Computing and Informatics, Vol. 30, 2011, 419–428

DESIGN AND IMPLEMENTATION OF AN INTRANET SECURITY AND ACCESS CONTROL SYSTEM IN UBI-COM

Malrey Lee

Center for Advanced Image and Information Technology
School of Electronics & Information Engineering
ChonBuk National University
664-14, 1Ga, DeokJin-Dong, JeonJu, ChonBuk, 561-756, Korea
e-mail: mrlee@chonbuk.ac.kr

Nam-Deok Cho

School of Computer Science & Engineering
Chung-Ang University, Heukseok-dong, Dongjak-gu, Seoul, Korea

Keun-Kwang Lee*

Department of Beauty Arts, Koguryeo College
Chonnam, Naju City, 520-713, South Korea
e-mail: kklee@kgrc.ac.kr

Kyoung-Sook Ko

Department of Beauty Design, WonKwang University
Lksan Chonbuk, 570-749, Korea
e-mail: koks31@wku.ac.kr

Abstract. Currently, most enterprise intranet systems process user information for security and access authentication purposes. However, this information is often captured by unauthorized users who may edit, modify, delete or otherwise corrupt this

* corresponding author

data. In addition, corruption can result from inaccurate communication protocols in the web browser. Therefore, a method is needed to prevent unauthorized or erroneous access and modification of data through the intranet. This paper proposes an efficient security procedure that incorporates a new model that allows flexible web security access control in securing information over the intranet in UC. The proposed web security access control system improves the intranet data and access security by using encryption and decryption techniques. It further improves the security access control by providing authentication corresponding to different security page levels relevant to public ownership and information sensitivity between different enterprise departments. This approach reduces processing time and prevents information leakage and corruption caused by mistakes that occur as a result of communication protocol errors between client PC's or mail security methods.

Keywords: Web security access control system, intranet security system, encryption, communication protocol, cooperation system, UC (Ubi-Com)

1 INTRODUCTION

The Internet, which is a distributed and open system, provides access to diversified information created by various organizations and individuals and is geographically distributed worldwide. The Internet, a hypermedia system, is commonly used as the first source of information because downloading text, audio and graphical information is so convenient. Corporate intranet users need to develop systems to share information in virtual space through the Internet without risking the security and integrity of their data. Many enterprises share and reuse information through the intranet. However, the intranet systems, which provide many types of service, need to incorporate solutions for security and access control [5, 6, 8]. In order to provide this type of corporate system, the Basic Support Cooperative Work (BSCW) system and Domino system have been developed [9] and integrated into a new model and system called SecuIntranet.

Currently, most enterprise intranet systems process user information for security and access authentication. However, unauthorized users often capture this information and may edit, modify, delete or otherwise corrupt this data. Additionally, corruption can result from inaccurate communication protocols in the web browser. Therefore, a method is needed to prevent unauthorized or erroneous access and modification of data through the intranet. This paper proposes an efficient security procedure that incorporates a new model and allows flexible web security access control in securing information over the intranet. The proposed web security access control system improves the intranet data and access security by using encryption and decryption techniques. It further improves the security access control by providing authentication corresponding to different security page levels relevant to public ownership and information sensitivity between different enterprise departments. This approach also prevents information leakage and corruption by mistakes

that may occur as a result of communication protocol errors between client PC's or mail security methods. The SecuIntranet method encodes web pages whenever the client request intranet server information. This encoding model is not an external program. To save processing time, this method utilizes API for encoding processes and ActiveX control for decoding processes. Installation of these encryption and decryption programs on the existing web system is required for implementation and use.

This paper is organized according to the following structure: Section 2 presents related works and some basic descriptions for similar security and access control systems; Section 3 presents the detailed design of SecuIntranet; Section 4 discusses the development procedure and results of the implementation; and, finally, the conclusion is presented in Section 5.

2 INTRANET SECURITY AND ACCESS CONTROL SYSTEMS

2.1 Channel Based Web Security Method

This method is the encoding technology that adjusts the TCP/IP connection, which exists between the http layer and the TCP/IP layer, and sends the messages to http. SSL, which was developed by Netscape, is a standard for web security system protocols [1, 2]. The SSL secure socket layer, as shown in Figure 1, describes the hierarchical model in which SSL exists between the Internet application layer and the TCP/IP layer. SSL can adapt to http, telnet, FTP and other application protocols. However, SSL cannot provide digital text signature translation in business market applications.

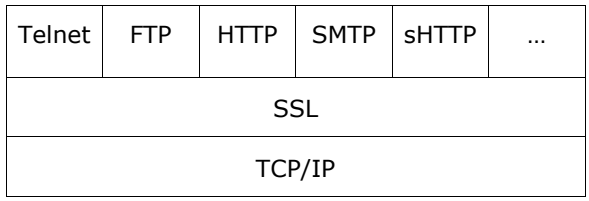


Fig. 1. SSL hierarchical model

2.2 Content Based Web Security Method

This method is an implementation for security in the http layer using the existing coding system. Also, this method needs to have extra encoding and decoding process programs installed on the server and web browser. Figure 2 shows the structure of this method, which uses an external program in order to implement system security. This method can perform the system security without modifying the existing encoding system. An external program is used to require http to encode and decode the

response messages. The advantage of this external program is that there is no need to modify the requirements of the existing encoding and decoding system. However, the external program is located in the Internet application layer and requires additional processing time [4].

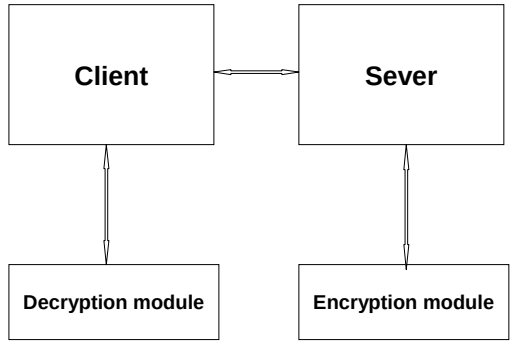


Fig. 2. External program implementation

2.3 Access Control Matrix (ACM) Model

The ACM security model, where a subject represents a user and an object represents a web page, is shown in Figure 3. As shown in Figure 3, subject1 has no authority to read, write or execute object1 but it does have the authority to execute and read object3 [3, 7, 10]. Similarly, in row 2 of Figure 3, subject2 authority is shown. Different authority is assigned to users according to their defined access level. Each department of the enterprise defines these access levels according to the sensitivity of the document.

	Object1	**Object2**	**Object3**
Subject1	-	(execute)	(execute, read)
Subject2	(read, write)	(execute)	-

Fig. 3. Access Control Matrix (ACM)

3 SECUINTRANET SECURITY SYSTEM DESIGN

This paper proposes a system to prevent corruption of information and to control access according to different users' security level in the enterprise. This system performs in a basic client/server environment and is installed on an existing intranet system. Also, authorized users can see encoded server web pages, when permitted by their security level. The installed client decryption program decodes these web pages. The decoded web pages allow access according to users security permissions. Figure 4 shows overall structure of the system.

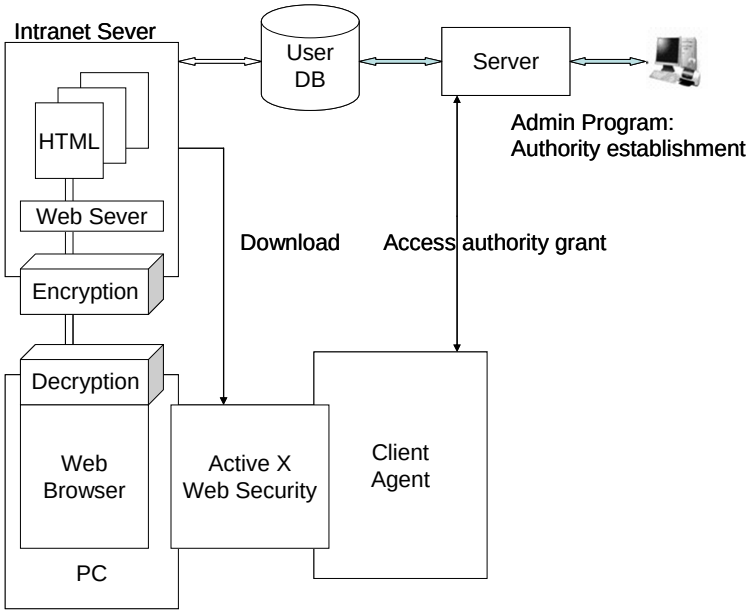


Fig. 4. SecuIntranet design model

3.1 Authentication of Users

Authentication of users uses the logins that exist on the enterprise intranet. Users login through the browser and the server provides access authentication using authorized ids. Even if the user passes the login, the user cannot access the system if they have no authentication for reading. Authentication of the user requires two steps. The first step is comparison of the user information database on the intranet authentication server to the user login information. Next, the specific access authority for the user and the requested web pages is evaluated for access. Unauthorized server seeking information from the Internet has sets of access authentication to the

intranet system, thereby securing information from unauthorized external Internet access.

3.2 Encryption and Decryption for SecuIntranet

If authentication is permitted, the intranet server sends the required web page to the client. The SecuIntranet system includes the requested web pages using a call to the encoding API. Figure 5 shows the encoding program prototype. Text strings in the web pages are encoded by providing an input value to the source string and returning the result as shown in Figure 5. To encode the whole web page, the file pathname is given as the input value to the source string as shown. The Rijndael algorithm, which was developed by Joan Daemen and Vincent Rijmen in 2000, is used to encrypt and decode the information in each web page [11]. This algorithm can process specified block sizes and provides a high level of security for many types of computer environments. SecuIntranet uses the Cipher Block Chaining (CBC) operation mode of the algorithm. The CBC mode provides fast encoding and decoding through keyed encoding of the first block using an initial vector and XORing operations upon subsequent blocks of data.

Depending on the sensitivity of the information in the web page, either the whole page is encoded or only parts of the web page. This ensures the security of the web page when it is downloaded to client's PC. In this system the downloaded web page can be decoded using ActiveX control that is installed on client's PC. After the web page is decoded it can be read by the browser. Because this system provides encoding only to security sensitive portions of the web page, the requisite processing time for encryption and decryption can be reduced significantly.

```
function FileEncrypt()
{
   var vRe = DSSLATL.RequestFileEncrypt (source_string, Authority, dest_sting);
}
// source_string : data for encryption
//Authority : user authority information
//dest_string : result data for encryption
```

Fig. 5. Encoded API program prototype

3.3 SecuIntranet Authentication Control

Authorized users can get permission or limit the permission assigned during server authentication. The list of control in Figure 6 shows the method of assignment used for server access control that manages the authorization of departments using

the intranet system. The program administrator manages the lists containing the information for program authentication and users for security and access control.

Read	**Read the Web Page**	**0) Disable 1)Enable**
Print	**Print the Web Page**	**0) Disable 1)Enable**
Source Viewing	**Source Viewing of the Web Page**	**0) Disable 1)Enable**
Edit	**Edit the Web Page**	**0) Disable 1)Enable**
Capture	**Capture the Web Page**	**0) Disable 1)Enable**

Fig. 6. List for access control

4 SECUINTRANET IMPLEMENTATION

Figure 7 demonstrates an encoded web page beginning with the marker $swsmanstarts$ and ending with the marker $swsmanend$. If the web pages do not need complete encoding, the start points and end points can be used to begin and end partial encoding. Figure 8 shows a web page that is viewed by unauthorized users. This system also needs a program administrator to allow decoding privileges.

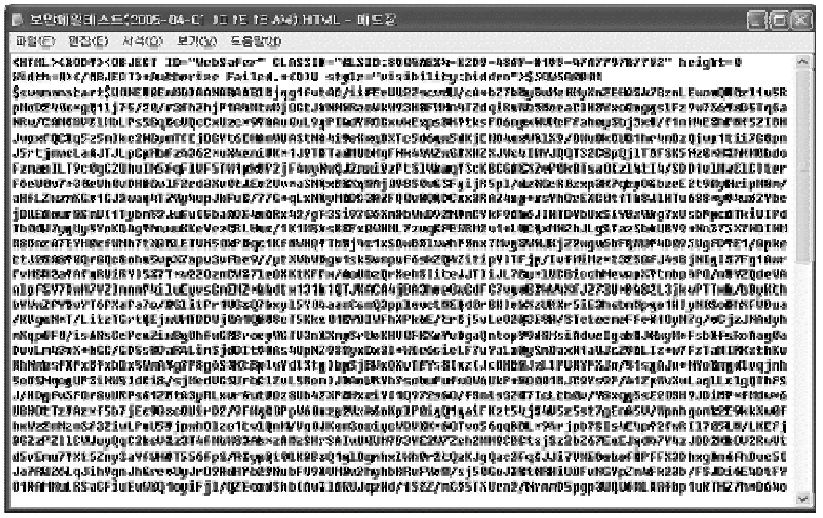


Fig. 7. Encoded web page

Figure 9 shows the authentication Window for the program administrator to set permissions for reading, printing, source viewing, capturing and writing web pages. The encoding module adjust in this system is an API, not an external

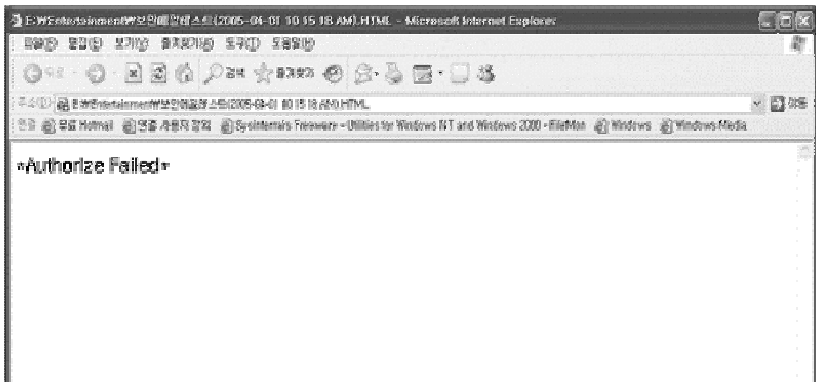


Fig. 8. Example of unauthorized user web page view

program. Therefore, the encoding time is faster than existing intranet systems. Also, this system provides many functions and prohibits the access of information by unauthorized users.

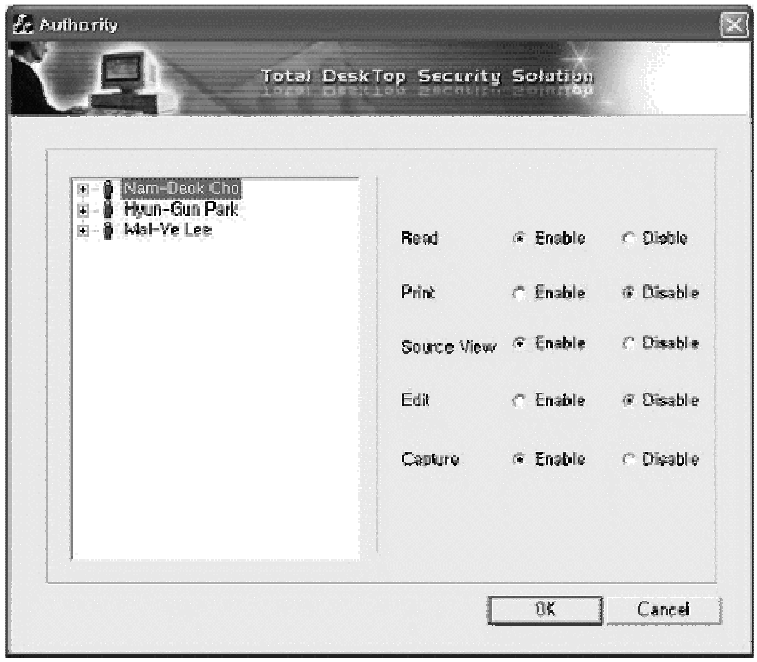


Fig. 9. Program administrator window

5 CONCLUSION

In this paper, a method providing web page access control for departmental security in existing intranet systems is presented. The proposed web security and access control system improve the intranet data access security by using encoding and decoding. Further, the system improves the security access control by providing authentication corresponding to different security page levels relevant to the data sensitivity identified by each enterprise department. This approach also prevents information leakage and corruption caused by mistakes occurring as a result of protocol interface errors in client's PC. Also, encoding is performed by an API intranet program, not by an external program, thereby reducing the processing time. In the future, this research will be extended to evaluate each document in the enterprise and identify those documents with identical information and eliminate redundancies.

Acknowledgments

This work was supported by grant from Yu-dang Jisung Yang Memorial Fund, 2010.

REFERENCES

[1] Freier, A.—Karlton, P.—Kocher, P.: The SSL Protocol Version 3.0. `http://www.netscape.com/eng/ssl3/3-spec.ps`, 1996.3.

[2] Rescorla, B. et al.: The Secure HyperText Transfer Protocol. RFC 2660, 1999.8.

[3] Eckert, C.: On Security Models. International Conference on Information Security, p. 29–38, 1996.

[4] Weeks, J. et al.: CCI-Based WebSecurity: A Design Using PGP. WWW Journal 95, pp. 57–69, 1995.

[5] Kang, S. G.: Web Security and Payments. WWW-KR Workshop, Vol. 4, 1996, pp. 6–122.

[6] Kang, S. G.—Park, J. S.: Web Security Technical. Journal of Korea Information Processing, Vol. 7, 2003, No. 2, pp. 23–30.

[7] Kim, Y. S. et al.: Cooperation System based on Web for Document Security. Journal of Korea Information Processing, Vol. 9, 2002, No. 2, pp. 11–20.

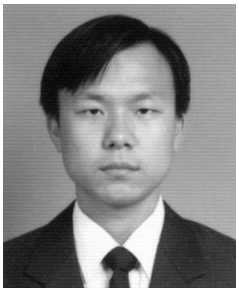
[8] Park, J. S. et al.: Web Security Technical and Future. Journal of Korea Information Science, 1997, pp. 78–88.

[9] Bently, R.: Basic Support for Cooperative Work on the World Wide Web. International Journal or Human Computer Studies, 1997, pp. 121–128.

[10] Dierks, T. et al.: The TLS Protocol 1.0. RFC2246, 1999.1.

[11] Jamil, T.: The Rijndael Algorithm. IEEE Potentials, Vol. 23, 2004, No. 2, pp. 36–38.

Malrey Lee received a Ph. D. in Computer Science from the University of Chung-Ang. She has been a Professor at the Chon-Buk National University in Korea. She has over forty publications in various areas of computer science, concentrating on artificial intelligence, robotics, medical healthcare and software engineering.



Nam Deok Cho received a Ph. D. in Computer Science from the University of Chung-Ang. He has been a researcher at the Security research Center in Korea. He has many publications in various areas of computer science, concentrating on artificial intelligence, robotics, medical healthcare and software engineering.

Keun-Kwang Lee received a Ph. D. in Applied Biology from the University of Doung-guk. He has been a Professor at the Koguryeo College in Korea. He has over ninety publications in various areas of biology, beauty and healthcare. Now he is concentrating on hybrid artificial intelligence with healthcare, biology and beauty.

Kyoung-Sook Ko received a Ph. D. in Public Health from the University of HanNam. She has been a Professor at the Wonkwang University in Korea. He has over ninety publications in various areas ofBeauty, and healthcare. Now she is concentrating on Hybrid Artificial Intelligence with Healthcare, and Beauty.