Design and Implementation of Security System for War game Simulation System

Jong Seok Song, Chu Yu Li, Long Jin, Keun Ho Ryu
Dept. of Computer Science, Chungbuk National University
12, Gaesin-dong, Heungdeok-gu, Cheongju, Chungbuk 361-763, Korea
{jssong, lichuyu, kimlyong, khryu}@dblab.chungbuk.ac.kr

Abstract: War game Simulation System is a simulation system of military operation. In order to ensure all of the data that are running are secure, this system has to emphasize the security policy. In this paper, we analyze the running environment and the weakness of the security about exiting system. For improving the weakness, we design and implement this security system that is consisted of three components: Authentication System, Encryption System and Network Security System. Therefore, we can apply War game Simulation System to security system and improve the secure performance of this one.

Keywords: War game Simulation System, Security System, Authentication, Encryption, Network Security.

1. Introduction

I will design the war game simulation environment that will take into accounts of the network security and implement them into the war game simulation. The system needs to prevent unauthorized users to gain access to the army secret information and data. A user authentication system needs to be implemented. And a database management tool will take care of the army secret files and information. So we will implement the user authentication system that will prevent unwanted users to gain access to the military secret information. Secondly, the information and data from the war game simulation will be stored inside the database and managed there. When the war game simulation is operated, data is transferred between the network, simulation server, network server and the intermediation server to the client. So the information needs to be protected and managed within the database system. This uses a SEED algorithm which is one of the Korean Standard Algorithms for security area. Because the algorithm uses a software encryption library, the clients can conveniently use it.

Thirdly, the information is being transferred from simulation server and network server, intermediation server, to client PC. This needs to be implemented with SSL(Secure Socket Layer) or IPSec protocol or another protocol. But the operation load from using the protocol was too much and so we have implemented it with SSL protocol instead.

The Section 2 of this paper will be about the analysis of the war game simulation and Section 3 will be my analysis of the system security and its weakness. Section 4 will be about the security design of the simulation and Section 5 is the test results and last section is my final conclusion.

2. Analysis for the war game simulation system

The system's relationship between each component is as below. Simulation engine acts as the server that takes care of the scenario and reads in the game sessions and the network server takes care of the network connection. The intermediation server being in the middle of the client and simulation server manages the military files and geographical data being passed in between. When the war game is operated, the commanders will go through user authentication system and send the simulation instructions and connect to the simulation engine thus session is made. Simulation server sends the session information to the intermediation server and the client PC receives them and displays on the PC screen. This is repeated within the war game system. The data from simulation engine, network system, and the overall resulting data will be saved in the server for future analyze.

3. The security policy for the war game simulation

Events are used to represent and exchange events read by RFID readers in logistics environment. In this section, we describe the definition and structure of the events.

1) Analysis of the security weakness

The result from the war game simulation and its analysis of the security threats in the simulation environment is as follows. First, any user could connect to the system and there is no current ability to monitor and control the user connections. Second, the sensitive data are transmitted in the network in ASCII format and stored in the database. Third, the military secret data are being used and operated in the war game system and transmitted through TCP/IP, the packets and data is susceptible to hacking and data being stolen. Fourth, simulation server, network server, and intermediation server are directly connected to network and the threat of attack and unauthorized approach is including. And also authentication between systems is impossible. For the solution of security weakness that was analyzed in the operating circumstance of war game simulation, the policy of security should be set up in the next chapter.

2) Security policy making

The security policy of war game simulation system is requested to establish the technical security system in the prospect of authentication, access control, confidentiality and integrity, non-repudiation, and availability. The first, it is required to introduce user's authentication system for solving user's authentication problems in the system of control officer. For the user's authentication mechanism, there are ID, password system, one time password system, public key certificate usage system etc. The users of war game simulation system have ID and password and should pass through the procedure of user's authentication and keep security based on the certificate of authentication of SSL. This is because that it can provide stronger user's authentication by unifying the simple ID/password system and authentication system. The second, for the control of client and approach to server system, in case of server system SSH and SSL are used. For the client's access control, user's authentication mechanism is operated in combination. The third, in order to compensate the weakness of data in simulation system, the software secret code library is used. The software secret code library is operated after loading the secret code module in client. But because the open key should be used, it is difficult to manage the key. The fourth, the army secret information is transmitted by each components of war game simulation system and the threat of wiretapping and forgery is occurring. For solving this problem, it is required to use decode communication protocol. If SSL used in TCP, confidence of safety is increasing and the network security can be setup within the limit that capability of war game is not decreasing. The fifth, it is required to setup the security policy for detecting hacker's attack and DOS attack by introducing invasion intercept system and detection system.

4. Design for war game simulation security system

1) User's authentication system

The user's authentication system is divided into two categories; "simple ID/password management system" that is using by registration of user's ID and password and "one-time password management system" that is used different password whenever it is used.

And there are two systems; one is "digital ID system" which is used for authentication for users by X.509 public key and the other is "IC card/USB security token system" that is used by H/W for safety management of authentication information. In the war game simulation system, "the simple ID / password management system" that password management is easily controlled and "the digital ID system" that can be grafted to secret code communication are combined and designed. The each ID and password is to be authenticated by user's authentication system and ID and password are to be protected by SSL based on authentication certificate. And it is designed to produce the log for all users, which is approaching to war game simulation system and it can be used for information inspection. The composition of user's authentication system is shown on diagram 3 and the mutual function of each system is as follows. The manager registers the user on the user management homepage and the user management homepage keeps registration of users and database. The manager provides users with ID and password and the user inputs client with ID and password. The client transmits the ID and password that were input to user's authentication system.

The user's authentication system transmits user's level and key for duplication as the result of user's authentication and the user approaches to war game simulation. Such algorithms are shown section 4.2.

2) Encryption System

The encryption system is embedded in the client module that authenticates the user login and implemented in the S/W encryption library format. But it is can also be in the shape of Smart cards and USB modules and other H/W peripherals. Block algorithm has been implemented in the security program within the war game simulation program for data protection. The algorithm is a 128 bit length national standard encoding protocol, called SEED. It is designed and operated in the client side in the form of 'S/W encryption library'. The functions in the security system consist of the following: the encryption library authenticating the users also known as IC fundamental user authentication module, data confidentiality encryption/decryption modules, data integrity MAC, etc. Such algorithms are shown below.

```
/* declaration for use crypt.dll */
public declare function authentication Lib "crypt.dll" as
integer

/* declaration of encryptData, decryptData, encryptFile,
decryptFile is same */
/* System Call   for use library   */
public declare Sub CopyMemory Lib "Kernel32" Alias
"RtlMoveMemory"

/* constant value for authentication */
```

Fig. 1. Import function declared within DLL

```
Dim ret As Integer
ret = encryptFile("a", "1111",
AUTH DIGITAL ID ICC, ALG SEED)
```

Fig. 2. User Authentication

```
ret = encryptfile(inFileName, outFileName)
ret = decryptfile(outFileName, decFileName)
```

Fig. 3. File encryption/decryption

```
/* encryption binary data declaration for use
   encryptData */
Dim inData(256) As Byte
indata(0) = &H1
...
/* pointer declaration for store output encryption result */
Dim inLength As Long
inLength = 5
Dim outData_ptr As Long
/* pointer declaration for store encryption binary data */
  inData_ptr =Varptr(indata(0))
/* binary data encryption */
ret = encryptData(inData_ptr, inLength, outData_ptr,
outLength)
/* function copy contents of point into byte array*/
Dim outData(256) As Byte
call      memcopy_from_ptr_to_byte_array(outData_ptr,
outData, outLength)
```

Fig. 4. Binary data encryption/decryption

3) Network security system

SSL has the record protocol and handshake protocol. SSL record protocol consists of the handshake protocol and other high level protocol encapsulation ability. SSL handshake protocol helps authenticate the user, maintains the TCP/IP connection and security algorithm and encryption key agreement during the server-client connection within the war game simulation program. War game simulation network security library's components are show in Table 1. It mainly consists of server modules and client modules. The components help connect, transmit, and disconnects the connection between the server and the client. It also consists of the function to encode the data sent between the two sides within the war game simulation system.

Table 1. Network security library

Class	Module name	Explanation
Server module	int CQSSL_server_init (char* config_file)	Initiating a secure communication session from the server program to the client program.
	SSL* CQSSL_server_accept (int client_sock)	Server program that sets up the secure connection for the client
	void CQSSL_server_close (SSL* con)	Server program that closes the client connection
Client module	int CQSSL_client_init (char* config_file)	Client program that initiates the communication session with the server program
	SSL* CQSSL_client_connect (int client_sock)	Client program that sets up the secure connection
	void CQSSL_client_close (SSL* con)	Client program that closes the secure connection
Common module	int CQSSL_write (SSL* con, const void* buf, int num)	Transmits data through the secure connection to client or server program
	int CQSSL_read (SSL* con, void* buf, int num)	Receives data from the secure connection
Aid module	void CQSSL_con_init(void)	Initializating SSL and socket mapping table
	int CQSSL_con_add (int sock_fd, SSL* con)	Adding a SSL socket into the mapping table
	int CQSSL_con_del (int sock_fd)	Deleting a SSL socket from the mapping table
	int CQSSL_con_find (int sock_fd)	Finding a SSL socket_fd index from the mapping table
	SSL* CQSSL_con_get _by_sock	Returns the SSL pointed by the pointer
	SSL* CQSSL_con_ get_by_idx(int idx)	Different from CQSSL_ con_get_by_sock, it returns the SSL in the table index
	int CQSSL_set_write _socket (SSL* con, int write_socket)	A function that makes the SSL to use write_socket

5. Experimental results and analysis

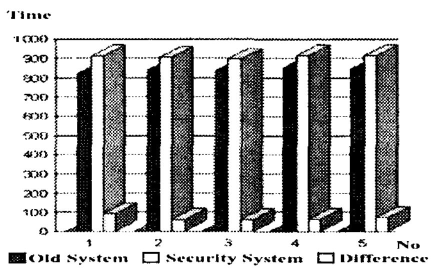
War game simulation security system has been tested and evaluated within the war game environment and compared with the original system without the security system. Results may differ from different system performance status.

1) Performance evaluation of network security

Table 2. Test procedures/data

Test procedure	Order Number	Transmition Data	Unit
Replay Run	20,220	89,726 kbyte	Second

The result of operating 20,220 commands and repeating it 5 times within the developed system has shown the average time result of 70.4 second. The operation time is short and there is virtually no overhead cost. The result shows that the developed system is feasible for usage.



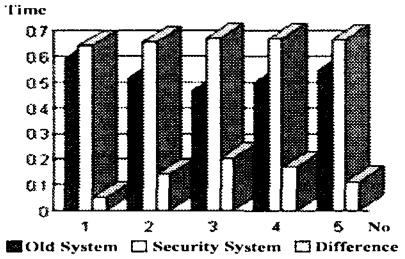
No	Old System	Security System	Difference
1	821	912	91
2	841	904	63
3	836	897	61
4	852	917	65
5	843	915	72
Average	838.6	909	70.4

Fig. 5. The results of performance evaluation of network security

2) Performance evaluation of data security

Table 3. Test procedures/data

Test procedure	Data amount	Data size	Unit
Encryption image display	1:50000 Map 20 unit	1:50000 184 kbyte	second



No	Old System	Security System	Difference
1	0.593750	0.640625	0.046875
2	0.515625	0.656250	0.140625
3	0.468750	0.671875	0.203125
4	0.500000	0.671875	0.171875
5	0.550000	0.663375	0.113375
Average	0.550000	0.663375	0.113375

Fig. 6. The results of performance evaluation of data security

Security System will display the 1:50000 maps 20 encrypted map images to the screen. The test result shows that on average of 0.11 second from displaying the two different kinds of map. It is considered as short time cost and viable for usage.

6. Conclusions

The data being used in the war game simulation are military sensitive data and needs to be controlled and protected. Especially the map and geographical information and military base data used in the simulation are not managed and protected from security weakness and processed danger to data being stolen. And thus a security system is needed to maintain and control and protect the information from being breached and data stolen. This essay has analyzed the faults and loopholes in the security within the war game simulation system and has shown the implementation and design that needs to be implemented to protect the data. War game simulation system's security system can be divided mainly into three categories: user authentication system, encryption system, and network system. The user authentication system has been implemented with ID/PASSWORD management system and digital ID system. Encryption system is implemented with national standard algorithm SEED within the client System. SEED is considered as usage friendly and implemented as client side s/w encryption library format. And SSL is used for the design and implementation of the network security system.

The test result shows that there is no overhead from implementing the new security system and has proven to protect the military secret information successfully.

References

[1] Matt Bishop, 2002. Computer Security Art and Science, *Addison-Wesley.*

[2] Ben Galbraith, et. al., 2002. Professional Web Services Security. *Wrox.*

[3] Alan O. Freier, Phillip Karlton, Paul C. Kocker, 1996. The SSL Protocol version 3.0, *Netscape.*

[4] Jin Soo Kim, 2003. A-MEDIAS: Concept and Design of an Adaptive Integrating Event Notification Service, *PhD Thesis.*

[5] William Stallings, 2003. Cryptography and Network Security-Principles and Practices, *Prentice Hall.*

[6] John Cheesman, John Danieless, 2001. UML Component-Based Software(The Component Software Series), *Addison-Wesley.*

[7] Zhiqun Chen, 2000. Java Card Technology for Smart Cards. *Addison-Wesley.*

[8] Uwe Hansmann, Marin S. Nicklous, Thomas S. Nicklous, Frank Seliger, 1999. Smart Card Application Development Using Java, *Springer.*

[9] IPHIGHWAY, Inc., 2002. Introduction to Policy-based network and quality of service. *http://www.iphighway .com.*

[10] B. Moore, E. Ellesson, J.Strassner, A. Westerinen, 2001. Policy Core Information Model – Ver. 1 Spec., *IETF RFC3060.*