measures, some loopholes remain in the software while publishing it to public release.

Cyber criminals make use of these loopholes (in this case, memory related) to access the inaccessible areas of RAM. The main intention is not only to read the protected data, but also to overflow the memory with junk data to crash the system. This overflowing is also called Stack Overflow Violation. Also, in older RAM chips (earlier than DDR2 version), some overused cells used to change their polarity and become redundant. So, hackers took advantage of this 'feature' to continuously write-delete-write to the same memory cells continuously as long as they are running. Once failed, next batch of memory cells are occupied. And the process repeated till all the memory cells became unusable.

3. Programs with Excessive Permissions: In past few years, operating systems have started focussing on providing more security to the device and have modified their structure in such a way to give the users more control of their data. To do this,

indivisual hardware level permissions were introduced which allowed and denied specific programs to access specific hardware. The benefit of this model is that the final operating system is much more secure and has a tight hold of hardware underneath.

A simple example would be of a calculator. Many users do not like the stock calculator given by the manufacturers. So, they download one from their respective apps store provided by the operating system. Since the introduction of the new permission structure, every app mentions the permissions it will ask for full experience of the program. Now, those fake programs which appear (or try to appear) to be genuine also have to mention their requirements. Thus, the only input from user will be the logical part where one should analyse whether he/she should download a calculator which asks location, microphone and (in some cases) camera permission! A calculator asking for location, a music app asking for camera, a translation app asking for contacts, etc are some of the key red flags which help to filter potentially hazardous applications from regular safe ones.

3. TYPES OF SECURITY BREACHES

Now that the basic understanding of protection factors is established, understanding the classification of security breaches, if one happens at all, is important.

A security breach is a deliberate internal/external attack to steal, modify or damage information to create a havoc in some manner. This can be done by anyone regardless of his authorization. Security breach in sensitive places such as an important database can potentially lead to large scale loss in financial and other areas.

There are 4 main types of security breaches:

1. Breach of Confidentiality: A breach of confidentiality occurs when a client's data gets exposed to some non-trustable third party without the consent of the client in question. Confidentiality breach is a legal scandal and can have lots of serious consequences if a business if found guilty for that. Data and types of confidentiality breaches include credit card numbers, trade secrets, patents, secret formulae, manufacturing procedures, medical information, financial information, etc.
2. Breach of Integrity: In simple terms, data integrity means accuracy, consistency, and completeness of data over a period of time, generally unless and until modified or edited by authorised personnel. This is one of the most common cases of virus infected computers. The malware enters the system and modifies the system registry; changing the values and files which are important to the system. Databases which store critical information also experience integrity breaches, but those systems generally have backups and can undo the damage to some extent. Integrity breach includes unauthorised modification and editing of data, like opening up of security holes during installation of software or service, changing of credit card numbers of account holders without their knowledge, etc.
3. Breach of Availability: Imagine walking down a staircase at 40th storey. Suddenly at 35th floor, the stairs end and start directly at 20th floor. This means further descent is not possible and have to return back to starting point. Meaning, the unavailability of stairs suspended the task undertaken. This is exactly what happens in breach of availability. Not only data but unavailability of services too can affect some systems to a large extent. This is even more crucial in time bounded areas such as nuclear plants, chemical factories, etc.
4. Breach of Service: The unavailability of certain, or all, services when required is known as breach of service. DOS (Denial of Service) and DDOS (Distributed Denial of Service) attacks are the best representation of service breaches. In operating systems, service thefts can be used to deprive resources to genuine requests. This is done by generating forced deadlocks, changing system registry details and even in some cases, disabling of the particular hardware (speaker, microphone, camera in most cases) and then using them for unethical purposes. DOS attacks are service requests from same source infinite number of times. It can be tracked and stopped eventually. DDOS attacks are more dangerous as the source demanding resources and services changes after every request. Tracking down the main source of the chain of sources is very difficult and, in most cases, permanent shut down is the only option left.

4. WORMS

A worm is a process that uses fork/spawn process to make copies of itself. It can produce multiple copies of itself without the need of human intervention and doesn't even need a host program to attach itself. Worms take advantage of non-alert users. They can enter the systems through software vulnerabilities, attachments in emails, fake SMSs, fake MMSs, fishing sites, etc. Once clicked or downloaded, they redirect to the place where the worm is waiting to enter the system. Since the redirecting program has the required read/write permissions, the worm has no issues getting inside acting as 'genuine'.

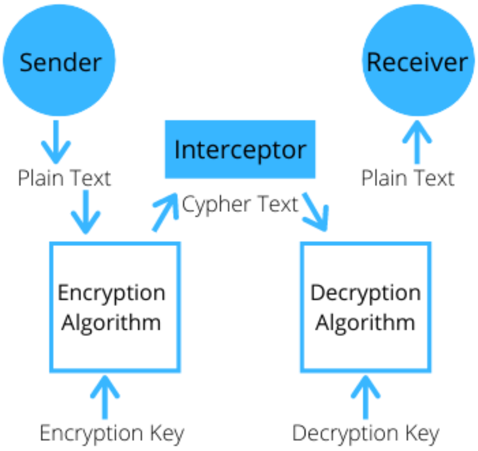
Worms can delete, modify, edit and create files on the hard disk, external storage drives and also the system registers. They consume system resources, block other processes essentially gaining the highest priority and then start multiplying in numbers. Exactly like real worms. Some worms can also propagate over network and 'eat' bandwidth in all ways possible. Generally, it is done by downloading some tool which helps to locate and upload important files to the creator's server and steal information in the background, without the user having any knowledge of this.

In Linux computers, *rsh* (remote shell) command is executed by the worm to access one computer's data from another computer, with the later acting as a host. This is dangerous because it can be done without the requirement of any password if both the computers have the same account in use. Another important command frequently executed by worms is *sendmail* command. It is used for routinely sending and forwarding emails to self, executing them and delete them to erase all traces and at the same time generate '3n' processes in every iteration (where n worms are executing the sendmail command).

5. ENCRYPTION

The best solution (till date) to protecting data is to encrypt it. Even if the most secure system is built such that no malware, virus or worm can enter, after a few days/weeks, it falls behind, and some new variation succeeds in getting into the systems. So, accepting that the system will be breached, and data is going to be stolen, modified and deleted; there needs to be a new type of protection that will not protect the system, but the data present in the system. This type of data-oriented security is known as encryption. Encryption is the process of encoding data in such a way that only the program/people with the knowledge of decrypting can access it.

The process of encryption is fairly simple, at software level. Once things move on to hardware level encryption (which is discussed later in the text), it starts becoming quite complex in terms of recovering data in emergency. But more on hardware encryption later. The following diagram explains the entire process.



The process of encryption can be categorised into 2 parts, Symmetric and Asymmetric Encryption. A detailed explanation of how they work is given as follows.

1. Symmetric Encryption: In symmetric encryption, the key which was used for encryption, is used for decryption. Therefore, the key has to be kept secret to as to avoid data loss and other potential risks. Some of the most commonly used symmetric encryption algorithms are:

   a. Data Encryption Standard (DES): In DES, the message is first broken down into 64-bit chunks and the chunks are rearranged in a specific manner so as to break the continuity of the data. It is then encrypted with a 56-bit key, making the effective encoding bit size of 128-bits. Same key is used for decryption and algorithm used to rearrange chunks is applied again to regain the original data.
   b. Triple DES: TDES, or Triple DES, is an improvement to DES algorithm. The difference between DES and Triple DES algorithms is that there is 1 encryption and 1 decryption process in DES. While in Triple DES, there are 2 encryption and 1 decryption stages, making total of 3 stages. Hence, the name Triple DES. The effective length of encrypted data chunks after 2 encryption stages is 168-bit. Triple DES was introduced after DES algorithm failed to protect data from powerful brute-force attacks. Even before Triple DES showed signs of weakness, a more advanced algorithm was made.
   c. Advanced Encryption Standard (AES): Similar process as that of Triple DES, but instead of 2, 10 to 14 rounds of encryption take place, making the effective encrypted data secure to a remarkably high extent. Depending on the type, size and continuity of data, variable encryption key length of 128, 192 and 256-bits was used. And that variation for every chunk of data. Thus, the entire process of encryption (as well as decryption) time consuming if the size of data to be encrypted was high.
   d. Other popular encryption algorithms are Twofish, RC5 and RC4 algorithms.
2. Asymmetric Encryption: The main difference between symmetric and asymmetric encryption is that in asymmetric encryption the key which is used for decryption is not the same as the one used for encryption. Thus, the algorithm has to generate 2 different keys (and arguably 2 different algorithms) for both the processes. This makes asymmetric encryption computationally more expensive as compared to symmetric encryption. It is feasible only for small scale data protection, such as passwords and OTPs, and also CD-keys, product keys, etc. One of the most commonly used asymmetric encryption algorithm is RSA algorithm.

6. BitLocker

BitLocker is a hardware level encryption technology implemented at sub-system level. It protects the computer from unwanted malware and trojans by scanning and encrypting data before starting and shutting down the machine. This ensures the system is secure before permanently applying changes (after shutting down) and the changes made are still secure to use.

BitLocker encrypts all the contents of the Operating System partition and a special BitLocker key is generated when BitLocker is activated and is required to access the contents of the encrypted volume. This is a 2-stage process in reality. The BitLocker key shared with the user is just to confirm the authenticity of 'user' and not data integrity. For the verification of data integrity and completeness, a special 256-bit TPM (Trusted Platform Module) generated key is used for the purpose.

Another important feature of BitLocker is that if a complete drive is selected for encryption, and somebody physically removes the drive and puts it into another computer then the person cannot access any of the data from the stolen drive. This is because BitLocker actually encrypts the sectors on the drive making it impossible to recover data if the drive has been put into another computer or there has been an attempt to retrieve data without BitLocker key and TPM key. BitLocker has 2 requirements at software and hardware level.

1. Software: One needs to have the 'Pro', or, 'Enterprise' version of Windows Operating System, valid from version Windows XP through Windows 10. This is particularly because some disk management, data partition and data security Kernel files (which are used for corporate purposes mostly) are included only with Pro version and not the Home version (although there are third party solutions to overcome this barrier, but in-house security is always preferable to anything else). Since BitLocker is a Microsoft technology, it is not available on other operating systems.
2. Hardware: BitLocker requires TPM chip (Trusted Platform Module) to be present inside system for encryption. This is because TPM generates a 256-bit key, which is crucial for checking data integrity as well as for accelerating the process of encryption-decryption. TPM chip takes-off 95% of the CPU load which helps to boot system safely and at the same time, stay fast (because CPU can freely execute next processes in line). Since 2018, Intel ships TPM chips along with its processors using SoC technology. Therefore, if user has a machine purchased after 2018, he/she already has sufficed the hardware requirement for using BitLocker.

When a potential threat is detected (by Windows Defender), or, it is a scheduled scan, system performs what is generally called as SIC, System Integrity Check. This scans each and every bit of data, including BIOS, using TPM chip as a key-generating-reference. If TPM key value changes at the end, system is at risk; and safe otherwise. SIC follows the following path, in brief.

1. TPM examines the start-up files of encrypted and unencrypted partition, with encrypted partition requiring BitLocker key for reading and scanning.
2. TPM generates a system identifier key based on the components of the system.
3. After data scanning, a new identifier key is generated based on those components.
4. The 2 keys are matched with one another.

System boots like normal if the keys match. Gives error otherwise. (System goes into recovery mode in this case. But further actions are determined by manufacturer)

7. CONCLUSIONS

There are thousands of viruses getting detected, antiviruses are being made for them and the illusion of world is becoming a safer place is becoming more profound. But it would be unwise to not consider the hundreds of new viruses being made to trouble user, create nuisance and misuse data every single day. And the number is going to rise if the masses do not protect themselves against these digital threats.

Advanced solutions like BitLocker are required for more devices. Similarly, more advanced security standards, like biometrics, etc. should be made available to kids devices, public usage service devices (like ATM machine, banking counters at railway stations and bus stands, etc.) so that data leaks should be restricted to personal, low content and adult usage data and not minors' and mass scale amounts as mentioned above. This will take time, but with the ongoing level of research and development, it won't be wrong to say the number of protections available will surely be higher than rate of rise of new threats.

REFERENCES

[1] Gaurav Sharma, Ashish Kumar, Vandana Sharma, "Windows Operating System Vulnerabilities", International Journal of Computing and Corporate Research, November 2011, Vol – 1, Issue – 3

[2] Wesam S. Bhaya, Mehdi Ebadi Manna, "DDoS Attack Detection Approach using an Efficient Cluster Analysis in Large Data Scale", Proceedings of Annual Conference of New Trends in Information & Communications Technology Applications (NTICT-2017)

[3] Sven Turpe, Andreas Poller, Jan Steffan, Jan-Peter Stotz, Jan Trukenmuller, "Attacking the Bitlocker Boot Process", Fraunhofer Institute for Secure Information

Technology (SIT), Rheinstrasse 75, 64295 Darmstadt, Germany

[4] Himanshu Raj, Stefan Saroiu, Alec Wolman, Ronald Aigner, Jeremiah Cox, Paul England, Chris Fenner, Kinshuman Kinshumann, Jork Loeser, Dennis Mattoon, Magnus Nystrom, David Robinson, Rob Spiger, Stefan Thom, David Wooten, "fTPM: A Firmware-based TPM 2.0 Implementation", Microsoft Research, MSR-TR-2015-84

[5] Felix Schuster, Thorsten Holz, "Towards Reducing the Attack Surface of Software Backdoors", Horst Görtz Institute for IT-Security Ruhr-University Bochum, Germany

[6] Shohreh Hosseinzadeh, Bernardo Sequeiros, Pedro R. M. Inácio, Ville Leppänen, "Recent trends in applying TPM to cloud computing", Security and Privacy. 2020;3:e93. https://doi.org/10.1002/spy2.93

[7] Victor Costan, Srinivas Devadas, "Intel SGX Explained", Computer Science and Artificial Intelligence Laboratory Massachusetts Institute of Technology