A Survey of Layered Approach to Threats and Countermeasures

Dina S. Bujud1, Ahmed S. AlGhamdi2, Malik Najmus Saqib2

1Department of Information Technology, Marymount University, USA, dsb56678@marymount.edu
2Department of Cybersecurity, College of Computer Science and Engineering, University of Jeddah, Saudi Arabia, {ahmedg, mnajam}@uj.edu.sa

Abstract – In today's technological world it is extremely essential to identify the valuable assets of an organization, possible dangerous threats and state of the art defenses. It is necessary to raise the awareness of sophisticated threat among every employee of an organization. In this paper, we have elaborated most risky and smart threat that may trick user to get access of organization assets. It discusses information assurance component of an organization. It further discussed how layered approach is applied to organizations through Information Assurance elements. Each layer must be working correctly to ensure security.

Keywords: Threats, Countermeasure, Attack example, Information assurance.

1. Introduction
In the digital world in which we live in, it is apparent that there are more individuals, businesses, organizations, and governments that are interconnected through a huge network known as the Internet. The internet has become an essential component in which businesses, organizations, and governments depend on. Because of the interconnectivity nature of the Internet, cyber risks and attacks are becoming more sophisticated, destructive, and more complex. Huge amount of resources, money and time are consumed by the private and government sectors organizations to develop tools and strategies to effectively confront cyber security threats and attacks. One of these strategies is “Defense-In-Depth” [10].

Defense-in-depth is the idea of shielding the information system by implementing multiple defensive layers. If one defensive layer failed to fulfill its duty another one will already be in place to identify and prevent an attack. To measure security readiness, organizations need to evaluate security controls such as intrusion detection system, intrusion prevention system, firewalls, and antivirus system alone as well as their joint efficiency when deployed together in defense-in-depth. This paper will attempt to identify threats and vulnerability that currently threaten the safety of the cyber, the information assurance and its components, the components of defense-in-depth, and finally defense-in-depth layers.

This paper is organized as follow. Section II outline threat overview. Section III discusses a recent incident of a virus attack on major organizations. Section IV provide the details of information assurance component. Section IV discuss the essential layers’ mechanism to protect the organizational assets from the potential threat describe in section II. In last section VI concludes the paper.

2. Threats overview
To efficiently prevent attacks against its valuable assets, an organization is required to identify who are the adversaries, why they are attacking, what are techniques, and what capabilities they possess. The possible potential advertisers can be cyber criminals, any opposition country, hacktivist, insider threats, competitors. Their motivations may include denial of service, theft of customer data, reputation damage, and intelligence gathering. Their techniques may include social engineering, phishing, spread spam, network exploration, SQL injection, and malware installation.

2.1 Social engineering
In social engineering the attacker misleads or deceive people to show their sensitive information that are deemed important to launch a successful attack [4]. There are different types of social engineering attacks, for example:

- **Reverse social engineering**
  This one of the most commonly used technique by social engineering attackers. It's when that attacker causes a problem of the victim’s system and then make himself/herself available to fix the problem [7]. Once the problem is solved that attacker is perceived as a “hero” and thus secure the trust and confidence of the victim.

2.2 Spying and Eavesdropping
The attacker can configure the ID number and the password by simply observing the victim when he/she is typing it on the keyboard “All he needs is to be there behind the user and be able to see his fingers” [19].

2.3 Phishing [19]
Phishing is used by hacker to attract victims to visit a fake website. This website is crafted in a way that convince victims to provide sensitive financial and personal information. In some instances, these kinds of fake websites may contain malicious codes such Trojan key logging software that can be installed on the victim’s system in an attempt to gain more sensitive information about the victim.
2.4 Expert attacker

These kind of attacked are launched by skilled group of people [10]. Attacked by such class occur very less but if it occurs it is likely to be very successful. This is because such attackers perform deeply investigating his/her target, employ additional methods and techniques of attacks, and being more destructive with the advanced tools in his/her possession.

2.5 Insider threats

A clear and comprehensive understanding of insider attackers and their methods will help security professional to best prepare defense against them. Insider attackers are trusted individuals that are granted a higher level of trust than outsiders. This biggest kind of threat to an organization is an insider threat. Since the insider know much better than outsider that what is the sensitive information and where it is located [3]. Insiders have a login access to system resources. When insider intend to act maliciously then there are very less preventions because of the default trust on insiders. Usually, trust is established through processes of authentication followed by authorization to internal systems.

2.6 Hacktivists:

Many hackers are now working with each other to reach their goals. Some of these groups are called hacktivist based on political and social agenda, their intention is to challenge the authority, gain publicity, and create scandals. Working in groups gives them the advantage to strengthen their methods and expand the disruptive nature of their activities. Their methods include: social engineering, spread phishing, data exfiltration, network penetration, web page defacement, and denial of service attack [6].

3. ATTACK EXAMPLE – SHAMOON

According to the Kaspersky Lab report [14], the three attacked of Shamoon malware are observed recently on 17 Nov 2016, 29 Nov 2016 and 23 Jan 2017.

The first attempt was on August 15 2012, the Saudi Aramco was attacked by a campaign known as Shamoon. It delivers a malware called a disttrack. Distrack is a multipurpose tool that shows a similar behavior as warm. Disttrack can destroy data and make the victim system unusable [13]. It disseminates approximately 30,000 computers that are operating in Aramco network. Those all computers are running windows operating system. The company took full 2 weeks to recover from that virus attack completely. The major recoveries were the revival of its daily business operations that were caused by data loss and enabled workstation that are disabled from the incident. This attack also left a burning US flag image on the computer screen of Aramco and RasGas CO Ltd.

In this incident the Aramco had to disconnect far-reaching means of communications like phones, emails and payment system. Overnight the entire company is dependent on fax machines [14].

On 17 November 2016 the Shamoon’s Disttrack samples has been observed again. The security firm of Symantec Corp, Palo Alto Networks Inc and USA CrowdStrike warn the authorities about the possibility of new attacks [15]. This attack left an image (very much disturbing) of Syrian kid whose name is Alan Kurdi and who drowned in Mediterranean in 2015.

Few characteristics of Shamoon are as fellows

- A completely functioning module called ransomware is included in Shamoon 2.0
- There are two components of Shamoon 32 bits and 64 bits
- The recently found samples of Shamoon in Jan 2017 were analyzed. This time it does not include the command and control communication. While the previously found samples has the functionality of command and control that is a local server on victim machine.
- Shamoon embeds Arabic-Yemen resource language module

3.1 Components of Shamoon

Shamoon targets the Microsoft Windows NT based operating systems. Shamoon stuck the computer systems by erasing the master boot records that are used to start up the system. It is configured to start permanent data destruction of hard disk at 8:45 pm on Thursday. This timed was configured because most staff had leave for home for the weekend. In this way the chance of detection of Shamoon would be reduced and the major damaged could be caused.

Shamoon uses two components to damage the computer of a victim organization.

1. Dropper: this component creates a service with name “NtsSrv”. This service is persistent on the victim computer. This service seamlessly spread across the network by copying itself to other computers. During this process it also installed an additional component called a dropper on the victim computer. The dropper has two version 32 bit and 64 bit. If 64 bit dropper finds the 32 bit architecture on victim machine than it will drop 32 bit dropper and vice versa.

2. Wiper: (it is not malware wiper). The wiper drops the third component on the victim machine. This component is called Eldos driver. Eldos driver allow access to the hard disk of the victim machine from the user-mode without using the windows APIs. Eldos driver is used by the wiper to overwrite the complete hard disk of victim with the photos of a Syrian boy.

3.2 How Shamoon works

Shamoon is a complex and multi-step attack process that target Saudi oil companies. Following are the step that describe its working precisely [14]

1. Steal legitimate passwords (maybe by using Trojan.Ismdoor)
2. Targeted email campaign is lunched
3. The payload disttrack (a wiper and a communication function) is spread through the local network and a denial of service attack
4. Erase the data and other system setting and make the computer machine unusable
4. INFORMATION ASSURANCE COMPONENTS

Information assurance is accomplished when the organization’s valuable assets are well defended for any possible attacks. Such defenses are accomplished by the incorporating security services like authentication, confidentiality, identification, non-repudiation, availability, authorization, and integrity [1]. It is recommended to follow the model of protecting the resources, detecting any possible threats and reacting if threat or attack is detected while implementing the said security services. Therefore, with the integrated defense mechanism the organization must be ready for attack. They must implement attack detection and prevention tools and security policies which enable them to get stabilized even after the attack. To accomplished information assurance there is a need to work on the three areas [16].

4.1 Employees

Employees are the most important element in the process of information assurance. Accomplishing information assurance starts with a top management engagement and dedication built on comprehensive understanding of threats and vulnerabilities. Employee are responsible for the plan, design, engineer, deploy, operate, authorize, measure, evaluate, test, and maintain countless security mechanisms. For organization to confirm that they have expert who have the knowledge and expertise to perform these complex tasks, are required to develop a practical experience and awareness training program, and comprehensive plan for education. It is important that the employee of the organization have technical trainings, certifications, knowledge of system, physical and personal security.

Training enables organizations’ employees to be sufficiently trained to operate and safeguard the organization information systems. By creating an information assurance empowered employees, the organization can support and meet demands of a changing organization. Certification documents that all employees are proficient while operating and protecting the organization’s information systems. Awareness enables employees to observe what technology can do for them and who is authorized to access a particular system. System security administration are for employees who are selected to operate and maintain security services and products used to protect the systems that they are responsible for. Physical security restricts and observed any attempted access to area where that hosts the organization’s valuable assets such as datacenter, servers, and network infrastructure are located. Personal security means protecting employees form many threats such as social engineering, and spread phishing attacks, also protecting the organization from insider threats.

4.2 Technologies

Nowadays a huge variety of solutions and tools are available to address information assurance mechanisms and to detect and prevent interruptions to the organization’s internal systems. To guarantee that the appropriate solutions are adopted and employed, the organization should develop a processes and procedure for its implementation. These processes can be the process of measuring the risk associated with the internal systems, defining security policies, what are the available services for information assurance and its principles, architecture of information assurance, Configuration guidance and adoption of state-of-the-art products and services.

Cyber criminals can launch an attack from multiple points. It can be from the inside of an organization or outside. An organization must have incorporated a protection strategy in many areas to deal with the upcoming cyberattacks. An organization needs to implement protection mechanisms at multiple area to confront all classes of cyber attacks. These areas are:

- Defend infrastructures and the network
- Defend the local and wide area communication networks.
- Ensure the integrity and confidentiality of data that transferred from networks by implementing strong en/decryption algorithms.
- Detect and prevent any intrusion to the organization’ network by deploying intrusion detection systems, intrusion prevention systems, and firewalls.
- Protect the information system environments by providing access controls on servers and hosts.

According to the National Security Attention Agency, it is not difficult for the skilled attacker to explorer and know the vulnerabilities in available products which it can exploit later. So to prevent the adversary from exploiting the target, an organization must deploy multiple defensive mechanisms at multiple areas. All such mechanisms are a kind of a barrier for the attackers. Additionally, these mechanisms must have detection, prevention and protection, measures in place. Another example of layered defense is firewalls, it must be deployed at internal and external network boundaries, also it should be coupled with intrusion detection systems. the internal firewall supports access controls and data filtering.

Identify the security assurance and strength of all the information assurance elements like function of the resource’s value that is required to be protected and the vulnerabilities and threats that can occur. It is operationally practical and more effective to install security mechanism at the network internal and external borders instead of the employee system.

Deploy public key infrastructure and enforce strong key management that must serve each of the combined information assurance solutions and extremely immune to attacks. Deploy security mechanisms to detect, prevent, examine, and compare the outputs and respond according to it. These security mechanisms must assist the operational employee to reply question e.g. are we in attack situations, who is the adversary? What is being targeted? What are the procedure to react appropriately? How did the adversary plan for the attack? What are the lessons learned for this attack? What must be done to prevent future attacks?

4.3 Operations

The operations elements deal with all the compulsory requirements that supports the security status of the
An organization must have a clear and comprehensive information security strategy. Any change in the standard of information assurance must be confirming and recognizing. The decision of risk measurement must be supported by these confirming and recognizing processes. Such processes must accept some residual risk in the information system.

Handling the status w.r.t to security of information assurance solutions. For instance, install software and hardware updates, install virus updates, install security patches updates, and maintain list of access control. It provides services for key distribution and defending the organization’s valuable assets.

Organization must regularly perform system security assessments to measure the security readiness. For example, perform vulnerability scanners, perform port scanning, and RED teams. It should detect and responding to possible situation of breach in. Detecting attacks, threat and vulnerability, giving cautionary signals and how to respond to it.

5. LAYERS APPROACH

The basic notion of Layered Approach is applying various layers of defensive mechanism to assure a higher degree of dependence on critical information systems. at each layer, appropriate security mechanisms are deployed to protect that layer [2]. This strategy provides some level of resistance against the processes that an adversary might carry out to exploit the systems vulnerabilities [5]. Following are the layers

5.1 Security Procedure

This layer is highly misinterpreted layer of information assurance process. Security procedures must provide the underpinning for each strategy. The main idea of security procedures is clarification to each employee about his/her responsibility to protect and maintain the technology infrastructures. The security procedures [19] help protects both the information systems and employees in many ways, for example, The security procedures provides the guidance and procedures to defend the internal system of the organization. It determines a group of instructions of how to behave for all employees during the threat recognition phase and under attack. It should authorize the security employees to execute many obligations e.g. password cracking, packet capturing, scanning, monitoring, etc. It provides baselines to assess and measure compliance. It illustrates the penalties of violations to the policies.

Finally, it works as a starting stage to create a regular evaluation and update for known vulnerability and emerging threats, also enhancements in fulfilling organization requirements and employees’ responsiveness [8]. In case of misunderstood and mismanaged of the security procedures and its deployments, information security is depend on the state of the art solutions for the detection, prevention and reaction to the possible threat or attack. Security procedures must be effective, clear, implementable, and comprehensive with goal that are achievable. Also, it should facilitate an equilibrium between productivity and protection.

5.2 Rule oriented password

Many organizations incorporated a only a password based login system based on rules as the only defense. As the password is the mechanism that provides authorized access to occurs, it threatens its own defensive layer. The organization desired that each employee used a strong password for his/her login. Such organization forced its employees to choose a string password and does not accept the weak password. The main objective of strong password is to make it complicated and difficult for an adversary to break the password and get an unauthorized access to the organization’s information system. The system administrator should avoid weak passwords on all information systems with the principles [17] as follows:

- The lifetime of the password should be 60 days. After that user must set a new password.
- The account must be lock out after three failed attempts to log in.
- The system must record the successful and unsuccessful attempts of login.
- Apply password filters to ensure character and length compliance.
- Prevent employees to reuse previous passwords.
- The system must apply strong encryption on all passwords.

With the implementation of the above principles, it would be very hard for an adversary to gain access with authorized username and password.

5.3 Inbound and Outbound firewall [18]

An important and vital element of the layered approach is definitely both kinds of firewall. Firewalls are the best protection mechanisms in information system. Usually, they are deployed at the perimeter gateway to permit or deny access various network parts based upon a set of rules specified earlier. Also, firewalls can be deployed at the internal system to defend identified individuals or networks hosts. Firewalls are an essential element and they provide the following protection mechanisms:

- Minimize risk by defending the system from the possible threats that may exploit the unknown vulnerability.
- To protect the privacy by hardening the process of gaining access to data and resources of the organization’s systems.
- Maintain and apply the organization’s security policy.
- Records all traffic for and audit and forensic analysis.
- Provide virtual private network with strong en-/decryption algorithms.
- Install and integrate filtering mechanism of contents.
- Screening and deny undesirable traffic.

To achieve strong security and functionality, firewalls must be deployed correctly. Firewalls are not considered to be perfect with respect to technology. Firewall are not able to defend the organization mis-configurated implementation, backdoors network access, viruses, poor configurations, software bugs, end users, etc.
5.4 Network and Host based Intrusion detection systems

An accompaniment to a firewall plan is the incorporation of intrusion detection system. As the firewall provide safeguard so it does not consider to be effective if employed alone. The firewall cannot defend the organization’s system against, poor configuration, poor maintenance, end users, social engineering, modem access, etc. So, with the implementation of firewalls alone, many network activities of the organization’s system will become undetected. Intrusion detection systems have two parts: Network based Intrusion Detection System (NIDS) and Host based Intrusion Detection System (HIDS); they are responsible for monitor, detect, and record all activity that occur on network and the host [12]. It analyzes the packets/data to recognize threat, attack, and suspicious activities. It is tremendously important as in the absence of intrusion detection systems, malicious activities occurring on the network and host will be undetected. The NIDS and HIDS must be used together to apply this layer of defense. The integration between the Host based Intrusion Detection System and Network based Intrusion Detection System is the strong, effective and practical method to deploy the defense by using intrusion detection.

5.5 Deep scanning incoming and outgoing traffic

In the digital age, most organization need, at least, web browsing and email to efficiently talk to the insiders, as well as outside entities. As this offers the organization with a method to communicate, it also facilitates the need for malware to grow rapidly and overwhelm the organization’s networks and systems. Furthermore, web surfing and non-business related activities affect the productivity of the organization’s employees resulting in an increase of operation costs. Deep scanning incoming and outgoing traffic is a practical method that is deployed to protect the organization by proactively preventing spam, malicious file attachments, viruses, and unnecessary web surfing [10].

5.6 Encrypting all data

The most commonly used form of encryption is the encryption of data in transit. Usually, encryption is performed on packets when departing the host and decryption is performed when it arrives at the receiver side. Secure Socket Layer and Transport Layer Security protocols are commonly incorporated by organizations to protect their traffic. In addition, Secure Socket Layer is a very safe method to encrypted FTP sessions. Typically, there is no assurance that all of the defenses will stop an adversary to carry out an attack on the ciphertext in transit, as well as data stored on the system [11].

6. Conclusion

The layered approach is the effective and state-of-the-art method to develop a security plan for an organization. It is the framework and underpinning for the information security requirements. The overview of how defense-in-depth process can be applied to organizations through Information Assurance elements is discussed. The three elements that information assurance is implemented are through employees, technologies, and operations. The Layered approach contains the layers as the following: security policies, rule oriented password, Inbound and outbound firewall, network and host-based Intrusion detection systems, deep scanning of incoming and outgoing traffic, and encrypting all data. These layers are applied through many network and security technologies that are widely available in technology market.

7. References


