International Journal of Security and Its Applications
Vol.8, No.3 (2014), pp. 235-240
http://dx.doi.org/10.14257/ijsia.2014.8.3.24

Architecture Design and Cyber Security Evaluation of a Festival Management System Server

Han Seong Son[1] and Soon Gohn Kim[2*]

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

Abstract

This article introduces an architecture design of a festival management system server. The design incorporates the concept of n-tier architecture and that of 'thin' server. The designed architecture was evaluated in view of cyber security, particularly defense-in-depth concept. The evaluation was performed to check if the features of the defense-in-depth concept according to a guideline are applied properly to the architecture. After reflecting the evaluation results, the designed architecture has become adequate for a festival management system when the high security is required for the system.

Keywords: *Festival Management System, Architecture Design, Cyber Security, Defense-in-Depth*

1. Introduction

The regional festivals have been hosted quite frequently because they have many advantages in terms of increasing the incomes of the local residents, raising the potential for regional development, and being suitable for the acceptance by the dynamic forms of the modern tourism. The festival management system is a system that is utilized to manage various activities and huge amount of data related to a festival. This system involves advanced information network and multimedia technology like the combination of media and computer, video conference system, the interaction between participants of different location with on-screen pictures of each other which are possible to use voice, text and graphic.

This article introduces an architecture design of a festival management system server. The design incorporates the concept of n-tier architecture and that of 'thin' server. The designed architecture was evaluated in view of cyber security, particularly DID (Defense-in-Depth) concept. The evaluation was performed to check if the features of the DID concept according to a guideline are applied properly to the architecture. The initial evaluation concluded that the designed architecture is not adequate for a festival management system when the high security is required for the system. The essential features of the DID concept were applied for the architecture according to the evaluation. As a result of the application, the designed architecture has become adequate for a festival management system in view of cyber security.

Section 2 briefly introduces the festival management system. Section 3 describes the initial design of the festival management system server architecture. Section 4 discusses the DID

* Corresponding Author

ISSN: 1738-9976 IJSIA

concept and the design improvement according to the concept. Section 5 presents the conclusions of this article.

2. Festival Management System

The festival management system enables a direct operation of all the festival processes such as preparation, operation, post festival management, and administrative tasks, and so forth [1]. One of the main features of the festival management system is the situation awareness capability, which is an ability to sense and analyze context from various sources; it allows the system to take different actions adaptively in different contexts [2]. To implement this feature, Kim and Ko proposed an adaptive agent of error or application sharing based on a hybrid software architecture [3]. The adaptive agent took advantages of the two approaches to software architecture on which distributed collaborative application, CACV (Centralized-Abstraction and Centralized-View) and RARV (Replicated-Abstraction and Replicated-View).

The festival management system requires various kinds of assessment data such as punctuality check, smoothness check, surveys, and so on and different kinds of management activities like schedule reporting, visitor feedback, event management, risk management, visitor traffic flow trace, and so forth. The functions for the design and construction of festival site facilities are essentially required for the system. Furthermore, for smooth feedback, the interoperability between the QRCode (Quick Response Code) management system and the automatic visitor processing system is essential [3].

The festival management system has the managers such as GSM (Global Session Manager), Daemon, LSM (Local Session Manager) and PSM (Participant Session Manager). GSM has the function of controlling whole session when a number of sessions are open simultaneously for festival data. LSM manages only one session for festival data. For example, LSM is a local session manager in distributed multimedia environment for festival data. GSM can manage multiple LSM for festival data. Daemon is an object with services to create session for festival data. Session management exchanges message or command between LSM and GSM. It also exchanges media data between media servers based on the interpretation of message handler for festival sites [3].

3. Initial Design of the Server Architecture

The festival management system should be a distributed system due to the features and functions described in Section 2. The festival management system server introduces the n-tier server architecture which is for distributed server systems. Figure 1 shows the initial design of the festival management systems server architecture which is the 3-tier server system architecture. The functions and the loads of the server are properly distributed to application servers, a DB server, and a mainframe server. Generally, 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 [4-7]. 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. On the contrary, in distributed servers, we can get clear boundaries among servers as well as between clients and servers by exposing explicit data-interchange interfaces.

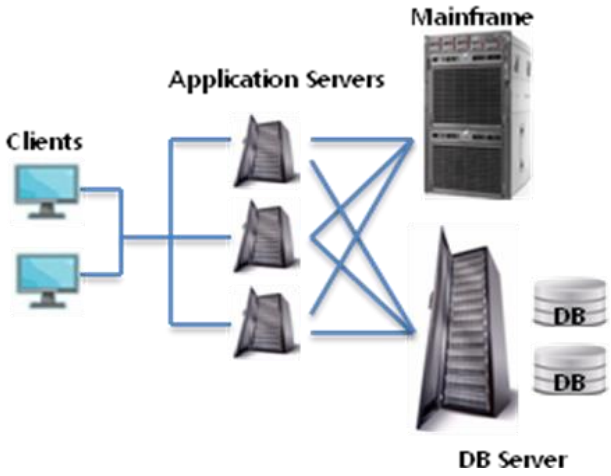


Figure 1. Initial Architecture Design of the Festival Management System Server

In this design, each distributed server is designed to deal with its own data and sessions. Application servers handles sessions. DB server supports the application servers with festival data and plays role of media server. Mainframe server operates daemons and supports error and application program sharing. GSM operates on Mainframe sever.

4. Cyber Security Evaluation and Design Improvement

The designed architecture was evaluated in view of cyber security, particularly DID (Defense-in-Depth) concept. DID concept and the design improvement according to the concept are described in this section.

4.1. Defense-in-Depth (DID) 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 [8]. 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 [9, 10]. 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 2.

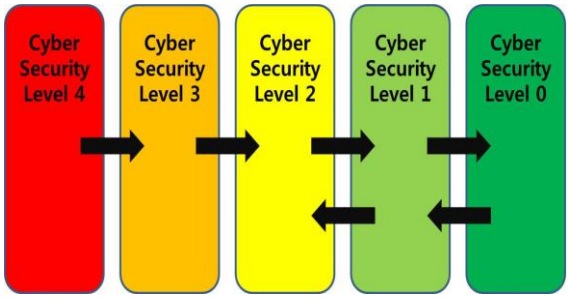


Figure 2. The Architecture of Defense–in–depth concept in Nuclear Industry Cyber Security [11]

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 2 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 [11, 12].

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 [11]. 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 related to the DID architecture, which are that there need to be clear system boundaries among all DID levels and that the 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 only when they offered the mechanisms of one-way data flow [11]. Thus, 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.

4.2. Evaluation Results and Design Improvement

As mentioned in Section 4.1, 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 inferred from the first special feature mentioned in Section 4.1, 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.

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. While doing this, the security level of information shall also 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.

To implement DID concept to the server architecture design, it shall 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.

Figure 3 shows the design improvements of the server architecture. Reflecting the second special feature of DID concept to the initial architecture design, as shown in Figure 3, the DB server in Figure 1 can be separated into two different DB servers according to the information security level. It is also suggested that some information should 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 architecture reflects the third special feature of DID concept. All the levels of the security architecture are shown in the improved architecture described in Figure 3.

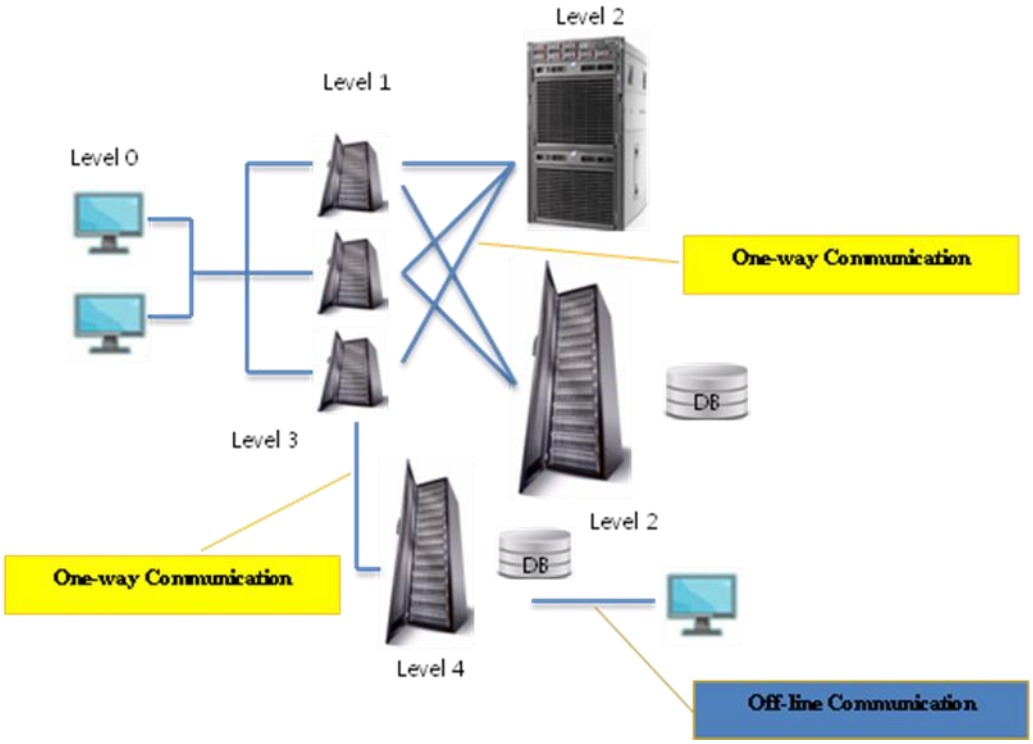


Figure 3. Improved Architecture Design of the Festival Management System Server

5. Conclusions

An architecture design of a festival management system server is described in this article. Initially, the design was based on the concept of n-tier architecture. The designed architecture was evaluated in view of cyber security, particularly DID (Defense-in-Depth) concept. The evaluation was performed to check if the features of the DID concept according to a guideline are applied properly to the architecture. The initial evaluation concluded that the designed architecture is not adequate for a festival management system when the high security is required for the system. Based on the lessons learned from the security level assignment case study, the special features of DID concept in nuclear industry cyber security have been deduced. The essential features of DID concept were applied for the architecture design improvement. The improved design incorporated the concept of 'thin' server and the one-way communication mechanism. As a result of the improvement, the designed architecture has become adequate for a festival management system in view of cyber security. This architecture is expected to be applied to improve the cyber security of various server systems.

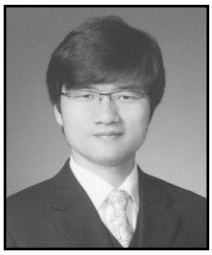
Acknowledgements

This paper was supported by Local Industry Technology and Development Fund (Project No. : A001100187), in 2011-2013.
Sunny Side Up

References

[1] B. C. Lim, S. G. Kim and B. C. Lee, "Requirements Analysis for Smart Festival Management System", Proceedings of the 37th International Conference of the KIPS, Jeju, Korea, **(2012)**, April 15-19.
[2] S. Yau, F. Karim, Y. Wang, B. Wang and S. Gupta, "Reconfigurable Context-Sensitive Middleware for Pervasive Computing", IEEE Pervasive Computing, vol. 1, no. 3, **(2002)**, pp. 33-40.
[3] S. G. Kim and E. N. Ko, "An Error Control Agent Running on RCSM for Smart Festival Management System", LNCS 7709, Edited T.H. Kim, **(2012)**, pp. 80–86.
[4] 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.
[5] 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.
[6] H. Jordan, "Dynamic Load Management for MMOGs in Distributed Environments", Proceedings of the 7th ACM International Conference on Computing Frontiers, **(2010)**, pp. 337-346.
[7] W. Rynson and H. Lau, "Hybrid Load Balancing for Online Games", Proceedings of the International Conference on Multimedia, **(2010)**, pp. 100-103.
[8] 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.
[9] ANSTO Replacement Research Reactor Project Safety Analysis Report Chapter 8 Instrumentation and Control, **(2004)** November 01.
[10] 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.
[11] H. S. Son and S. G. Kim, "Defense–in–Depth Strategy for Smart Service Sever Cyber Security", In CCIS 350, Edited T.H. Kim, **(2012)**, pp. 181–188.
[12] Regulatory Guide 5.71, Cyber Security Programs for Nuclear Facilities, U.S. Nuclear Regulatory Commission, **(2010)** January.

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, cryptographic protocol, methodology of software development, software evaluation, network security, and so on.

