Security

Table of Contents

1. The Core Security Mechanism for Windows

In recent days, we can see many customers or friends extremely worried about the security hazards towards their personal information through media. It is all because of the improper protection of information in the organizations. Data security applies four requirements - confidentiality, integrity, availability and authenticity - to ensure data is secure from offenders (Gollmann, 2011).

The members of cybercrime (Schultz, 2004) take much effort to prevent the threats or crimes. However, some hackers find new ways to gain control of some organizations' private data. Hence this causes many loss and risks to the organization. They suffer in recollecting the data from the backups; it can also affect the organisation trust and so. In this assignment, we are going to see the scenario in which the information regarding the Microsoft word files were harmed by the attackers. Therefore, in this assignment we are going to see the already available security architecture of the Microsoft organization and we are going to see the security mechanisms and services that are handled by the organization. Moreover, the security process handled by this organization is found to be easily accessible to any kind of malicious attacks. It is found that the attacker have an unauthorised account on the system. The mechanisms that are used by the organization to control the access of the unauthorised user are not up to the level. Thus, the organization needs to adopt an approach to fulfil the activities of the security issues and its services.

2. Functions of Access Control Mechanisms

Security is considered as a very important component of current operating system. Thus, the access control mechanism (Rudra and Vyas, 2015) helps to provide security. Mainly, it focuses on expressing an important portion of security in operating system. It not only helps to access the files, but also allows only the secured users to do certain functions in the system (Gollmann, 2011). Therefore, all the Windows operating system especially Windows 9x system makes use of this access control. Hence two various approaches were used to monitor access in the windows operating system.

2.1 Common-level access monitoring

This access control offers an easy method for allocating the resources. In this method, we can share the resources for Read-Only Access or Full Access (Yadav and Shah, 2015).

2.2 User-level access monitoring

This access control secures the allocated network resources by allowing only the authenticated user's request to access system. The security holder (Yadav and Shah, 2015) grants authorization only to the known users by validating the user name and passwords as those on the records of the user account which is saved on the internet security provider.

3. Low-Level Safety Mechanisms

3.1 Virtualization-based security

It is the primary standards for all the security in operating systems. The virtual based security makes use of hardware as well as software imposed mechanisms in order to generate a confined, secured and functional subsystem (HONG, 2006). This subsystem is created for protecting, reserving, performing and delivering other precise subsystems and data's. Certain portions of the operating systems can be altered with the help of this virtual based security system. Thus, the virtual based security (SENGUPTA, Mohanty and Bhadauria, 2016) becomes more secure and guides integrity application in windows operating system.

3.2 Safe booting

All the windows operating system is begun with safe booting mechanism (Rajendra Mudiraj, 2013). The booting process makes use of Bit Locker (Turpe et al., n.d.) and the Trust Platform Module chip to preserve the boot process. The windows 7 operating system comes out as a Unified Extensible Firmware Interface. It retrieves the highly conventional method BIOS. So, the Windows OS and Unified Extensible Firmware Interface (UEFI) combined worked together to make sure that it prevents the hardware and low level operating system from unauthorized access (HONG, 2006).

3.3 Windows Hello

It is the method experimented by the Windows 10 OS to avoid reuse of the stolen passwords. This method mainly focuses on the biometric authentication (Mudholkar, 2012). It then supports to gather the iris, finger print and facial impressions in agreement with a PIN. These impressions are detected by the devices for authentication of users and to prevent the arrival of hackers.

3.4 Passport

Microsoft passport is an innovative single-sign-on resolution (Pashalidis and J. Mitchell, 2013). It helps the windows OS to securely restore the asymmetric key of the software used in the OS in order to protect the software from hacker.

3.5 Authorization Guard

The Windows 10 authorization guard (Schultz, 2004) is implemented to prevent the harsh attacks. It preserves the Windows authentication expert and user derived authority from disconnecting the authentication service and by preserving the NTLM authenticated data in the virtual based security. Thus, the Virtual based security completely avoids the internet based attacks.

3.6 System Guard

It is a high protective component that describes which data's and applications should be permitted to operate on a specific computer. It utilizes the hardware control of Virtualization-Based Security (VBS) to preserve the integral information on a Windows OS (Wojtczuk, 2016).

3.7 Enterprise Data security

Normally the Bit Locker preserves our data whenever the device is hidden or stolen (Raj et al., 2015). Apart from this the advanced application for security is developed by Windows OS. It is called Enterprise Data security. It offers constant file-level encryption and essential rights to corporate files. Hence the Windows OS acts as an agent to preserve the data based on the defined policies. Therefore, the Enterprise Data security is excellent at recognizing, isolating and preserving corporate data.

4. Failure of Outlined Security Mechanisms

4.1 The Present Architecture of Security Mechanisms

Many organizations have doubt that whether they invest their security dollars in the correct areas because of the occurrence of data breaches. The recent strategic report says that more than 90 precent of the organizations in data are stimulated by the data exfiltration for the purpose of material gain or allied spying (Hayday, 1999). So many organization have a query that why we are proposing so much force in preserving the network perimeter instead

of securing the data from the hackers or allowing the information to be altered by the hackers. So, by investigating the current data gaps, it is clear that we have arrived a bend point in which it required a different approach for the information security. So, the new information security approach may focus on preserving the information by its own and also from the chaotic. Hence the Microsoft Company spends large amount of money to control a security perimeter every year. The security perimeter is constructed to reject the cyber-attacks or insider attacks. Since the security perimeter is losing their battle, most of the expenses are focused to maintain traditional protection system of security perimeter. The cyber-attack on the Microsoft word is a good example for this issue (Schultz, 2004). Certainly, the private data's are the important target for the attackers or hackers. Hackers have the ability to abstract highly delicate data's in spite of all the security elements placed in the systems.

Therefore, if we preserve the data disappearing from the organization or if the data's are being altered, the security over the network gaps becomes undemand able. So, the data's will not be made used for the further process in the organization. Finally, the data is kept unsecured. Many examples reveals that the organizations where unsuccessful in preserving the integrity of their data. As we search for data breaches or any information regarding the unencrypted data in the Internet. The web provides thousands and thousands of conclusions that explains the organizational failure in securing the integrity of their information and they do not encrypt the delicate information (Schultz, 2004).

5. Characteristics of OSI Security Architecture

The security framework (Stergiou, Leeson and Green, 2004) is defined as design artefacts in which it illustrates how the safety is arranged in the organization and how they are interconnected with the overall system plan. Thus, the controls present in the security architecture helps to protect the quality features of the systems like Integrity, availability and confidentiality (Patel, 1994; Gollmann, 2011). In this research paper, we are going to implement the modified security architecture called OSI privacy architecture. This OSI security architecture (Patel, 1994) improves the productivity of data processing systems and data transfers of an organization. It is mainly proposed to prohibit the security attacks. Hence this security architecture makes use of one or more security methods. This method often reproduces the functions which are usually combined with the physical records. The most important security service offered by the OSI security architecture is x.800.This x.800 service is constructed by the protocol layer for broadcasting the open system. It also helps in ensuring

the presence of sufficient security to the devices or networks (Patel, 1994). The other important services offered by the x.800 are confidentiality of data, data honesty, availability, authorization, non-repudiation, digital signatures, routing control and traffic padding to secure the information from attackers. Thus, these services make the attackers to loss the control of the windows administrator access (Stergiou, Leeson and Green, 2004).

6. Limitations of OSI Security Architecture

The main disadvantages of the OSI security mechanism is due to increasing the additional layers of authority (Information Security: Challenges and Solutions, n.d.) So, it restricts the usability of the security services. At times the security services will face the arguments on the additional security controls. So that these control will delays the functioning of the controls thus making it difficult for the users to access. Due to its complications, the OSI standards have to go away from the technical points such as coding and security (Price, 2008).

7. References

Gollmann, Dieter. 2011. Computer security. 3rd ed. Chichester;Chichester, West Sussex;: Wiley.

Hayday, J. (1999). Windows NT security architecture. Information Security Technical Report, 4, pp.17-18.

Information Security: Challenges and Solutions. (n.d.). [online] Available at: http://www.peterindia.net/ITSecurityView.html.

Mudholkar, S. (2012). Biometrics Authentication Technique for Intrusion Detection Systems Using Fingerprint Recognition. IJCSEIT, 2(1), pp.57-65.

Pashalidis, A. and J. Mitchell, C. (2013). A Taxonomy of Single Sign-On System. [online] Available at: https://www.researchgate.net/publication/2927769_A_Taxonomy_of_Single_Sign-On_Systems.

Price, G. (2008). The benefits and drawbacks of using electronic identities. Information Security Technical Report, 13(2), pp.95-103.

Rajendra Mudiraj, A. (2013). Windows Linux and Mac Operating system Booting Process: aComparative Study. International Journal of Research in Computer andCommunication Technology, 2(11).

Raj, H., Saroiu, S., Wolman, A., Aigner, R., Cox, J., England, P., Fenner, C., Kinshumann, K., Loeser, J., Mattoon, D., Nystrom, M., Robinson, D., Spiger, R., Thom, S. and Wooten, D. (2015). fTPM: A Firmware-based TPM 2.0 Implementation. Microsoft Research. [online] Available at: http://ssaroiu.azurewebsites.net/publications/tr/msr/msr-tr-2015-84.pdf.

Schultz, E. (2004). Windows 2000 security. Network Security, 2004(1), pp.6-9.

SENGUPTA, A., Mohanty, S. and Bhadauria, S. (2016). Low Cost Security Aware High Level Synthesis Methodology. IET Computers & Digital Techniques.

Stergiou, T., Leeson, M. and Green, R. (2004). An alternative architectural framework to the OSI security model. Computers & Security, 23(2), pp.137-153.

Turpe, S., Poller, A., Steffan, J., Stotz, J. and Trukenmuller, J. (n.d.). Attacking the BitLocker Boot Process. [online] Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.149.5116&rep=rep1&type=pdf.

Wojtczuk, R. (2016). ANALYSIS OF THE ATTACK SURFACE OF WINDOWS 10 VIRTUALIZATION-BASED SECURITY. [online] Available at: https://www.bromium.com/sites/default/files/us-16-wojtczuk-analysis-of-the-attack-surface-of-windows-10-virtualization-based-security-wp-v2.pdf.

Yadav, A. and Shah, R. (2015). Review on Database Access Control Mechanisms and Models. International Journal of Computer Applications, 120(18), pp.21-24.