A Design of the Digital Content Distribution System based on the Public key and the Hierarchical Web Caching Structure

Yun Ji Na[1], Ko Il Seok[2], Gun Heui Han[3]

[1] Department of Internet Software, Honam University, Gwangju, Korea, yjna@honam.ac.kr
[2] Dept. of Information & Communications Engineering, Chungbuk Provincial University of Science & Technology, Chungbuk, Korea, isko@ctech.ac.kr
[3] School of Information Communication, Cheonan University, 115 Anseo-dong, Chonan, 330-704, S. Korea, hankh@cheonan.ac.kr

Abstract. The illegal distribution of duplicated contents on the Web is causing digital content providers great economic loss. Therefore, Information security is becoming a more important factor in distribution of digital contents. In this study, we designed a digital contents distribution system based on the public key techniques in hierarchical web caching structures. The superior performance of the proposed system has been proven in the experimental tests. The results of experiment show that the supposed system improved the security of DC without decreasing process speed and improved user convenience.

1. Introduction

Security problems occur because the Internet is a transmission medium that does not consider security problem. Moreover, as the most server systems are exposed to threats of illegal invasion and data destruction, threats of hacking or cracking become worse. Therefore, security techniques for the protection of server systems and digital contents are required for the safe distribution of digital contents. Distribution of contents duplicated illegally in the Internet is causing great economic loss to the digital contents providers. Therefore, a study for security and efficient distribution of digital contents is required [1,2,3].

Generally, for the safe distribution of digital contents, plaintext is transmitted through an encryption process to convert the data into cipher text. On this process, the size of encrypted digital contents is grows, it causes a transmission delay as network traffic increases and increase response delay. Thus, we consider user convenience, execution speed and security in the design of a digital content distribution system.

In this study, we designed a secure and efficient digital contents distribution system based on a public key in a hierarchical web caching structure. We use web caching technology [4] to decreasing of network delay, and use the RSA encryption / decryption technique to improve security and efficiency. Experimental tests verified performance superiority of the proposed system. The experiment results show that the proposed system has improved the safety of the DC while not decreasing the process speed.

2. System design

Figure1 shows the configuration of the system. SPSM(Secure Proxy Server Manager) is an administrator managing a proxy server of the DCUG. DC means Digital Contents and DCP means Digital Contents Provider, DCUG means Digital Contents User Group.

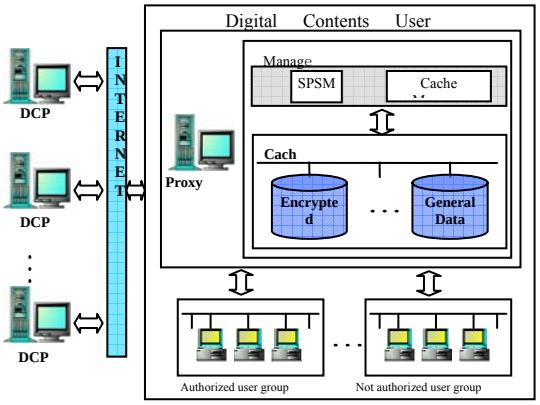

Figure 1. System structure

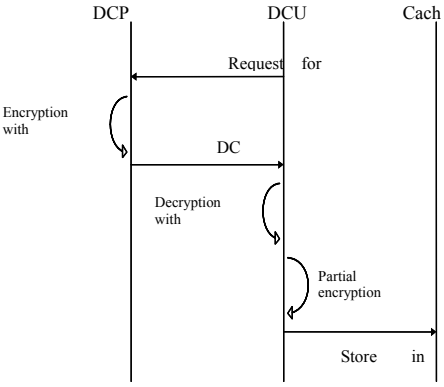

Figure 2. DC transmission

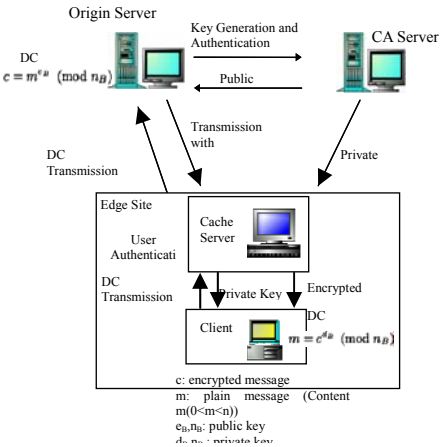

Figure 3. Authentication procedure

2.1 DC transmission and Authentication

Figure 2 is a procedure transmitting the DC from the DCP to the DCUG. The DCP server encrypts the DC, which includes the public key. By using a private key, the DCUG decrypts the DC transmitted from the DCP and makes the original public key and plaintext. 10% of these decrypted contents with a public key is partially encrypted and saved in the cache of the DCUG. These contents are decrypted with a personal key in the user browser. The proposed system has system side security and process

side security for the secure execution of contents. System side security can be attained through the security of the proxy server. It also has process side security by approved user certification on a system (the DCUG manager) and certification of private key value on the execution time (user browser). If a permitted user of the DCUG cannot find the desired contents in the cache list, the DCUG must transmit the contents from the corresponding DCP server. The DCUG and the DCP server must receive a certification statement to CA (Certificate Authority) server before exchanging encryption data. Figure 3 shows Authentication procedure for the system.

2.3 DC transmission from DCUG

If an approved user of the DCUG requests contents, the DCUG manager transmits the partially encrypted DC in the encrypted contents cache scope to a user. A user decrypts the transmitted DC and a player in the personal Browser executes this DC. Figure 4 is a procedure to transmit contents from the DCUG to the DC.

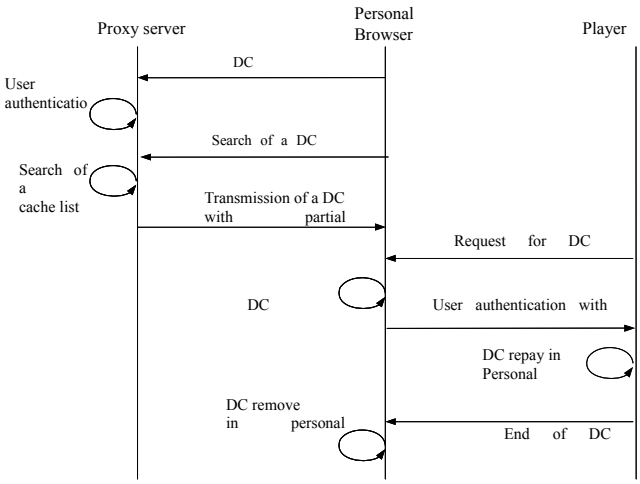

Figure 4. DC transmission and replay

When DC transmission is requested, User certification is performed in the system. Then the DC is searched in a cache list. And when the cache is accessed, pertinent contents are transmitted. And DC decryption is performed in a personal Browser after transmission is completed. A user certification procedure is performed with a key value, and DC is replayed. Finally, DC is deleted from a user area after replay is completed

3. Comparison to Other Systems

We compared the proposed system with SecuMAX and Digicap, which are the existing popular commercial systems to verify the superiority of the proposed system.

Table 1 shows the comparison of the security level between two commercialized systems and the proposed system.

Table 1. DC security: proposed system vs. Existing Commercialized system

Items \ System	SecuMAX	Digicap	Proposed system
Authentication method	Personal encryption key	Token	Public key method
Security on contents illegality currency	×	×	○
Hierarchical Approach	×	×	○
Web Caching	×	×	○
User browser	○	○	○

In most commercialized systems, a user's personal interface is supported for security and user convenience. Table 1 shows that a commercialized systems' DC security level is decreased for the improvement of processing speed. It is difficult to improve process speed and DC security level at the same time only through encryption and personal interface technique. The two commercialized systems work better than the proposed system when web caching is not applied. But the proposed system works better for security and performs faster when web caching is applied.

4. Conclusion

The proposed system decreases the delay factor caused by network traffic by using web caching and uses a hierarchical structure encryption / decryption technique in order to improve the security level of the DC. The experiment results show that the proposed system has improved the safety of the DC while not decreasing the process speed. The proposed system could be used for an ISP (Internet Service Provider) that distributes mass multimedia digital contents like online education, web movies, and web music contents

References

1. R. Iannella, "Digital Rights Management Architecture," *D-Lib Magazine, Vol. 7, No.6*, June, 2001.
2. Spctral Lines, "Talking About Digital Copyright," *IEEE Spectrum, Vol.38 Issue;6, pp.9*, June 2001.
3. Thorwkrth N. J., Horvatic P., Weis R., Jian zhap, "Security methods for MP3 music delivery," Signals, Systems and Computers, *Conference Record of the Thirty-Fourth Asilomar Conference on, Vol.2, pp.1831-1835,* 2000.
4. G. Barish, K. Obraczka, World Wide Web Caching: Trends and Techniques. *IEEE Communications, Internet Technology Series,* May 2000.