Defense in Depth: Multilayer of Security

Raed Alsaqour[1*], Ahmed Majrashi[1], Mohammed Alreedi[1], Khalid Alomar[1], Maha Abdelhaq[2]

[1]Department of Information Technology, College of Computing and Informatics, Saudi Electronic University, 93499 Riyadh, Saudi Arabia.
[2]Department of Information Technology, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, 84428 Riyadh, Saudi Arabia.

Abstract: Many types and methodologies of attacks have been developed to target the victims in different ways affecting their resources and assets. This paper reviews the defense in depth concept that has been developed in which multilayer of security controls are implemented to protect resources and assets from such attackers through consuming all the resources and capabilities of the attacker before malicious activities affect such targeted resources and assets.

***Keywords*:** Defense in depth; Multilayer of security; CIA model; Security control

1. Introduction

Security threats become the major concern for every user, security administrators, and even the management level of any organization since the number of attacking activities are in a repaid manner due to different motivation aspects such as financial gain, policies motivation, or personal gain [1] [2].

Defense in depth means placing a multi-layer of security defense where diverse strategies and controls are implemented and deployed to mitigate multiple kinds of risks could organization faced. The operation of defense in depth or multi-layer of security controls is based on if once layer is failed to perform the necessary protection the other layer would perform the required protection to achieve the overall necessary protection for the organization resource and [3].

while the number of attacking activities is increased and they can spread through taking advantage of the internet network, it is reasonably unsafe for a local network to connect the internet without placing appropriate security measures used to protect such local network [4].

The need for modern technologies and networking devices is increased since they provide effective and efficient means of performing daily business tasks due to fast processing capabilities and quick data transmission. The problem with such enhancement, attacking surface and vulnerabilities exist are increased which allow such attackers to break into the network or system in such unauthorized manner. For that reason, security measures and models need to be implemented to protect such attacking activities which could affect the operation of new technologies and networking devices.

As shown in Figure 1, for any security model and defense, the primary objective is to provide three concepts or goals that are confidentiality, integrity, and availability. The three concepts compose the CIA model which the objective for any security model and measure.

CIA model is used as a baseline for any security measures to protect the confidentiality, integrity, and availability of hardware, software, computing devices, network devices, and other assets that consider valuable resources for users and organization to conduct the necessary computing operation without any fear of unauthorized access, compromising and modification of resources and data that is used in an unauthorized manner, and interruption or delay of requests for resources or data that are required to perform a certain and specific operation.

It is the security measure where there is confidence for the user about the sensitive data privacy where there is a prevention mechanism that prevents an unauthorized user from disclosing such sensitive and private data where the access to such data could be done only in the authorized manner [5, 6]. Data confidentiality could be achieved by various techniques and mechanisms such as encryption and access control.

Data integrity means protecting the data from any method of modification or changing that could be performed on the data in an unauthorized manner and such modification is allowable to the authorized user [5, 7]. Data integrity mechanism is used to prevent cybercriminals from altering and interfering with data while processing, storing, and even transmitting data through implementing different techniques and algorithms.

The data availability concept is used to prevent any methodology that could be used to block the legitimate and authorized user from using and accessing the information and resources that are acceptable to be used by authorized users [5, 8].

Denial of Service (DoS) attack is an example of an attack that could affect the availability of resources and information where the attack functionality is based on blocking the legitimate and authorized users from access such resources and information where thus affect the availability [9].

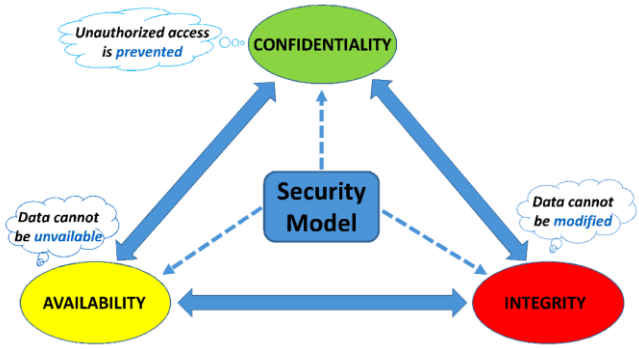

Figure 1. CIA model [5]

2. Defense in depth

The concept for the defense in depth is coming from the military sector where such defense mechanism is applied through implementing multiple and different defense measures to prevent all attacking resources and capabilities from successfully adopt or accomplish the attack where different lines of defense are used [3]. In information security, the concept is used as in the military sector where multilayer of security and defense are implemented in such a way that are

* *Corresponding Author*

would prevent attackers from attacking the organization resources, network, network, and assets from unauthorized access or any compromising activities that could be made in an unauthorized manner since the feature of adding multiple layers are an effective method for protection securing organizations' hardware, software, network, computing devices, and assets through overcoming any shortcuts or weaknesses that could result from implementing a single layer of defense where it could be quite easier for the attacker to target and hit the organization with one layer of defense than another organization who implement different security layers and defenses against such attackers [10].

Implementing a well-defined defense of layers would produce a strong level of security as well as an appropriate strategy and configuration mechanism made to these security layers since different software and hardware of security are being used to make them incorporate together and work as a single unit of defense with multiple features of protection methodology. Implantation of a well-defined defense in depth strategy would be effective and efficient for preventing a wide diverse range of attacking methodology and activity with an additional feature which is a real-time alerting for security administrators about any security incident or attack which consider an effective method for mitigation and elimination since the action is taking before the attack is getting diverse into the target organization and getting worse [10].

Defense in depth or multilayer of security covers a wide variety of attacking techniques and methodologies since different protection methods are used which introduce additional features regarding the protection mechanism. The defense in depth could be effective in protecting against an automated attack which could be performed by an attacker targeting an organization. Such an attack is performed automatically where the attacker is exploiting the organization resources and asset in such a real-time environment through using different techniques and tools for attacking activities which are quite harder to be prevented if only one single layer of defense is present whereas the implantation of multilayer of security or defense in depth security measure could be able to prevent such attack if a proper configuration was made [3, 10].

The concept of defense in depth is quite hard to be implemented since the different layers of security are needed to achieve the desired concept and heterogeneous properties for each layer which could result in overhead during administration tasks. Necessary skill, education, and enough experience are required to implement these different layers inappropriate way and functioning as planned and required without introducing any security threats or vulnerabilities to the organization. Improper implementation and configuration could lead to a massive loss for the organization since new security holes and vulnerabilities could be introduced which allow the attacker to compromise the system, hardware, software, and network in such an easy way rather than make it harder to accomplish such attacking activities [10].

As a result, the process for implementing such depth in defense strategy quite heavily processes and task unless the necessary skill is present, a level of education, and enough experience are available which all work together to provide comprehensive implantation of defense in depth strategy and plan. After the implantation is conducted successfully, maintaining and mentoring the functionality of each layer of security is considered a hard task to be performed, and proper management and maintenance should be present, otherwise security threats could result from such a layer of defense instead of providing a mechanism for protection.

Since every layer of defense is different from another layer, each layer has its management and administration process that is different from other layers which thus increases the administration overhead if such an inappropriate maintaining process is taking place. New security vulnerabilities and holes could be introduced and exploited by attackers if no such administrating roles are performed and done properly which resulting in security threats that could affect the organization's business process and generate a massive loss more than expected rather than providing effective means of protection against attacking activities. Defense in depth is considered a more flexible technique for protection if the appropriate implementation is performed and proper maintaining is achieved since it could prevent the new emerging threats and enhance the environment for protection against most threats that could be faced by the organization.

2.1 Defense in depth component

Since the concept of defense in depth means implementing and deploying multilayer of security, different components and elements are gathered together to form and achieve the concept of defense in depth. Figure 2 shows the model for defense in depth:

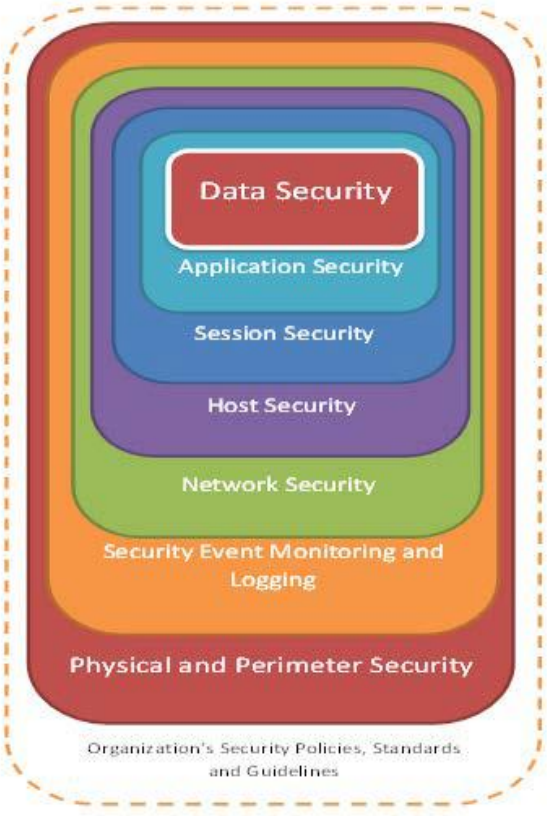

Figure 2. model for defense in depth [3]

The model describes the different components of the defense in depth since different approaches for security are forming the concept of defense in depth. Below is the list of different components.

- Policies and procedures for security
- Physical and perimeter security
- Network security
- Monitoring and logging event

- Host security
- Session security
- Application security
- Security for data

2.1.1 Policies and procedures for security

Before any deployment of any security measure, the security policies and procedures should be first identified and generated to control and guide the internal and external behavior of the users whether such acts are acceptable or unacceptable within the organization's facilities and resources. Policies and procedures are considered one of the important layers of security since such security control can identify the internal security threat. Policies and procedures could be used at different levels of abstraction such as a high-level policy that is used to describe the acceptable and unacceptable behavior regarding assets usage as well as the acceptable and unacceptable assets [11].

Low-level policies are used to describe the required and desirable behavior of general employees within working hours or toward organization information and assets [11]. Policies and procedures need to be first identified before other security controls and measures, since such policies and procedures control directly or indirectly the implementation and deployment of the other security controls which help to reduce the number of modification and updating whether the policies or the security measure to satisfy and fit the security need which thus generates overhead working time that could be reduced from such losing time [11, 12].

Figure 3 describes those policies are used to explain and describe the behavior within a specific organization or situation while standards are developed by international organizations to specify the specific behavior regarding the general situation that needs to kind of uniformity among different organizations. Guidelines and procedures are considered the baseline for policies where such recommendation are developed to help organizations to create their policies based on their needs and the configuration could be made on such guidelines and procedures to create and formality a specified own policy for specified organization that would eventually fulfill the necessary security needs and objectives of the organization.

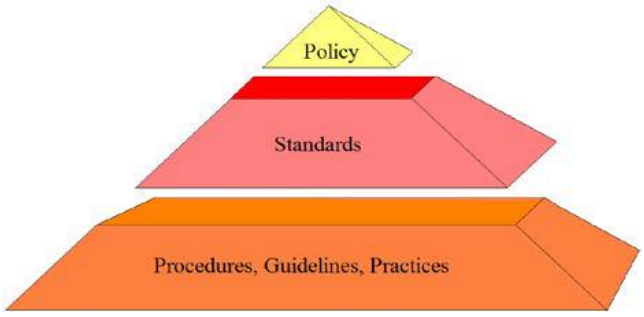

Figure 3. Policy, standards, procedures, guidelines, and practices [3]

2.1.2 Physical security

Physical security is considered one of the important safeguards and protection needed for all organizations. The physical security plan should cover technologies, devices, and materials that use for internal, external, and boundary protection functions such as sensors, monitoring devices, cameras, access control devices, and other assets that could be targeted physically by attackers or intruders [13].

2.1.3 Security of the network

Networking in today's business is an essential part of every organization due to its effectiveness in the way that the business is running. Many attacking activities could be generated and targeting the organization through outside network technologies since the network provides efficient means of delivering attacking activities remotely without physical attendance. As a result, organizations should protect their internal network from any threats and malicious activities that could come from outside networks. To provide an effective way of protection, an understanding of network design is essential to determine where should the protection device is installed and how to determine its functionality to achieve the required and objective level of protection. Figure 4 explains how a typical firewall could be implemented to act as a gateway for incoming and outgoing packets traffic and how the filtration process is performed as well as the appropriate positioning for the firewalls to perform the necessary function of security as required and planned for installation.

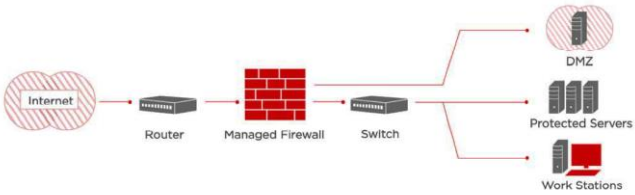

Figure 4. Firewalls implementation [5]

Firewalls working mechanism is based on filtering process where the filtration process relay on rules that are identified and predefined by network administrators in which every packet that passes through the firewall whether incoming packet or outgoing packet is examined and such packets are tested to allow or block the examinee's packet from passing through the firewall in which the examination process is done based on predefined rules and if satisfaction is achieved through meeting all the defined rules the packet is allowed to pass the firewall otherwise, the packet would be not allowed to pass the firewall and thus blocked [14]. The functionality of the firewall should be first test and assess before actual implantation is executed to ensure that the firewall is carrying out its necessary functionality as objective and planed without any errors and misconfiguration which could leave behind some vulnerabilities that might be exploited by an attacker and generate some threat to the organization resources and assets [14]. Installation of firewalls could be at the perimeter of the internal network to isolate the external or untrusted network from the internal network. Additional network hardware or software is Intrusion Detection Prevention Systems where are used to detect and prevent abnormal activities and behavior within the network [15]. Figure 5 shows the typical IDPS deployment within the network.

An example of security measures used to protect the network is Intrusion Detection Prevention Systems. Software, hardware or both could compose the IDPS in which the functionality is based on the examination process for the passing packets. If such suspicious activities are present on the network, and alerting report is generated to alert the network administrators about threatening activities. Whereas the Intrusion Prevention Systems are used to immediately prevent a detected threat where the passing packet traffic through IPS

is examined to decide if the packet is eligible to pass through the secure network or not [4].

IDPS functionality is performed in two ways that are anomaly-based and signature-based. Anomaly-Based detection is carried out by comparing the behavior of the captured event with a set of rules that determine the acceptable situation of such event with threaten situation and alert the administrators of such abnormal event. Whereas signature-based detection is performed through recognizing specific patterns of captured event or packet which has a potential threat to the network and such event or packet is associated along with specific attacking activities [4].

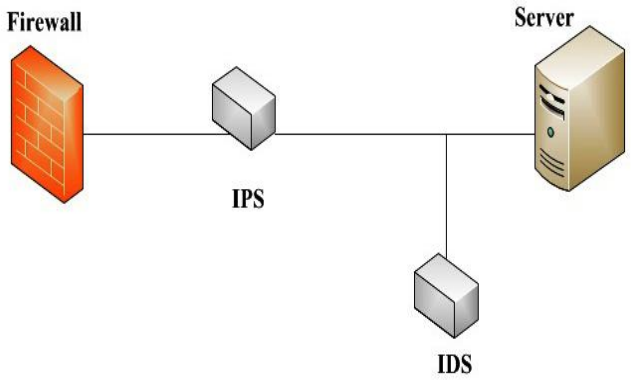

Figure 5. IDPS deployment [15]

Network-Based IDPS operates based on input gathering that is performed through capturing data by monitoring network traffic such as the packet is captured by network interfaces that are in promiscuous mode whereas Host-Based IDPS is implemented in the software where it exists at the top of the operating system and the operation depends on collected events that are captured by hosts that they monitor where the examination process is performed on the behavior of the internal host [4].

2.1.4 Monitoring and logging event

Tracking all activities of the network is important to eliminate any potential threat at the beginning phase before it is becoming worse and hard to be eliminated as well as the ability to perform root cause analysis to avoid such threat in the future with appropriate planning and security tools and measures enhancement as well as accomplishment. Continuous monitoring for the network activities should be carried out to cover all activities. Intrusion Detection Prevention Systems could be used as logging event activities where such alarm is generated to administrators once abnormal behavior is detected to help administrators to respond to such behavior as soon as possible in a very effective and short time manner which thus reduce the negative consequences on the organization or the network or even cause nothing [4]. A daily inspection should be performed by administrators or security personnel to keep up monitoring network activities on such a daily basis where such threat could be eliminated in advance before it is getting harder to recover or eliminate from the system or network and getting worse [16].

2.1.5 Host security

Security for every workstation is a crucial aspect where each host is protected as an individual to increase the level of security to a desirable level. Multiple techniques and tools are implemented for each host to increase its security level. Figure 6 shows how the process of implementing defense in depth of a host through placing a multilayer of security tools and techniques to increase the level of defense against such attack. Attackers would find out that, breaking into a host is quite harder since multiline of defense are placed to struggle such attack through consuming all resources and capabilities of the attacker to prevent such attack from successfully harm the target with such malicious activities.

Such tools and techniques that could be used are Anti-viruses and Anti-malware, firewalls that are placed for the individual host, Intrusion Detection and Prevention systems specialized for a specific host and hardening process for the operating system of the host through implementing various techniques and tools. Host security is so important as the security of the network where the objective of placing multiple layers of security is to achieve the concept of defense in depth where the purpose of implementing such concept is to consume all resources and capabilities of the attacker before the actual attack is successfully taking place and harming the resources and assets of the targeted organization which thus the attack is prevented.

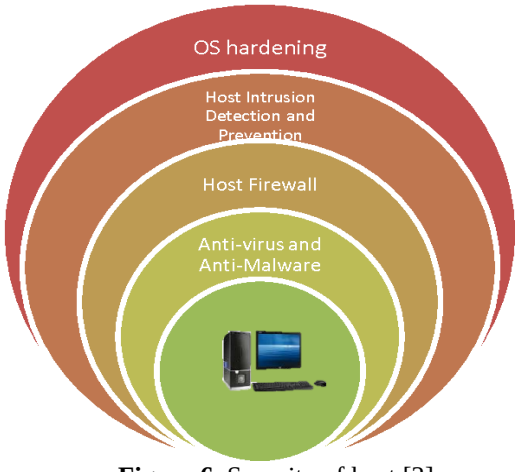

Figure 6. Security of host [3]

2.1.6 Session security

Security of session is a mandatory task since the session is used be between the client and the server to establish the connection between them. Attackers usually hijack such legitimate users' sessions to bypass the access control mechanism to get unauthorized access in such a way that could be in an authorized manner since legitimate session ID has been used. Attackers could use various techniques and methodologies to hijack sessions of the authorized user by for example sniffing methods where the attacker is monitoring the passing packet through the network to figure out the content of such packet and the containing information regarding session such as session ID to be used for access mechanism to make such access to appear as legitimate access [4]. Cross-site scripting is one of the techniques could be used where an attacker injects malicious codes into the website application or web system by using JavaScript, ActiveX, and HyperText Markup Language to expose session credential once the legitimate user access to such infected website or application [17].

Brute-force could be one of the methods used to hijack the session by trying all the possibilities of usernames, passwords, unique characters, symbols to crack such login credential or session credential where could be used later time for making unauthorized access to be done in an authorized manner [18]. To prevent such attack from taking place, secure communication channel should be used such as HTTPS that deploy a secure protocol for data transmissions such as Secure

Socket Layer / Transport Layer Security where such encryption algorithms are used to prevent an attacker from hijacking the legitimate session as well as implementing a technique that used to calculate hash digest before granting access to a legitimate user's session where the server performs the necessary calculation of the hash digest for the attacker's browser details and parameter of the system in which after that a comparison is made against hash digest that already generated for session ID of the legitimate user [19, 20]. Figure 7 shows that the typical way of session hijacking attack.

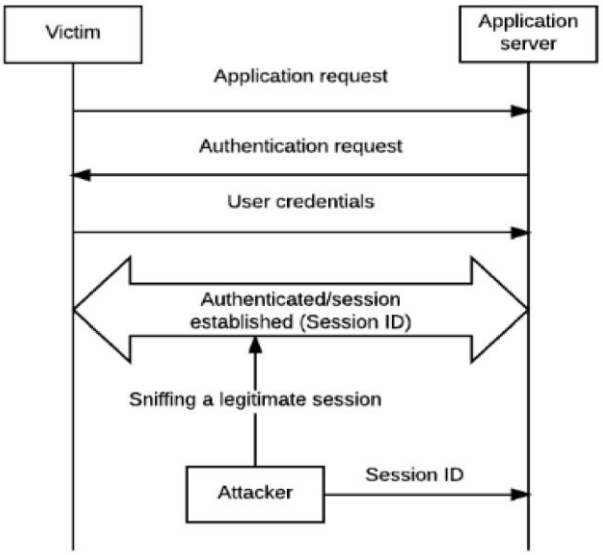

Figure 7. Session hijacking process [20]

2.1.7 Application security

Securing the application that is used within the system or network is necessary through implementing Access Control List, authentication and authorization mechanism, vulnerabilities elimination, security assessment, data backup, and restoration mechanism, and input validation to prevent any possible way of malicious code injection [15]. SQL injection and Cross-site scripting are some of the techniques and methods used by the attacker to inject such malicious codes into the web application to retrieve such confidential information. The database could be exploited by SQL injection attack whereas JavaScript, ActiveX, and HyperText Markup Language could be used to carry out the cross-site scripting attack where both are using a malicious code to compromise the application performance and process [17]. Input validation mechanism should be in place to prevent any such malicious code from executing in such a way and convert it into normal text with disabling the possibility of execution function to prevent such attack from taking place [20].

2.1.8 Security for data

Data should be secured while processing, transmission, and even at storage place to make sure that objective from security control is achieved which is confidentiality, integrity, and availability that compose the CIA model which used testify the security measure against CIA model that use as a baseline for the implemented security measure or control [5].

3. Security risk and threat assessment

Vulnerabilities and security risk assessment is considered one of the security controls since the purpose of such assessment is to identify the potential threats and vulnerabilities which could be exploited by attackers to successfully perform malicious activities and thus harm the organization's resources and assets [21]. A continuous assessment is one of the methodologies used to identify such security risks before an actual attack is taking place and the assessment should be performed regularly since new vulnerabilities and attacking techniques are continually developed and used where such assessment needs to be performed to catch up the new emerging attacking activities [21].

3.1 Advantages of defense in depth

There are some features and advantages of placing multi-layer of security controls that help the organization to protect its resource and data. Diversification where each layer is achieving a desirable and objective task regarding the mitigation of security risk. Every layer possesses its feature regarding security protection where overall layers provide full protection against multiple security risks and threats instead of placing one layer of defense.

Effective protection could be achieved since multi-features have been acquired and used which enhances the protection against any threats and risks that could affect the organization's work process [10] [3]. Placing multi-layer of security has proven that is a defended against an automated attack that could be launched by an active attacker that is intended to breakdown security controls of the organization as well as scalable and adaptable since its multilayers can address and identify new threat might attack the organization resources and data through placing new security control that used to mitigate the newly discovered threat. In addition, it could be adaptable to large, medium, and small organizations that looking for full and powerful protection [3]. Moreover, assets isolation where critical assets could be isolated and harden with powerful security control which prevents any attack from breaking such security control if it is one layer. So, the crucial assets and resources are protected against any attack with the help of multi security layers [3].

3.2 Disadvantages of defense in depth

Despite the advantages of defense-in-depth, some disadvantages need to be considered when implementing such a concept to the security controls to correctly deploy the multi-layers of security and achieve the maximum benefit from such implementation. Such drawbacks are heterogeneous implementation could be faced which affect the administrative task. So, skilled administrative personnel is necessary to be present to provide accurate implantation to achieve the maximum benefit from the multi-layer of security in addition to that, administrative tasks could possess overhead regarding the right control of the multilayers.

So. Skilled and expert personnel is necessary to be present to make each layer functions as one unit minimizing the generated overhead that could thunder the process of protection [10] [3]. Besides that, the right implementation is necessary required to achieve the maximum benefits of multilayer security features. So, the corrective implementation through addressing the necessary assets and recourses that are crucial for the organization. If such addressing is failed and security controls are not placed in a corrected manner, features and advantages of multi-layer of security would not be achieved and thus overhead could be generated which make such resources and assets vulnerable to threats [10].

Table 1. Advantages and disadvantages of defense in depth

No	Advantages of defense in depth	Disadvantages of defense in depth
1	Reduce the likelihood of a data breach.	Difficult to find the right balance between protective capabilities, cost, performance, and operational concerns.
2	Reduce the chances of the system having a single point of failure.	The three essential principles of security: confidentiality, integrity, and availability, are difficult to apply.
3	Defend against a wider range of threats.	
4	Enhance the efficiency with which valid enquiries and requests are responded to.	For most small businesses, this is a costly kind of security.
5	--	More technical concerns and challenges would emerge from increased complexity.

4. Conclusion and Recommendations

The defense in depth concept is an effective methodology for protection since multi-layers of security have been implemented and that is the purpose of the defense in depth. In defense in depth, all layers are corporate with each other to produce an overall security control that aims to consume all the resources and capabilities of the attacker before the attack is successfully take place and harm the target.

As a recommendation, while designing our network system, we should include security processes that give many layers of protection against potential Internet security threats, which can occur at many levels. Take a multilayered approach to building your Internet security strategy to ensure that an attacker who gets past one layer of defense is stopped by the next. We recommend that your security method secure the following layers of the traditional network computing model. Security should be planned at all levels, from the system level through the transaction level.

System level security

Your system security procedures are your final line of defense in the case of an Internet-based security incident. Therefore, configuring basic system security should be the first step in establishing a complete Internet security plan.

Network level security

Network security methods defend the i5/OS operating system and other network systems. Make sure you have suitable network-level security procedures in place before connecting your network to the Internet to protect your internal network resources from unauthorized access and incursion. The usage of a firewall is the most common approach of network protection. Your Internet service provider (ISP) can assist you with network security. Your network security plan should include the security protections offered by your ISP, such as filtering rules for the ISP router connection and public Domain Name System (DNS) protections.

Application-level security

Application-level security restrictions limit users' ability to interact with specific applications. In general, you should set up security settings for each application you use. However, you should pay close attention to the security of the apps and services that you will use or provide over the Internet. These apps and services might be used by unauthorized users looking for a backdoor into your network systems. The security measures you pick must handle both server-side and client-side security vulnerabilities.

Transmission level security

At the transmission level, security methods secure data communications inside and across networks. When connecting over an untrusted network like the Internet, you have no control over how your communication is routed from source to destination. Your data and traffic are routed via several systems over which you have no control. Anyone can see and utilize the info you have transmitted. Your data is protected while it moves between security levels due to security features at the transmission level.

While developing your overall Internet security strategy, you should construct a security plan for each layer independently. You should also detail how each set of techniques will work together to provide a comprehensive security safety net for your organization.

5. Acknowledgment

This research was funded by the Deanship of Scientific Research at Princess Nourah bint Abdulrahman University through the Fast-track Research Funding Program.

Reference

[1] A. Hamid, M. Alam, H. Sheherin and A.-S. K. Pathan, "Cyber Security Concerns in Social Networking Service," *International Journal of Communication Networks and Information Security,* vol. 12, no. 2, pp. 198-212, 2020.

[2] R. Verma and S. Sayyad, "Implementation of Web defacement detection technique," *Int. J. Innov. Eng. Technol,* vol. 6, pp. 134-140, 2015.

[3] A. Shamim, B. Fayyaz and V. Balakrishnan, "Layered defense in-depth model for it organizations," in *Proceedings of the 2nd International Conference on Innovations in Engineering and Technology, Bengaluru, India,* pp. 21-23, 2014.

[4] F. Hock and P. Kortiš, "Commercial and open-source based Intrusion Detection System and Intrusion Prevention System (IDS/IPS) design for an IP networks," in *2015 13th International Conference on Emerging eLearning Technologies and Applications (ICETA),* pp. 1-4, 2015.

[5] M. Frustaci, P. Pace, G. Aloi and G. Fortino, "Evaluating critical security issues of the IoT world: Present and future challenges," *IEEE Internet of things journal,* vol. 5, no. 4, pp. 2483-2495, 2017.

[6] M. N. Alenezi, H. Alabdulrazzaq and N. Q. Mohammad, "Symmetric Encryption Algorithms: Review and

Evaluation study," *International Journal of Communication Networks and Information Security*, vol. 12, no. 2, pp. 256-272, 2020.

[7] Z. Chiba, N. Abghour, K. Moussaid, A. El Omri and M. Rida, "Intelligent and improved self-adaptive anomaly based intrusion detection system for networks," *International Journal of Communication Networks and Information Security*, vol. 11, no. 2, pp. 312-330, 2019.

[8] J. F. Herrera-Cubides, P. A. Gaona-García, C. Montenegro-Marín, D. Cataño and R. González-Crespo, "Security aspects in web of data based on trust principles. A brief of literature review," *International Journal of Communication Networks and Information Security*, vol. 11, no. 3, pp. 365-379, 2019.

[9] G. Vasconcelos, R. S. Miani, V. C. Guizilini and J. R. Souza, "Evaluation of dos attacks on commercial wi-fi-based uavs," *International Journal of Communication Networks and Information Security*, vol. 11, no. 1, pp. 212-223, 2019.

[10] S. Groat, J. Tront and R. Marchany, "Advancing the defense in depth model," in *2012 7th International Conference on System of Systems Engineering (SoSE)*, pp. 285-290, 2012.

[11] W. Pieters, T. Dimkov and D. Pavlovic, "Security policy alignment: A formal approach," *IEEE Systems Journal*, vol. 7, no. 2, pp. 275-287, 2012.

[12] D. Zhang, "Big data security and privacy protection," in *8th International Conference on Management and Computer Science (ICMCS 2018)*, pp. 275-278, 2018.

[13] S. Al-Fedaghi, "Conceptual maps for physical security," in *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*, pp. 343-348, 2015.

[14] S.-d. Krit and E. Haimoud, "Overview of firewalls: Types and policies: Managing windows embedded firewall programmatically," in *2017 International Conference on Engineering & MIS (ICEMIS)*, pp. 1-7, 2017.

[15] A. A. Sharifi, B. A. Noorollahi and F. Farokhmanesh, "Intrusion detection and prevention systems (IDPS) and security issues," *International Journal of Computer Science and Network Security (IJCSNS)*, vol. 14, no. 11, p. 80, 2014.

[16] M. Z. A. Bhuiyan, J. Wu, G. Wang and J. Cao, "Sensing and decision making in cyber-physical systems: the case of structural event monitoring," *IEEE Transactions on Industrial Informatics*, vol. 12, no. 6, pp. 2103-2114, 2016.

[17] A. K. Sinha and S. Tripathy, "CookieArmor: Safeguarding against cross-site request forgery and session hijacking," *Security and Privacy*, vol. 2, no. 2, p. e60, 2019.

[18] A. K. Baitha and S. Vinod, "Session Hijacking and Prevention Technique," *International Journal of Engineering & Technology*, vol. 7, no. 2.6, pp. 193-198, 2018.

[19] W. Burgers, R. Verdult and M. Van Eekelen, "Prevent session hijacking by binding the session to the cryptographic network credentials," in *Nordic Conference on Secure IT Systems*, pp. 33-50, 2013.

[20] K. D'silva, J. Vanajakshi, K. Manjunath and S. Prabhu, "An effective method for preventing SQL injection attack and session hijacking," in *2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*, pp. 697-701, 2017.

[21] H. Asgari, S. Haines and O. Rysavy, "Identification of threats and security risk assessments for recursive Internet architecture," *IEEE Systems Journal*, vol. 12, no. 3, pp. 2437-2448, 2017.