International Journal of Advanced Smart Convergence Vol.10 No.2 10-14 (2021)
http://dx.doi.org/10.7236/IJASC.2021.10.2.10

IJASC 21-2-2

A Study on the Contents Security Management Model for Multi-platform Users

Hansol Joo*, Seung-Jung Shin**

PhD student, Department of IT Convergence , Hansei University, Korea
Professor, Department of ICT Convergence, Hansei University, Korea
a20016@hansei.ac.kr, expersin@hansei.ac.kr

Abstract

Today people adopt various contents from their mobile devices which lead to numerous platforms. As technology of 5G, IOT, and smart phone develops, the number of people who create, edit, collect, and share their own videos, photos, and articles continues to increase. As more contents are shared online, the numbers of data being stolen continue to increase too. To prevent these cases, an authentication method is needed to encrypt the content and prove it as its own content. In the report, we propose a few methods to secure various misused content with secondary security. A unique private key is designed when people create new contents through sending photos or videos to platforms. The primary security is to encrypt the "Private Key" with a public key algorithm, making its data-specific "Timeset" that doesn't allow third-party users to enter. For the secondary security, we propose to use Message Authentication Codes(MACs) to certify that we have produced the content.

Keywords: *Contents Security, MAC, Timestamp, Public key, Private key*

1. Introduction

As shown in Figure 1, as telecommunications infrastructure and broadcasting converge, new types of digital content are emerging through various platforms. The population of digital content usage continues to grow exponentially with the rapid development of 5G, network transmission methods and mobile devices [1]. Therefore, contents theft has increased, the importance of security to protect contents, copyrights and watermarks becomes to be more considered [2]. Because "Leapfrogging phenomenon" of the mobile expands, making security management of content more urgent [3]. This study analyzes the security characteristics of the content management system of the platform. We would like to propose a security management model for multi-platform web contents with enhanced protection.

Manuscript Received: March. 22, 2021 / Revised: March. 25, 2021 / Accepted: April. 4, 2021
Corresponding Author: expersin@hansei.ac.kr
Tel: +82-10-3664-0666, Fax: +82-31-450-5172
Professor, Department of ICT Convergence, Hansei University, Korea

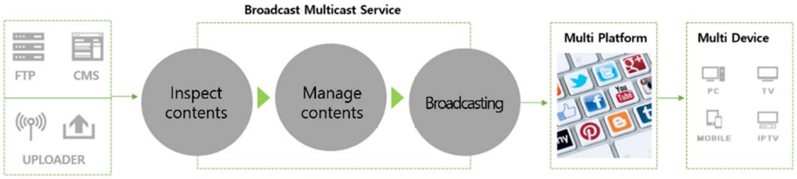

Figure 1. Process of the Content Utilization

2. Related Research

2.1 Asymmetric Key Algorithm

Table 1 shows the aspects of public keys and private keys. Public key algorithms disclose content and hide certain information, such as private key, so that it can only be known by itself. The characteristic of public key algorithms is that even when cryptographic algorithms and cryptographic keys are exposed, the decryption key cannot be calculated. One of these two keys is used for encryption and the other for decryption. It is impossible to steal this content because it is difficult to access it without the creator [4].

Table 1. Aspects of Public Keys and Private Keys

Public Key	Private Key
Same algorithm, different keys for decryption	Same algorithm and key for decryption
Key exchange not need (use public keys)	Exchange keys between recipients and sender
Keep one of the keys (private keys) confidential	Keep the shared keys confidential
Expose a public key	Hard to distribute keys
1000 times slower than private Key	1000 times faster than public key

Public key cryptography plays an important role in security management, because it verifies cryptocurrency transactions from computer system. Through interlinked private keys and public keys, the asymmetric cryptographic algorithm solves the security management problem raised in symmetric cryptography. Public key cryptography has been used as an authentication method for many purposes for years. In recent, a new security program is being used in the blockchain and cryptocurrency markets. Examples of public key algorithms include RAS, Elagmal, and DAS [5].

2.2 Message Authentication Code

In the Internet of Things (IoT) environment, encryption technology is widely used to prevent security threats providing encryption message authentication code and algorithm with integrity and confidentiality [6]. There are already several encryption technologies that have been verified for safety. Since it is difficult to apply the new technology to IoT mobile devices that have low quality of performance and power, many other types of lightweight encryption technologies have emerged. Interests of the block-type cryptographic algorithms steadily increase [7].

Message authentication code (MAC) is used for certification of message. The message is authenticated by inputting the secret key with the message authentication code (MAC) algorithm. The value of MAC protects the authentication of data by the verification procedure. MAC usage is shown in Figure 2.

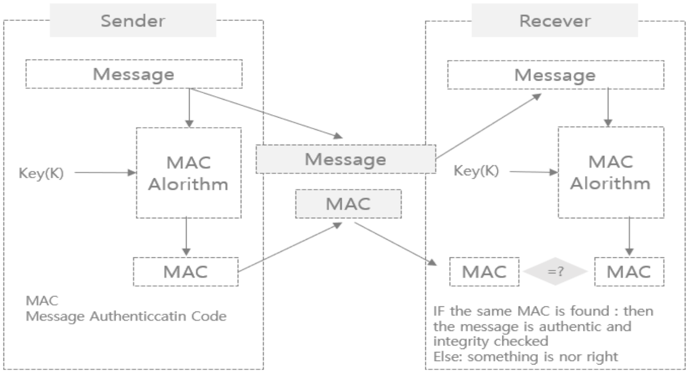
Sender
Message
Key(K)
MAC
Alorithm
MAC
MAC
Message Authenticcatin Code
Message
MAC
Recever
Message
Key(K)
MAC
Alorithm
MAC
=?
MAC
IF the same MAC is found : then
the message is authentic and
integrity checked
Else: something is nor right

Figure 2. Process of the MAC Exploitation

3. Changes and Applications of Content Management Systems

The Contents Management System (CMS) efficiently manages a lot of content collected in various ways. It has been optimized so that users can provide services in the desired form. It was used as an archival of common documents made in a common format used by all, so that many documents could be shared and used in convenience. Now, content is produced in digital form, regardless of usage field, therefore CMS has also evolved with digitization. The importance of the web continues to increase, as managing web contents and web sites has become more essential, thus, the Web Content Management System (WCMS) was introduced [8].

Strictly, CMS is a higher level including WCMS, but these days it is mostly used as an alternative term for WCMS. The CMS that most people currently use is in the form of blog software, recognized in opening and managing web blogs [9]. However, CMS is related to a series of content management processes that are carried out in order to process the accumulation, operation, management, distribution, etc. in stages for efficient use of contents. It creates, produces, collects, manages, and distributes various media contents according to various media types. In other words, it is a system that manages the entire content life-cycle from content production to use and disposal. In addition, CMS is a system that manages content within a company according to the purpose of the content platform company. In addition, it is developing into a system that can manage various types of contents that make up a website.

4. Suggestions of Security

A Timestamp refers to electronic information to which verification information at the time of occurrence of the record. It is added to verify the validity and authenticity of the record [10]. Electronic data can be easily forged and altered. Therefore, many problems can arise; how to check when data is newly created or changed. This can assist to confirm the evidence for a point in time using timestamps. Timestamping is a digitally signed value by encrypting a hash value of data and time that is currently occurring. The electronic document is stored at a certain point in time (the time stamp is issued) and thereafter, guaranteed to be unmodifiable by a trusted third party. After hashing the original text, it is encrypted with a private key.

As shown in Figure 3, Saving images after shooting with the mobile device camera, TimeStamp, that is displayed to verify that the data existed at some time, proves the interface of a specific mobile device connected to the network on the web and the location of the device. It stores the IP Address that acts as an authentication to display the message. In the process of transferring images between mobile devices, TimeStamp and IP Address engraved on the images can increase security.

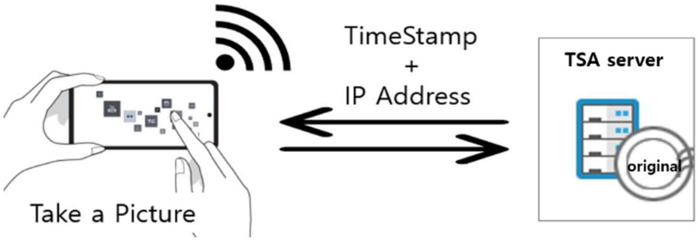

Figure 3. Example of using TimeStamp and IP Address built into Mobile devices

5. Conclusion

With the development of technology, various digital contents are being used in mobile devices. As the market size of digital contents grows, the broadcasting environment are expected to continue to change too. According to the content usage statistics, the scale of infringement due to illegally copied content is about 1.4 million cases, which is about 20% of the total content usage 6.9million cases. If we consider all the contents that have not been investigated as infringement, the scale of damage is expected to be greater. (2012). The emergence of personal media broadcasting services; such as IPTV (VOD), online video streaming (OTT), and web contents, and distribution platform, we intend to propose a model as above in accordance with the demand for supplementing the imperfections of security technology. In addition, multi-DRM and watermark technology according to the expansion of distribution environment, carving technology that measures the loss of additional information such as meter data and restores it to the original image, and proactive response through artificial intelligence monitoring technology and technology enhancement that applies self-do content recognition technology need.

References

[1] Seung-Jung Shin, "The Model Proposal of Mobile Cloud Security Technology," The Institute of Internet, Broadcasting and Communication (IIBC), Vol. 11, No. 6, pp. 151–156, Dec. 2011.
DOI: https://doi.org/10.7236/JIWIT.2011.11.6.151

[2] Cho, Jung-Won, "Digital Audio Watermarking System for Copyright Protection of Web Contents," Korea Academy Industrial Cooperation Society, pp. 558-560, 2006

[3] Shin, HyeWon and Ji, SeongWoo, "A Normative Study on the Paradigm and Solution of the New Digital Divide in the Smart Media Era," Study on the American Constitution, Vol. 25, No.3, pp. 171-203, Dec 2014.

[4] Seon-Joo Kim, "Secure Management Method for Private Key using Smartphon`s Information," The Korea Contents Society, Vol. 16, No. 8, pp. 90-96, Aug 2016.

[5] Wook-Lae Cho and Kyung-Wook Shin, "Scalable RSA public-key cryptography processor based on CIOS Montgomery modular multiplication Algorithm," Journal of the Korea Institute of Information and Communication Engineering(JKLLCE), Vol. 22, No. 1, pp. 100- 108, Jan 2018.
DOI: http://doi.org/10.6109/jkiice.2018.22.1.100

[6] Minwoo Kim and Taekyoung Kwon, “Analysis of Research Trend and Performance Comparison on Message Authentication Code,” Journal of KIISE, Vol. 43, No. 11, pp. 1245-1258, Nov 2016.
DOI: https://doi.org/10.5626/JOK.2016.43.11.1245

[7] Mun, Si-Hun, Kim, Min-U and Gwon, Tae-Gyeong, "Lightweight encryption technology trends for IoT communication environments", Information and Communications Magazine, Vol. 33, No.3, pp. 80-86, 2016.

[8] Man-Seub Park, Chang-Su Kim and Hoe-Kyung Jung, "A Study on the Management of the WCMS-based Web-Contents," Journal of the Korea Institute of Information and Communication Engineering, Vol. 17, No. 4, pp. 857–862, Apr 2013.

[9] Md. Sadique Shaikh and Vasundhara Fegade, "Modeling Essentials of Content Management System (CMS) for Web-Based MIS Application," International Journal of Engineering and Technology, Vol. 2, No. 3, pp. 379-383, Mar 2012.
DOI: https://doi.org/10.6109/jkiice.2013.17.4.857

[10] Hyung Suk Won, Jonghyuk Roh, Daesun Choi and Seunghun Jin, "TSP SDK Implementation," The Korean Institute of Information Scientists and Engineers, Vol. 29, No.2, pp. 589-591, Oct 2002.