Vol. 7, No. 6 June 2016 ISSN 2079-8407
Journal of Emerging Trends in Computing and Information Sciences

http://www.cisjournal.org

# Defense-in-Depth: Layering Strategy

**Faisal Alghamdi**
Information Security, Lewis University, United States

## ABSTRACT

Industrial control systems form an important part of software applications which aids in facilitating the various operations in the crucial sectors of the industry. There has been a vast growth in issues with cyber security, which has negative impacts on the industrial control systems. This paper describes the direction and guidance to be used in developing and layering defense in depth strategies for the different organization using the control system networks. The different control networks should maintain a multitier information structure which requires accessing the facilities through the modem or data link. Also, access to the robust business environment requires several connections to the external internet, system domain, and other peer organizations. Across different private and public domains, there are many shared attributes that regard data communication and IT deployments in information infrastructures, for example in the control system domain. Many systems use the robust architectures in enhancing business and reducing costs where they increase the integration of business, control system networks, and the external environment. However, the integration of the multi-network strategies often brings about vulnerabilities thus reducing the organization skills and exposing mission-critical control systems to the cyber threats. Defense in Depth is an effective and efficient way of building an information security plan. It provides a framework for the organizational security needs.

**Keywords:** Defense in depth, layering, strategy

## 1. INTRODUCTION

Defense in Depth involves using multiple security mechanisms that incorporate layers across the network infrastructure in protecting the users, networks, the internal data, and systems [5]. The use of multiple defense measures is very useful so that if one fails, then the others can continue to protect the organizational assets. Major industries such as transportation, energy, and manufacturing are supported by critical infrastructure systems that are very dependent on the information system for the control and command functioning. Even in the high dependence on legal control systems, the critical infrastructure systems have migrated to the new technologies in communication. As a result, of this migration, open architecture standards, and common communication protocols have been assimilated, which have both negative and positive impacts on security matters [3]. The new communication protocols and standards, which provide increased control and interoperability in the control systems, have also been exploited in the networking domain and also on the internet. History shows that, initially, the control system security meant identifying and locating the problems in a closed-loop system, but now the authorized intrusion has issues that need to be addressed.

## 2. SECURITY CHALLENGES THAT EXIST IN THE INFORMATION SYSTEMS

Vulnerabilities are the weak points in the devices or systems that allow threats to compromise a system. For the computing environments that are based on the modern TCP/IP, the securities issues and technology-related vulnerabilities should be addressed. An example of this computing environment is the corporate infrastructure that manages the business that operates in the control system. For a long time, the security issues are governed by the operating plan and security policies which protect the important information assets in the organization. There are a lot of security issues in many network-based communications which must be addressed [4].

## 3. ATTACK METHODOLOGIES

Over the time, there has been an evolution of control networks from stand-alone domains to interconnected networks coexisting with the different corporate IT environments. The interconnection has introduced various security vulnerabilities and threats. The following are some of the pressing security issues that should be addressed in the information systems.

- **Man-in-the-middle Attacks:** In this case, the attacker exploits vulnerabilities in the information system such as poor integrity checking or weak authentication protocols. In this attack, the attacker may re-engineer and review the packet and payload content, as well as re-inject new packet into the network.
- **SQL data injection Attacks:** The attacker may inject SQL (Structured Query Language) command, via the web form input box, to make changes to data or gain access to resources. SQL commands that exploit non-validated input weaknesses may be injected in a database backend, and the attacker executes SQL commands via the web application. The use of sequential commands always makes it easier for the attackers to inject SQL commands in the database backend.
- **The attack in information systems through remote devices:** Many of the information systems today have a capability that allows people to access the terminal end point remotely. To enable the collection of maintenance and operational data, equipment has integrated web servers and file servers which facilitate robust communication. The remote accessing has given the attackers an opportunity to leverage control over the remote devices and cause unauthorized actions. The attacker may execute several procedures that alter

Vol. 7, No. 6 June 2016 ISSN 2079-8407
Journal of Emerging Trends in Computing and Information Sciences

http://www.cisjournal.org

data which is sent to the servers, or change how the device behaves.

- **Improper Cybersecurity Procedures:** The growth in complexity of operating large systems as well as the integration of networks, has also increased the personnel accessing the control networks. Improper procedures, such as the use of modems, have increased the success of the attacks. The modems may be improperly managed and hence, cause security issues.
- **Insecure coding techniques:** The lack of encryption or authentication within the applications in the information systems. The systems that have little encryption or authentication mechanisms can be comprised very easily. The vendors of the base software that is used to run the information systems may have vulnerable code, which may be publicized.

## 4. DEFENSE-IN-DEPTH STRATEGIES

Information Security involves the process of minimizing the risks while maintaining integrity, availability, and confidentiality of the data and system as a whole. The Defense-In-Depth was developed to defend the strategic assets or real world military where layers of defense are created, which would make the attacker spend a considerable large amount of time and resources. The main and tactical aim is delaying and rendering the enemy attack unsustainable for them. The Defense-In-Depth is used in defending the kinetic world, and Loss of Strength Gradient (LSG) is the main indicator the Defense in Depth is effective [5].

## 5. INFORMATION ASSURANCE

In Defense in Depth, achieving Information Assurance is an important aspect which requires a balanced focus on the three primary elements in an organization: People, Technology, and Operation (See Figure 1). Information insurance is a key goal desired to be achieved by every organization where the information systems and the information are protected against attacks by applying the security services. These security services include Authentication, Availability, Confidentiality, Non-Repudiation and Integrity [3]. The application of the security services is based on the Detect, Protect, and React paradigm. Even after incorporating the protection mechanisms, different forms are expected and therefore, the organizations should include the attack detection tools and procedures to recover from these security attacks.


**Figure 1.** Information assurance measures & actions Source: https://www.sans.org

The information technology security practitioners have established a component of Defense in Depth which is called the Layered Defense. The Layering strategy is where multiple layers of defense are implemented and this helps in combating multiple security issues. The figure below shows the use of multiple layers of defense in protecting the vulnerabilities.

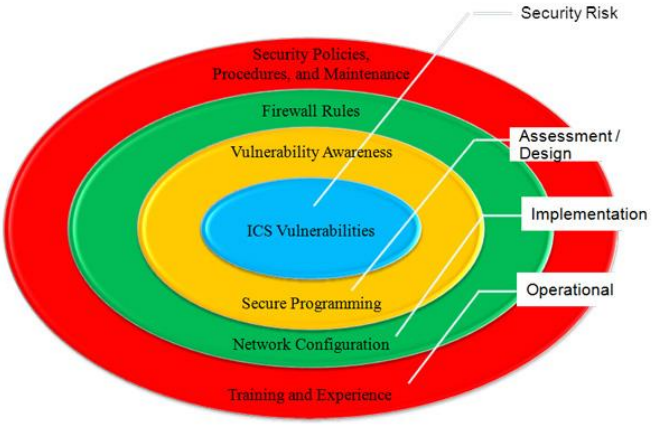


**Figure 2.** Planning and designing for defense-in-depth Source: https://www.isa.org/templates/blog-detail.aspx?id=126256

This strategy is based on the use of security countermeasures that go across the network, operational and host functionality. The aggregation of all the security activities gives a complete protection over the entire architecture.

## 6. DEFENSE-IN-DEPTH STRATEGIC FRAMEWORK

The information security personnel should take a holistic approach and leverage all of the resources available in any organization so as to provide effective layer protection. The following are the defense layers that available in the Defense in Depth strategic framework as described by Son& Kim (2014).

- **Security Policies Layer:** Security policies are the foundation for the planning of Defense in Depth. The main purpose of the security policies is educating all the system users of the obligation they have in ensuring that the business information and technologies are secure. Security Policies help both the employees and business information in ways such as providing guidance on what the users should do in protecting the business information and establishing rules of conduct for the users of the system. The layer also provides authorization for the personnel dealing with the information security to perform duties related to security issues. The Security Policies also defines the consequences of violations to the policies. The policies must be effective and realistic having achievable goals. These policies should balance between productivity and

protection of the information and should always be reviewed and revised on at least an annual basis.

- **Strong Password Layer:** Many organizations rely on password as their defense. The password is the key through which the authorized users access the system, and it forms a defense layer. The use of strong passwords usually involves password specification and enforcement by using the Password Security Policy. The main goal of using password is making the access to a system very difficult for an attacker with the use of an authorized password and username.
- **Perimeter Protection with Firewalls Layer:** This layer is the most essential and crucial part of the Information Security. Firewalls are an important protection control mechanism that is defined in information security policies. Firewall is deployed at perimeter gateway and it is used as a traffic cop, which allows or denies access to and from network segments. Firewalls serve an important role in Defense in Depth strategy. They provide some elements of protection such as reduction of risks of attempts to exploit vulnerabilities by protecting systems and increasing the privacy of the information by making it harder to get information. Firewalls enforce the security policy of an organization and provide VPN/Encryption capabilities. It also perform Network Address Translation (NAT), filter unwanted traffic and provides Integration with the content filtering systems.
- Firewalls are categorized into three types which include the Packet Filter, Stateful Inspection, and Proxy Server Firewall. The Packet Filter is a router that uses the access control lists. The packet filter checks every packet both outbound and inbound, and it also checks the source port and the destination port by the rule set that is defined. Proxy Server firewall runs in certain proxy application software, for example, Gauntlet. This server mediates the traffic between networks. The Stateful Inspection Firewall balances a packet filter that is faster but less secure, and the proxy server that is slower but more secure. Their functionality is based on packet filtering while they also provide proxy service that is less robust. They give high degree security and also a faster throughput [4].
- **Intrusion Detection Systems (IDS) Layer:** This is Defense in Depth strategy that complements the Firewall strategy. IDS layer is divided into two categorized into two types which are the Network Intrusion Detection Systems (NIDS) and Host Intrusion Detection Systems (HIDS). The Intrusion Detection Systems collect and monitor the activities of end users, poor configurations, social engineering, and modem access on either a host or the network. They examine the information or data in traffic to detect malicious activity, attacks or threats. The combination of NIDS and HIDS is an effective and efficient way of implementing an Intrusion Detection defense layer.
- **Content Filtering Layer:** This is a Defense in Depth layer that provides an efficient way of protecting the business information from the spam, viruses, and erroneous web surfing. This layer protects the users against unwanted images, websites or emails. It actively scans for viruses and other malware and also filters out unwanted traffic.
- **Data Encryption Layer:** This is the last layer of defense in the Defense in Depth strategy. Data Encryption is used to prevent an attacker from sniffing the network for a session replay attack or man in the middle attack. The data is encrypted by the host and decrypted by the client. Many organization use SSL/TLS with a strong encryption algorithm to enable secure Client/Server communication. The stored data should also be encrypted for proper security.

## 7. CONCLUSION

Defense in Depth is an effective and efficient way of building an information security plan. It provides a framework for the organizational security needs. Other security techniques that complement the Defense in Depth strategy include Network Scanning, Vulnerability Scanning, Patch Management, Log Review, Penetration Testing, and System Hardening. The Implementation of the Defense in Depth strategic plan helps in killing all kinds of attack and ensures the system is safe. Each of the mechanisms discussed is very important, but when they are implemented together in a layering strategy they become more powerful in implementing security plan. Information Security involves the process of minimizing the risks while maintaining integrity, availability, and confidentiality of the data and system as a whole. The Defense-In-Depth was developed to defend the strategic assets where layers of defense are created to make the attacker spend a considerable large amount of time and resources.

## REFERENCES

[1] Adamski, M., Frankowski, G., Jerzak, M., Stokłosa, D., & Rzepka, M. (2011). Defense in Depth Strategy: A Use Case Scenario of Securing a Virtual Laboratory. Remote Instrumentation for eScience and Related Aspects, 75-101.

[2] Cohen, F. B. (1992). Defense-in-depth against computer viruses. Computers & Security, 11(6), 563-579. doi:10.1016/0167-4048(92)90192-t

[3] Kuipers, D.& Fabro, M. (2006). Control Systems Cyber Security: Defense in Depth Strategies.

[4] Smith, C. (2003). Understanding concepts in the defense in depth strategy. IEEE 37th Annual 2003 International Carnahan Conference on Security Technology, 2003. Proceedings.

[5] Son, H., & Kim, S. (2014). Defense-in-Depth Architecture of Server Systems for the Improvement of Cyber Security. IJSIA, 8(3), 261-266. doi:10.14257/ijsia.2014.8.3.27

[6] Svendsen, A. D. (2015). Advancing "Defence-in-depth": intelligence and systems dynamics. Defense & Security Analysis, 31(1), 58-73.