실행속도와 보안성을 고려한 공개키 기반의 디지털콘텐츠 분배

고일석[*], 조동욱[**], 나윤지[***], 임춘성[****]
[*,****]연세대학교 컴퓨터산업시스템공학과
[**]충북과학대학 전자상거래과
[***]충북대학교 컴퓨터공학과
e-mail:isko0326@korea.com

Distribution of Digital Contents based on Public Key Considering Execution Speed and Security

Il-Suk Ko[*], Dong-Uk Cho[**], Yun-Ji Na[***], Chun-Seong Leem[***]
[*,****]Dept of Computer and Industrial Eng., Yonsei Univ.
[**]Dept of Information Communication Eng., Chungbuk Provincial Univ. of Sci. and Tech.
[***]Dept of Computer Eng., Chungbuk National Uni.

Abstracts

]Information security is becoming a more important factor in distribution of digital contents. Generally, illegal facsimile of high-quality multimedia products such as DVDs, MP3s and AACs is possible without damaging quality. Thus, the illegal distribution of duplicated contents on the Web is causing digital content providers great economic loss. Therefore, a study of security and efficient distribution of digital contents is required.

The most important issues in the design of a digital content distribution system are user convenience, execution speed and security. In this study, we designed a digital contents distribution system that uses web caching technology and encryption/ decryption techniques in hierarchical structures. We propose a digital content distribution system that improves user convenience, security and execution speed. The superior performance of the proposed system has been proven in the tests. The results of experiment show that the developed system has improved the security of DC without decreasing process speed.

1. Introduction

Generally, for the safe distribution of digital contents, plaintext is transmitted through an encryption process to convert the data into cipher text [1,2]. In this process, the size of encrypted digital contents is larger than the size of plaintext. This increase the size of digital contents causes a transmission delay as network traffic increases. Ultimately, this traffic increase delays user speed, as well. Also, the increase in size of digital contents through encryption increases decryption time, and this becomes a delay factor in digital contents execution. Thus, the most important issue in the design of a digital content distribution system is user convenience, execution speed and security.

In this study, we designed a secure and efficient digital contents distribution system based on a public key that improves security, execution speed and user convenience. The proposed system uses web caching technology for the decrease of network delay and uses a hierarchical structure encryption / decryption technique to improve security and efficiency. 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. Contents security technologies

Web security protocol and the encryption / decryption algorithm of plaintext data are required for the guarantee of reliability and security between the clients and servers on the web [1,2]. There is a method which encodes and transmits the whole message on an application layer, and a method which encodes and transmits only the parts of whole message on the web security protocol. Currently, a method like SSL (Secure Socket Layer) is widely used [3]. This method encrypts the DC by inserting an additional encryption layer between the application layer and the transport layer. We need the authorization procedure on CA (Certificate Server) between a client and a server in order to obtain reliability and security. In this process, a set of user data is a certification statement. The most widely used certification statement is X.509 of ITU-T [4].

The DES (Data Encryption Standard) developed in the United States is a 64 bit symmetry key algorithm [5], and each country of the world develops its own IDEA, FEAL, RC-5 algorithm. In Korea, SEED, a 128-bit- symmetry-key-algorithm, has been established as the national standard [6].

Two different keys are used in the public key encryption method. The key used for encryption is the public key and the key used for decryption is the secret key (private key). In the public key encryption method, the public key is open, while the secret key is kept secret [1,7].

In a web security system based on the public key, an encryption channel is made up after authentication of a client and a web server is finished, and a public key and a private key are used when the contents are exchanged. Many algorithms were released after a public key concept was released. Currently RSA and Diffe-Hellman are considered the most secure algorithms. However, an RSA public key algorithm has been widely used in a commercialized web base security system [7]. The time required for encryption / decryption computation in the RSA method is longer than the time required in the symmetry key method. However, the public key method is used more in many commercialized systems than the symmetry key method because of the convenience and safety of the key distribution.

3. System design

3.1 Encryption

The DCUG(Digital Contents User Group) of layer 2 is operated as a client of the DCP(Digital Contents Provider) server of layer 1. These content transmissions between two classes are performed through the Internet with no security. Therefore, the secure encryption technique whose security is verified is indispensable in contents transmission between the DCP and the DCUG. We use the RSA public key technique for safety and efficiency of key distribution in the experiment for the proposed system. The DC encrypted in layer 1 with a public key becomes a decryption by the personal key in the DCUG of layer 2. The DCUG partially encrypts only 10% of the contents with a public key on the decrypted DC plaintext, and saves it in a cache. Transmission between layers 2 and 3 is a transmission with system security on an intranet. Layer 2 provides the partially encrypted contents only to approved users.

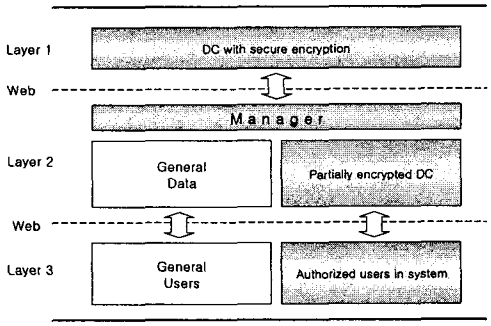

Figure 2. Encryption/decryption layered structure

3.2 DC transmission

Figure 3 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).

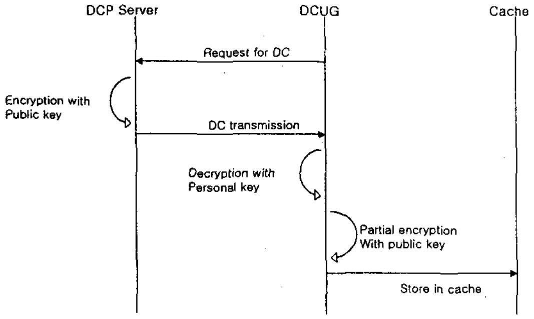

Figure 3. DC transmission

3.3 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.

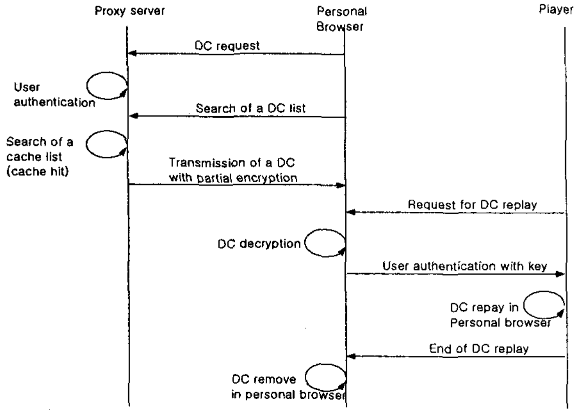

Figure 4. DC transmission and replay

1) DC transmission is requested.

2) User certification is performed in the system.

3) The DC is searched in a cache list. And when the cache is accessed, pertinent contents are transmitted.

4) DC decryption is performed in a personal Browser after transmission is completed.

5) A user certification procedure is performed with a key value

6) DC is replayed.

7) DC is deleted from a user area after replay is completed

3.4 Authentication procedure

The publication procedure of a certification statement is as follows.

1) CA server is accessed.

2) A certification statement to CA server is requested.

3) CA server transmits an authentication request statement to the DCUG and the DCP server

4) The DCP server and the DCUG generate a distinct key pair and compose a authentication request statement.

5) The DCUG and the DCP server transmit a distinct key and authentication request statement to CA server.

6) CA server confirms the received authentication request statement and publishes a certification statement which includes a public key.

7) CA server saves authentication request statement information, a certification statement of the DCUG, and the DCP server in DB

8) CA server transmits a certification statement to the DCUG and the DCP server.

9) The DCUG and the DCP server save the certification statement which was received from CA server together with their own secret key

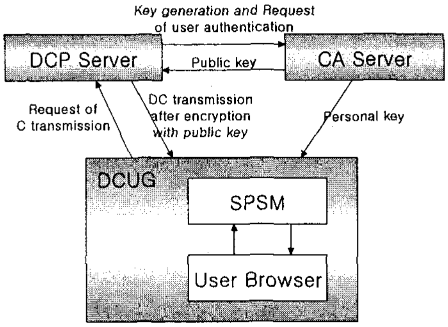

Figure 5. Authentication procedure

A certification statement includes publisher signature, serial number, publisher, issue date, due date, owner, and owners public key as basic structure necessary for authentication. Publisher signature and a publisher in a certification statement format are the fields related to CA. Using these fields, the CA ensure that a key in the certification statement in fact belongs to the owner of the statement. Each certification statement includes a public key of an owner. Therefore, the public key can be used for the encryption of data to be transmitted to the owner of a certification statement. Also a certification statement includes publishers digital signature of the CA. Therefore, this is to guarantee reliability of the saved information and that the certification statement is not modified. When the DCP server encrypts contents, a public key is used as in Figure 5. A personal key(a private key) is provided to the DCUG and the user.

4. Analysis

The proposed system is a contents distribution system with improved user convenience, execution speed, and security that are the principal issues of a digital contents distribution system.

4.1 Speed

A speed influence factor of a digital contents distribution system is a time delay caused by network traffic and decryption in the user interface. The file size of the original DC grows larger through encryption. Moreover, the encryption transmission of large-sized multimedia contents such as MP3 increases network traffic radically. The proposed system improves this delay factor. Contents encrypted safely with a public key at the DC server are transmitted to the DCUG. The transmitted DC is decrypted with a personal key partially encrypted again, and saved in a cache. Finally, the DC saved in a cache is provided to an approved user of the DCUG. Therefore the user time delay caused by the influence on Internet traffic is decreased. Also, execution time decreases because the user interface decrypts the partially encrypted contents.

4.2 Security

A digital contents distribution system must have transmission security and execution security. In the proposed system, the DC server transmits contents encrypted safely with the RAS public key method, through which security was verified to the DCUG. Therefore the DCUG, which has a private key, has transmission security because it can only decrypt the transmitted DC. Moreover, the proposed system has security for the secure execution of contents. Because the DCUG is established by proxy server, security can be ensured by the system itself.

Cache list access is permitted only to the approved users of the DCUG through user authentication. For the user interface to execute the DC, the decryption of the DC is needed. And at this time, only the user who has the key can decrypt the DC, thus giving the proposed system additional security.

5. Conclusion

In this study, we designed a digital contents distribution system based on a public key that improved security, execution speed, and user convenience. The proposed system decreases the delay factor caused by network traffic by using web caching. It also uses a hierarchical structure encryption / decryption technique in order to improve the security level of the DC. Through experiments, we compared the process speed and security level of both the existing commercial systems and the proposed system. 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] W. Diffie and M. E. Hellman, "New Directions in Cryptography," *IEEE Transaction on information theory, Vol.IT-22*, no.6, Nov., 1976.

[2] Spctral Lines, "Talking About Digital Copyright," *IEEE Spectrum, Vol.38 Issue;6, pp.9*, June 2001.

[3] A. O. Freier, P. Karlton and P. C. Kocher, "The SSL Protocol Version 3.0," *www.netscape.com/eng/ssl3*, Nov. 1996.

[4] ITU-T Rec. X.509, Information technology-Open Systems Interconnection - The Dictionary: Public-key and attribute certificate framework, March 2000.

[5] National Bureau of Standard, *"Data Encryption Standard,"* FIPS Pub., 46, 1977.

[6] Korea Information Security Agency, A Development and Analysis Reoprt on 12bits Block Encryption Algorithm(SEED), 1998.

[7] R. Rivest, A. Shamir and L. Adelman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems," *Communications of the ACM, Vol.21, Nr.2*, 1978, pp.120-126