International Journal of Security and Its Applications
Vol.7, No.5 (2013), pp.139-146
http://dx.doi.org/10.14257/ijsia.2013.7.5.12

Content Reuse Prevention Scheme to Prevent Privacy Invasion of Social Network Service

Su-Young Jung[1] and Jin Kwak[2]

[1]*ISAA Lab, Department of Information Security Engineering, Soonchunhyang University, Korea*
[2]*Department of Information Security Engineering, Soonchunhyang University, Korea*
[1]*syjung@sch.ac.kr*, [2]*jkwak@sch.ac.kr*

Abstract

A social networking service (SNS) is an open service that enables its users to communicate freely without being constrained by time or space. In an SNS, users can share various types of content (such as pictures and videos) with government agencies, celebrities, and many other users online. If a person is able to access the content of another user, that content is automatically downloaded and stored in the "Temporary Internet Files" folder in the SNS user's PC. Moreover, the content stored in this folder remains there even when the content owner removes it from his SNS. Thus, the stored content is vulnerable to an invasion of privacy due to malicious user abuse. To address this possibility, we propose a content reuse prevention scheme based on digital right management (DRM) techniques to solve the problem of the unwanted reuse of stored content in a malicious user's "Temporary Internet Files" folder.

Keywords: *SNS, To Prevent Privacy, Privacy, Content Reuse Prevention*

1. Introduction

People have recently become able to employ a wide variety of functions due to the development of smartphones and tablet PCs. As a result, a social networking service (SNS) can now be easily used, and the number of SNS users is increasing rapidly.

An SNS is an open service that enables people to communicate freely with smartphones, tablet PCs, and desktop computers without being constrained by time or space. SNS makes it possible to make new contacts online and to establish communication with government agencies, companies, and celebrities. In addition, users are able to share many kinds of content on an SNS [1, 2]. However, these contents are stored in a "Temporary Internet Files" folder on the user's PC when the user accesses another SNS user's content. This stored content can be accessed by anyone who gains access to the user's PC. Thus, an attacker can access SNS content in a "Temporary Internet Files" folder and can then use that stored content or make an illegal copy. In addition, the content owner whose SNS content was removed can remain in any PC user's "Temporary Internet Files" folder.

There is a need, then, for an SNS to be able to protect the content that is in a "Temporary Internet Files" folder. In this paper, we propose a content reuse prevention scheme based on DRM techniques to solve the problem of the unwanted reuse of stored content in a malicious user's "Temporary Internet Files" folder.

The remainder of this paper is organized as follows. In Section 2, we provide a brief fundamental overview of "Temporary Internet Files" and DRM, and discuss security

ISSN: 1738-9976 IJSIA

problems related to the reuse of stored content in an SNS. In Section 3, we describe our proposed scheme, and in Section 4, we analyze key issues related to the security it offers. Finally, in Section 5, we summarize and conclude this paper.

2. Related Research

2.1. Content Stored in a "Temporary Internet Files" Folder

When a PC user accesses a web browser and views the image of a web page, that information is automatically flash-stored in the PC user's "Temporary Internet Files" folder. The stored content is used to make a rapid connection to the same web page the next time a connection is made. Thus, a user accesses an SNS when that user views the content of a SNS that is stored on a PC user's "Temporary Internet Files" folder.

Figure 1 presents screen shots that are examples of SNS content stored in a PC user's "Temporary Internet Files" folder [3, 4].

Figure 1. Comparison of Stored and SNS Posted Contents

2.2. Content Reuse Vulnerability in an SNS

The SNS can control user access to posts via various forms of permission, such as "public," "friend" on Facebook, and "follower" on Twitter, which permit only users who have access permission to read posts on the SNS. This access control is able to block information leakage primarily in terms of posting [5].

Users access other users' posts when they view pictures or video content that was automatically stored in a PC user's "Temporary Internet Files" folder. This stored content can be viewed at any time and may be used for purposes other than those that the original user intended. If a content owner removes content in an SNS, that content remains in the "Temporary Internet Files" folder of any PC user who has accessed that content. Thus, an attacker can exploit this vulnerability (since the removed content can remain in any PC user's "Temporary Internet Files" folder) for malicious purposes, such as illegal copying and reuse.

2.3. Digital Right Management

DRM is a technology that was developed to prevent the illegal copying and distribution of digital content. This technology offers continuous protection spanning from the creation to the removal of digital content. DRM is used to prevent the illegal use of such media as MP3, free movies, and company security documents [6].

3. Content Reuse Prevention Scheme

If any user reuses stored SNS content in a "Temporary Internet Files" folder, this constitutes an invasion of the privacy of the content owner. To address this, we propose a content reuse prevention scheme for "Temporary Internet Files" based on DRM.

The content owner posts content when an SNS server generates an encryption key, and the content is encrypted using that key. An SNS user gains access to posted content when the encrypted content is downloaded to the "Temporary Internet Files" folder of the user's PC. Reading of this encrypted content in an SNS can be done only by the computers of users who have joined the SNS. Further, the encrypted content is overlaid by an empty file that can prevent the attempted reuse of the contents after storage.

The following figure presents an overview of the proposed scheme.

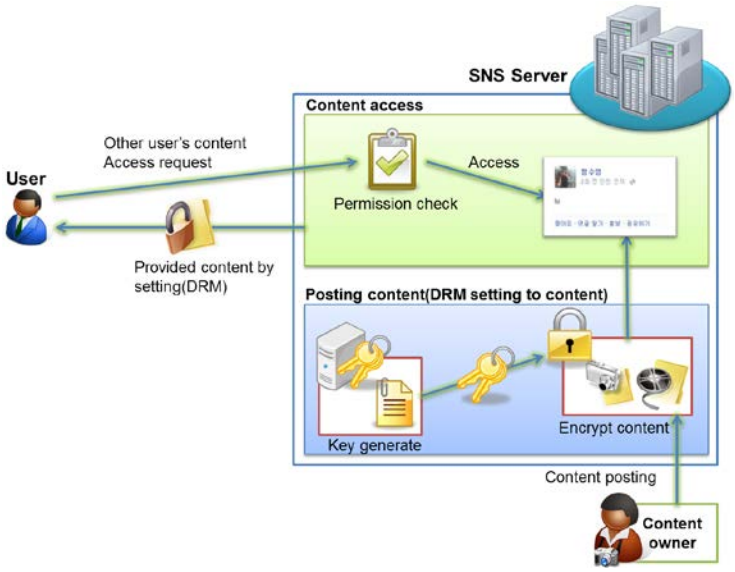


Figure 2. Overview of the Proposed Scheme

3.1. Phase of Preventing Content Reuse on SNS Server Side

This phase involves the encryption of the user's content that is posted on the SNS. This encryption is used to prevent the content from being reused on the SNS server side.

Step 1. Content owners request the posting of content on the SNS. When writing a post, the content owner sets the mode of post access permission (such as "public", "friend" on Facebook, or "follower" on Twitter).

Step 2. The content owner completes the setup for permission for the posting and uploads the content.

Step 3. The SNS server generates a key for content encryption. When generating the key, the defined range of the key being used depends on the file name, and the content file name is set using an ordinary upload sequence number on the SNS server.

Step 4. The SNS server encrypts the content using the key generated in Step 3.

Step 5. Once the encryption is completed, the content is posted using the text written by the content owners. Other SNS users can now access this post on the SNS.

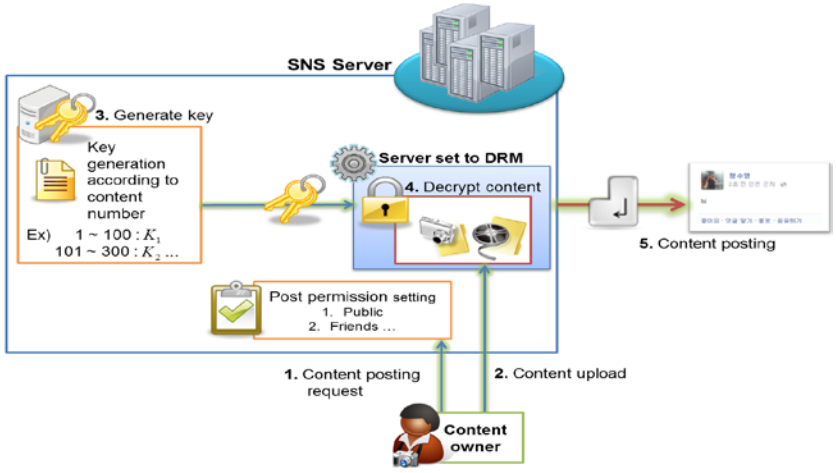


Figure 3. Phase of Prevention of Content Reuse on the SNS Server Side

3.2. Phase of Preventing Content Reuse on User Side

This phase is used when one user accesses another user's content post when the user receives the encrypted content to be opened. In order to view the content, the user needs to decrypt the content because the content transferred from the SNS server is encrypted.

To employ this function, the user connects to the SNS when the SNS installs the DRM application in the user's PC. The DRM application function has the ability to create a list of the access contents and to perform content decryption.

Step 1. The user's DRM application receives a decryption key from the SNS server, which enables the user to read posted encrypt content.

Step 2. The user's DRM application decrypts the encrypted content using the decryption key that was received, and the user is then able to view the content. If the user's DRM application to decrypt content is an empty file, the user's DRM application requests an original content download. The following figure graphically presents this process.

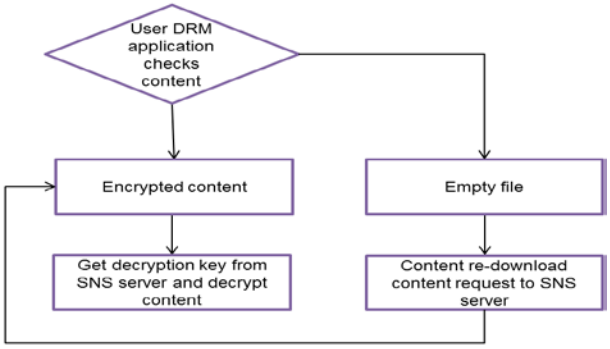


Figure 4. Process for Checking Content

Following this step, steps 3, 4, and 5 describe the process that takes place after re-logging in to the SNS.

Step 3. When the user re-logs in to the SNS, the user's DRM application transmits the user's list of contents to be accessed.

Step 4. The SNS server creates an empty file whose file name is set based upon the user's access content list form that the user received in the DRM application. The SNS server then transmits the content to the user.

Step 5. The user's DRM application overlays the content in the "Temporary Internet Files" folder those content is re-downloaded from the SNS server.

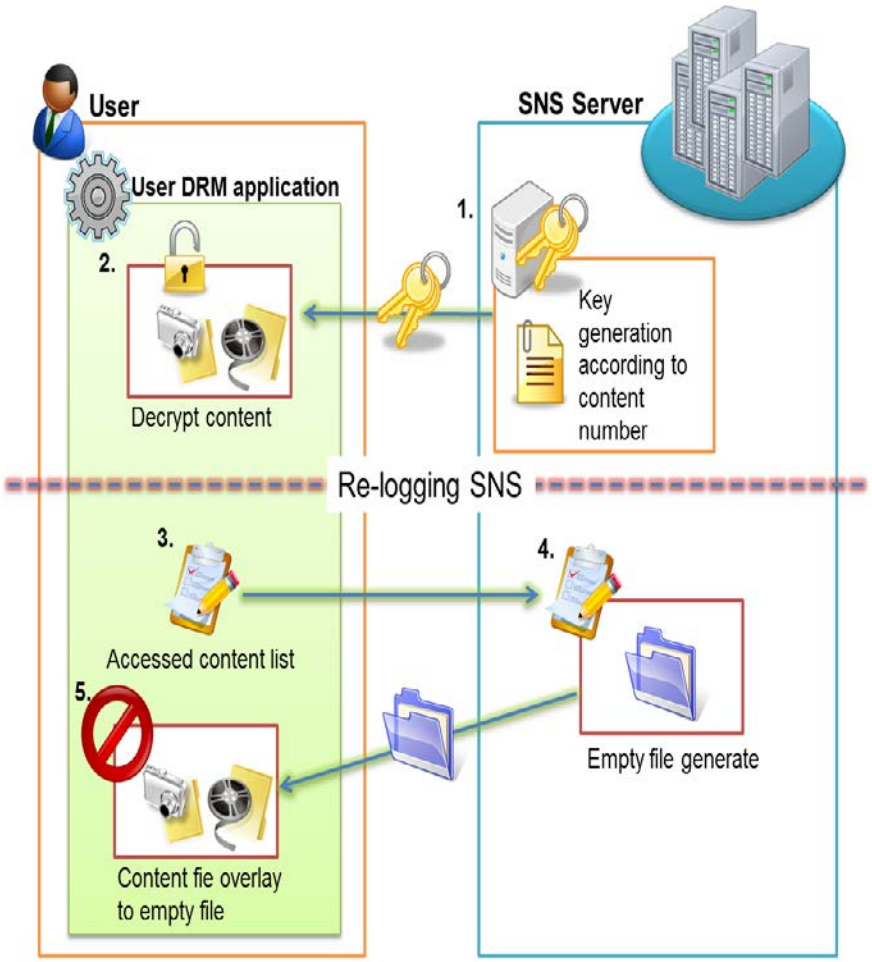


Figure 5. Phase of Prevention of Content Reuse on User Side

4. Security Analysis

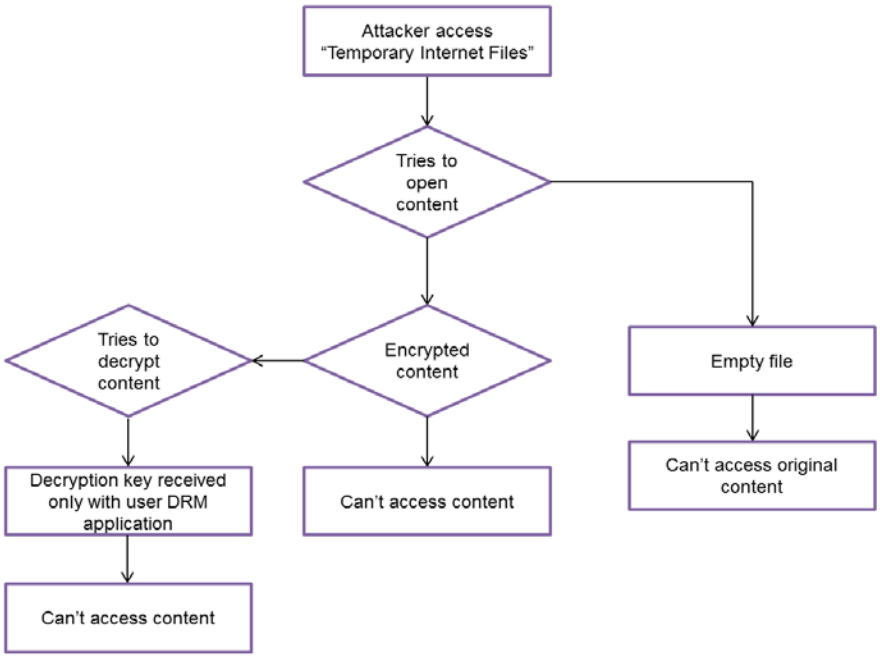


Figure 6. Flowchart of Security Analysis

Currently, the user views content on the SNS that is automatically stored in a "Temporary Internet Files" folder on the user's PC. Unless there are different settings, anyone is able to access and copy this stored content, which creates the potential for invasion of privacy. To address this, we propose a content reuse prevention scheme based on DRM techniques.

The conceptual flowchart in Figure 6 demonstrates how our scheme provides security with regard to the problem of content reuse. If an attacker tries to open and copy stored content, two possible sequences of take place, and in either case the content cannot be accessed because the content is either encrypted or there is an empty file.

Therefore, our proposed scheme is able to prevent the reuse of existing stored content in a "Temporary Internet Files" folder.

5. Conclusion

Users can access another user's post when the content is automatically stored in the first user's PC in a "Temporary Internet Files" folder. This stored content can then be viewed at any time and may be used for purposes other than those intended by the user. If an attacker reuses this stored content, this can constitute an invasion of privacy.

In this paper, we have proposed a content reuse prevention scheme based on DRM techniques in order to solve the problem of the unwanted reuse of content in a malicious user's "Temporary Internet Files" folder.

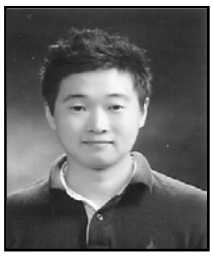
Acknowledgement

This work was supported by the Soonchunhyang University Research Fund.

References

[1] L. A. Cutillo, R. Molva and T. Strufe, "Privacy Preserving Social Networking through Decentralization", Wireless On-Demand Network Systems and Services, WONS 2009. Sixth International Conference, **(2009)**.
[2] T. Y. Youn and D. W. Hong, "Security Issues in Social Network Service, Electronics and Telecommunications Trends", vol. 26, no. 4, **(2011)**.
[3] Facebook, available at http://www.the Facebook.com.
[4] Twitter, available at http://www.the Twitter.com.
[5] P. Kumari, Requirements Analysis for Privacy in Social Networks, 8th International Workshop for Technical, Economic, **(2010)**
[6] J. H. Park, Y. J. Jeong and K. S. Yoon, "Trends of DRM Technology", Electronics and Telecommunications Trends, vol. 22, no. 4, **(2007)**.

Authors



Su-Young Jung received his B.S. degree in Information Security from Soonchunhyang University (SCH), South Korea, in 2012. He is currently an M.S. candidate at the Information Security Application and Assurance Lab, SCH. His research interests include cloud computing and smart grid security.

Jin Kwak received his B.S. (2000), M.S. (2003), and Ph.D. (2006) degrees from Sungkyunkwan University (SKKU), Korea. Before joining the faculty of Soonchunhyang University (SCH) in 2007, he was a visiting scholar at Kyushu University, Japan. Subsequently, he served at the Ministry of Information and Communication (MIC), Korea, as Deputy Director. Furthermore, he served as Dean of the Department of Information Security Engineering (DISE) at SCH (2009–2010) and Vice-Dean of the College of Engineering (2009) at SCH. He is now Professor at DISE. In addition, he is Director of the SCH BIT Business Incubation Center and of the Industry-University & Institute Partnership Division Center at SCH. His main research areas are cryptology, information security applications, and information assurance.