International Journal of Security and Its Applications
Vol.8, No.3 (2014), pp. 261-266
http://dx.doi.org/10.14257/ijsia.2014.8.3.27

Defense–in–Depth Architecture of Server Systems for the Improvement of Cyber Security

Hanseong Son[1] and Soongohn Kim[2*]

[1]Department of Game Engineering, Joongbu University,
201 Daehakro, Chubu-Meon, GumsanGun, Chungnam, 312-702, Korea
[2]Department of Computer Science, Joongbu University,
201 Daehakro, Chubu-Meon, GumsanGun, Chungnam, 312-702, Korea
hsson, sgkim@joongbu.ac.kr

Abstract

In this work, the features of the Defense-in-Depth (DID) concept of nuclear industry cyber security have been studied to obtain the insights of the DID architecture of server systems. Through the feature analysis, we have found out that there need to be clear system boundaries among all DID levels, systems should be classified by smaller scale, and one-way data flow makes it possible to assign a high cyber security level to a system. Based on the finding, we have suggested a DID architecture for server systems. The architecture is an n-tier and 'thin' server architecture which introduces the special features of the nuclear industry DID concept. The suggested architecture is expected to be very useful to improve the cyber security of various kinds of server systems.

Key Words: *Defense-in-Depth, cyber security, n-tier server architecture, thin server architecture, multi-leveled security architecture*

1. Introduction

In order to improve the cyber security of server systems, the integrated consideration of methods, techniques, tools, people and processes required to protect information is crucial. This is because there is no single measure or single technology that will make information safe and secure from all external and internal threats. Defense–in–Depth (DID), which is a design concept, originally coined in a military context and crucially used in nuclear industry, can be a useful concept for the improvement of cyber security [1]. This work has studied the DID concept of nuclear industry cyber security. Son and Kim, in a previous work, assigned cyber security levels to a typical digital I&C system using the DID concept and obtained the lessons learned from the security level assignment [2]. This work has revisited the lessons and deduced a few special features of the DID concept which are related to server system architecture. Based on the special features, which are described in Section 2, we have suggested a DID architecture for server systems, which is an n-tier and 'thin' server architecture introducing the special features of the nuclear industry DID concept. The suggested architecture is described in Section 3. The suggested architecture is expected to be very useful to improve the cyber security of various kinds of server systems.

[*] Corresponding Author

ISSN: 1738-9976 IJSIA

2. Defense-in-Depth in Nuclear Industry Cyber Security

2.1. Defense–in–Depth Concept

Originally, DID is a basic concept for safety design of nuclear facilities. The multi-barriers and multiple levels of protection concept are used in nuclear power plants for DID design [1]. With the introduction of digital systems, nuclear reactors are forced to care for the problem of cyber attacks because I&C systems have been digitalized using networks or communication systems [3, 4]. DID is also an approach in which multiple levels of security and methods are deployed to guard against failure of one component or levels in terms of cyber security. The architecture of DID for cyber security is presented in Figure 1.

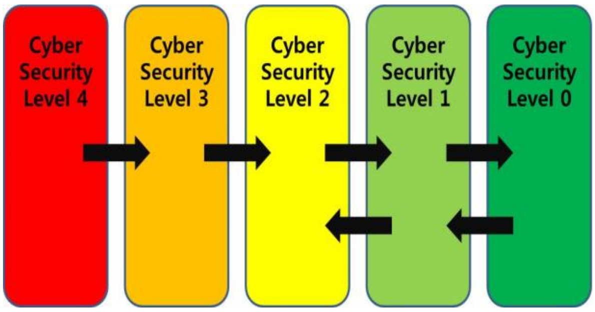


Figure 1. The Architecture of Defense–in–depth Concept in Nuclear Industry Cyber Security [2]

This defensive architecture includes the five concentric cyber security defensive levels separated by security boundaries. The systems requiring the greater degree of security are located within a greater number of boundaries. Figure 1 shown above does not always correspond directly to the physical location. The critical digital assets (CDAs) associated with safety, important to safety and security functions, as well as support systems and equipments which, if compromised, would adversely impact safety, important to safety and security functions, are allocated to Level 4 and are protected from all lower. And only one-way data flow is allowed from level 4 to level 3 and from level 3 to level 2. Here, the initiation of communications from digital assets at lower security levels to digital assets at higher security levels is prohibited. Data only flows from one level to other levels through a device or devices that enforce security policy between each level, by maintaining the capability to detect, prevent, delay, mitigate, and recover from cyber attacks [2, 5].

2.2. Special Features Related to DID Architecture

Through a case study, Son and Kim pointed out that the CDAs of cyber security DID Level 4 and Level 3 were classified clearly but the ones of Level 2 to Level 0 were not [2]. From this fact, the lesson that there are no clear boundaries among all levels for DID was obtained. The levels of security barriers shall be defined clearly and explicitly according to the DID concept. This lesson deduces two special features of the nuclear industry cyber security, related to the DID architecture, which are that there need to be clear system boundaries among all DID levels and that the digital I&C systems should be classified by smaller scale in order to have the clear system boundaries in view of the DID levels.

Another important lesson from the case study was that it was possible to assign Level 4 and Level 3 to the corresponding CDAs because they offered the mechanisms of one-way data flow [2]. If a system has the information that can flow one-way and is important to safety and security, it can be assigned to Level 4 or Level 3. This lesson also deduces a special feature that one-way data flow makes it possible to assign a high cyber security level to a system.

3. Architecture for Server System Cyber Security Improvement

Basically, the architecture proposed in this work is an n-tier server architecture, which is distributed properly. Figure 2 shows an example of 3-tier server system architecture. Distributed servers are applied for overcoming the problems with central server frameworks like poor distribution of processing, high user response latency, heavy state management on the servers, and reduced opportunity for interoperability [6-9]. When a server is centralized, the communications between clients and servers and among servers are hidden by the framework and the server 'endpoints' are hard or impossible to isolate. This is not helpful in assigning cyber security levels to servers clearly. On the contrary, in distributed servers, we can get clear boundaries among servers as well as between clients and servers by exposing explicit and secure data-interchange interfaces. As the first special feature mentioned in Section 2.2 infers, it is crucial to clearly assign the security levels to subsystems in implementing the DID concept for a system architecture. Therefore, the n-tier architecture is favorable for the cyber security of servers.

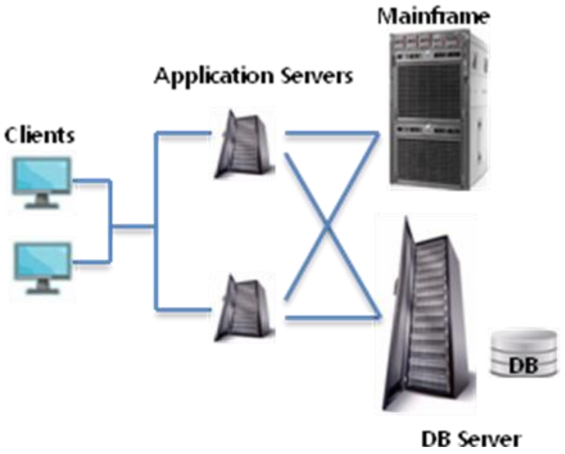


Figure 2. Example of 3-tier Server System Architecture

The second special feature is related to keeping a server as 'thin' as possible. Each distributed server shall be designed as 'thin' as possible so that it can be as easy as possible to encode or protect the information which it handles. To do this, the security level of information shall be considered. All the information that the server system deals with is broken down and assigned with different security levels. As the criticality of the information increases, the information shall be handled on the server with the higher level. Reflecting this feature to the DID architecture, as shown in Figure 3, the DB server in Figure 2 can be separated into two different DB servers according to the information security level.

It shall also be considered that when one server is penetrated by some cyber attacks, the other server can be maintained safely without the cyber attacks. Here it is checked if the system deals with the information that can flow one-way from a server to another and is important to security. If it does any, the information should be handled with a dedicated server, which shall be assigned to Level 3 or Level 4. This is directly related to the third special feature. This feature introduces the 'multi-leveled security' architecture. Figure 3 shows an example of server system that has the architecture proposed in this work. It is assumed that some information can be dealt with through off-line communication. Owing to one-way communication and even off-line communication, the server system can have Level 3 sub-system and Level 4 sub-system. Thus the system becomes to have the multi-leveled security architecture in a full scale.

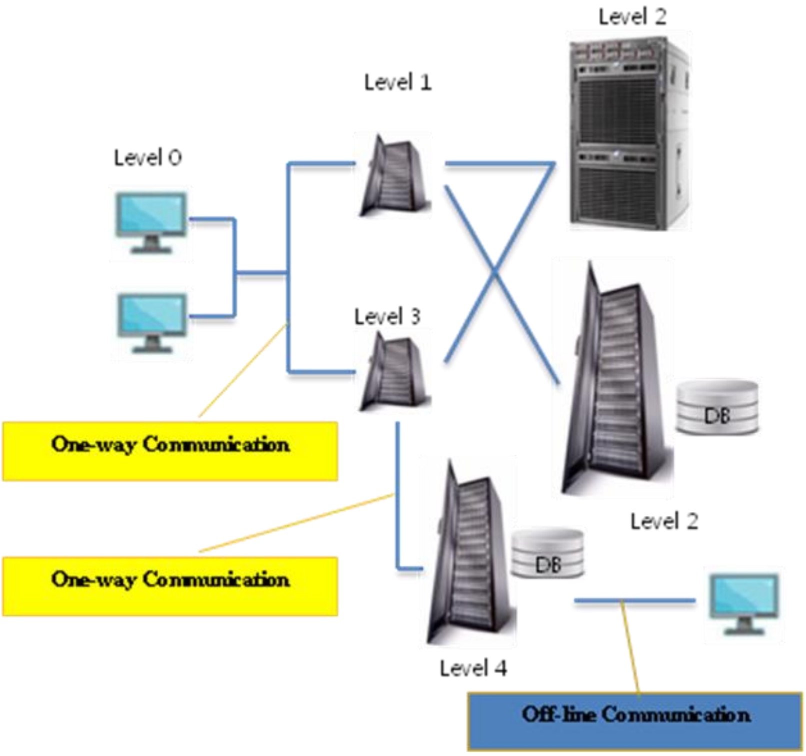


Figure 3. Example of Suggested DID Architecture for Server Systems

4. Conclusions

This work has proposed a DID architecture for the improvement of server system cyber security. The architecture is featured as the n-tier and 'thin' server architecture and the 'multi-leveled security' architecture. Based on the lessons learned from the security level assignment case study, the special features of the DID concept in nuclear industry cyber security have been deduced. The features are directly reflected onto the DID architecture proposed in this work. This architecture is expected to be applied to improve the cyber security of various server systems.

References

[1] E. G. Wallance, K. N. Fleming and E. M. Buras, "Next Generation Nuclear Plant Defense-in-Depth Approach", Idaho National Laboratory (INL), **(2009)** December 01.

[2] H. Son and S. Kim, "Defense–in–Depth Strategy for Smart Service Sever Cyber Security", T.-h. Kim et al. (Eds.): FGCN/DCA 2012, CCIS 350, **(2012)**, pp. 181–188.

[3] ANSTO Replacement Research Reactor Project Safety Analysis Report Chapter 8 Instrumentation and Control, **(2004)** November 01.

[4] B. Gan and J. H. Brendlen, "Nuclear power plant digital instrumentation and control modifications", Nuclear Science Symp. and Medical Imaging Conf., IEEE Conference Record, vol. 2, **(1992)** October 25-31.

[5] Regulatory Guide 5.71, Cyber Security Programs for Nuclear Facilities, U.S. Nuclear Regulatory Commission, **(2010)** January.

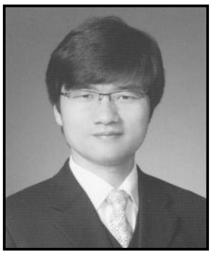
[6] J. Lui and M. Chan, "An Efficient Partitioning Algorithm for Distributed Virtual Environment Systems", IEEE Trans. on Parallel and Distributed System, vol. 13, no. 2, **(2002)**, pp. 193-211.

[7] P. Morllo, "Improving the Performance of Distributed Virtual Environment Systems", IEEE Trans. on Parallel and Distributed System, vol. 16, no. 7, **(2005)**, pp. 637-649.

[8] H. Jordan, "Dynamic Load Management for MMOGs in Distributed Environments", Proc. of the 7th ACM International Conference on Computing Frontiers, **(2010)**, pp. 337-346.

[9] W. Rynson and H. Lau, "Hybrid Load Balancing for Online Games", Proc. of the International Conference on Multimedia, **(2010)**, pp. 100-103.

Authors



Han Seong Son, he received a Ph.D. degree from Korea Advanced Institute of Science and Technology in Nuclear Engineering in 2000. He has been working as an assistant professor in Joongbu University from March 2008. His research interests include Software Engineering, Software Reliability, Cyber Security, and so forth.

Soon Gohn Kim, he received a Ph.D. degree from Chonbuk National University, Seoul Korea, in Computer Engineering in 1999. He has been working as a Professor in Joongbu University from March 1995. His research interests include Ubiquitous Computing, Distributed Computing, Database Integrity, Methodology of Software Development, Software Evaluation, Networks and so on.