INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

REVIEW ON DISTRIBUTING PRIVACY POLICIES OVER MULTIMEDIA CONTENT ACROSS MULTIPLE ONLINE SOCIAL NETWORKS

PROF. S. S. SHEKAPURE, MS. L.N.BAHURUPI, PROF. O. A. JAISINGHANI

Department of Computer Science & Engg., Dr. R. G. I. T. & R., Amravati.

Accepted Date: 15/03/2016; Published Date: 01/05/2016

Abstract*:* Online Social Networks (OSNs) are currently playing a crucial role in our everyday social life. Their great growth has sparked the interest of hackers and individual users that try to disclose as much information as possible, which in many cases unfortunately is possible. In such events, the users' privacy settings are bypassed by the leakage of their shared media content. To address this challenging but important research problem, we introduce a new distributed scheme for media content sharing on online social networks that may minimize users' privacy exposure, through automated procedures. The novelty of the proposed scheme is the ability to enforce a user's privacy policies across multiple online social networks, even if she is not subscribed to all of them, without using a trusted third party. Moreover, the proposed framework is a step towards enabling OSNs to interact, exchange information with equal rights, independently of their size, focus and underlying infrastructure.

Keywords: Cloud Computing, Data leakage, Data leakage hindering, Data leakage detection

Corresponding Author: PROF. S. S. SHEKAPURE

Access Online On:

www.ijpret.com

How to Cite This Article:

S. S. Shekapure, IJPRET, 2016; Volume 4(9): 1617-1624

PAPER-QR CODE

INTRODUCTION

Social media platforms like Facebook, Google+, Twitter and LinkedIn have completely changed people's behavior on the web. Simultaneously, new social media like Pinterest and Instagram highlight that multimedia sharing, more precisely images, either personal or computer generated, are a modern niche market with huge revenues for the service providers. Without any doubt, the biggest part of the shared information within social media is multimedia content, uploaded and shared by their users.

Many of the privacy risks that a user's privacy is exposed to stem from the authentication and management mechanisms of published information. Malicious users have reportedly managed to bypass users' privacy settings of these services in many cases. As a result, new offenses ranging from identity theft up to personal information exposure are disclosed on a daily basis. The ease of re uploading and re-publishing a user's images, without any form of notification, often harm the original owner both social and economically.

Related Work

1. Privacy Issues in OSNs

Privacy in OSNs can be approached by different points of view. Many researchers are focusing their efforts on the publication of anonymized graphs that represent the connections between users of OSNs. The majority of attacks are based on neighborhood attacks, a special type of attacks which is based on the fact that even if anonymization techniques have been applied on the provided data, an adversary may exploit some background knowledge about the ''neighborhood'' of a target victim. To this extent, known relationships among its neighbors can be exploited, leading to the re-identification of the victim. Therefore, special anonymization techniques, belonging to what is called privacy-preserving data publishing, are being applied to protect users. Even if the aforementioned attacks are very important, we are interested in attacks ''within the neighborhood''. This means that the attacker belongs to the victim's neighborhood, tries to enter the neighborhood or tries to create a neighborhood that can be attributed to the victim. The ideal scenario would demand users to allow access to people that they truly trust, so that their shared information is not leaked. Nevertheless, as everyday living shows, this is not the case. People within social networks tend to have hundreds or even thousands of ''friends'', allowing them to access information that they would not do in real life. Apart from the obvious problem of how people regard their privacy on the Internet, we argue that OSNs should provide

more mechanisms to increase the privacy of their users and protect them, as their privacy policies can be trivially bypassed as shown in. The main privacy issues in OSNs, as discussed in.

In an Identity Theft attack, the attacker tries to masquerade as another person to hurt his social profile, or to exploit the trust that other people have in his authority and to obtain money, usually in form of credit. The victim's shared multimedia, which is usually of high quality, can be used to launch attacks in real-life as well, e.g. print fake ID cards or company passes. Fraudsters can also extract useful information from the shared multimedia content on OSNs. In cyberspace the replication of victim's account, multimedia content and information, can be achieved easily while this process can even be automated. Closely related to the identity theft are the following two attacks, which are often regarded as specific cases. If we have replication of the victim's profile in the same OSN, then we have the so called Profile Cloning attack. Otherwise, if the attacker exports the victim's information and multimedia content and creates a profile to another OSN then we have the Profile Porting attack. This attack may be more effective for victim impersonation since a search query at an OSN will only return a single profile, the fake one. In the Sybil Attack scenario, a user creates multiple accounts to manipulate and affect a result as desired by him and his purpose. It is essentially an escalation of Profile Porting attack. The goal of the adversary can vary from a simple voting scenario to a de-anonymization attack. If a user uploads a multimedia file, setting her desired privacy policy for example to be shared only with her friends, implies that she trusts her group of friends in that they will not share or re-upload her file. Nevertheless, as already discussed in the introduction, in current OSNs her shared multimedia content is usually one click away from bypassing her privacy preferences, leading to the unauthorized content sharing attack. Another privacy exposure stems from the use of static links, which are used by the majority of OSNs. OSNs use static links to bind the shared content, which can easily be copied and arbitrarily shared on any other medium. Finally, most OSNs do not allow shared ownership of content. Anyone who possesses it is considered its sole owner and can define privacy policies for it. Thus, if she re-uploads it, she automatically can set different privacy policies.

2. Tools for privacy in OSNs

In principle, it should be noted that very closely related to our research is the work on Social Identity Management (SIdM). This can be understood as the set of methods that OSNs use to allow users to disclose information to specific groups of their contacts. This allows them to manage the attributes and information that they disclose regarding their social identities/roles,

attributed by others or themselves. As it becomes apparent, SIdM is not only focused on multimedia content, but any attribute that an OSN user can have.

Currently, several solutions concerning users' privacy on existing centralized or decentralized OSNs, have been proposed. The bulk of these solutions come as external applications and are not native solutions, having several drawbacks that do not allow their wide adoption. For instance, many of them are experimental solutions or proofs of concept. Therefore, the interface and support is quite limited. The nature of these tools might even bypass the terms of service of each OSN e.g. as they use cryptographic or steganographic methods, which hide the main source of income of OSNs, information. Therefore, the solutions which are discussed in the following paragraphs are not widely used and many times users are unaware of their existence. For instance, completely decentralized OSN architectures like Diaspora, Safebook & One Social- Web never managed to attract massive amounts of users to change the rules of the game.

In NOYB, groups of users share a key and break their personal information into ''atoms'' which are then permuted with the ''atoms'' of other users, using the key to generate the permutation. Thus, the real information is hidden from the OSN and the users who do not have the key.

Persona, allows users to encrypt their data and exchange a public key with selected users. This way, Persona provides an attribute based encryption to users' data, which allows them to apply their desired privacy policies regarding data access. Easier extends Persona, by creating decryption keys that are associated with each user, allowing data access, only when a user contacts the proxy with the appropriate key. Another encryption based tool, is Fly-by-night. It mainly uses public key encryption algorithms to exchange users' messages in Facebook. Scramble is a Firefox extension which allows OSNs users to encrypt their uploaded content storing it either at a Tiny-Link server or the OSN.

3. Watermarking

The most basic property of image watermarks is their invisibility that is they must be imperceptible by the human visual system, allowing them not to be traced and removed from unskilled attackers or to alter the quality of the image. Depending on the application needs, watermarks have different robustness. Fragile watermarks are used to check the integrity of multimedia files, as the slightest modification can break them, triggering an alert to the watermarking system. Semi-Fragile watermark systems detect malicious modifications on the host image, e.g. object insertion or cropping, while common image processing as random noise and/or lossy compression do not trigger any alarm. Finally, robust watermarks are made to

withstand a wide range of possible attacks as they are mostly used for proofs of ownership. An attack from a malicious user would be the removal of watermark or making it undetectable. However, this should not be possible without a great degradation of the host image. The capacity of the watermark refers to the maximum number of information bits that can be embedded to a multimedia file of a given size. Depending on the application, the minimum capacity that is required can range from 1 bit, in copy control application, to a whole photograph. Finally, there are two categories of algorithms based on the requirement to access the original multimedia file during extraction. Non-blind algorithms compare the original with the watermarked image to extract the information. On the other hand, blind algorithms do not need access to the original image.

4. Enforcing privacy policies within a single OSN

Users trust their multimedia files in OSNs and the majority of users do not seem to bother whether OSNs alter their content due to resizing or compression, as long as the content does not have visible distortions. When a conflict of multimedia content ownership or misuse occurs, OSNs are heavily dependent on user reports. This approach has major drawbacks. The most obvious one is the manual nature of the system. Secondly, this policy enables a malicious user to report everyone, adding an additional cost because there is not an automated system to handle these requests. Finally, and perhaps the most important, a user can report a misuse only when he becomes aware of it, which is usually through another user's feedback or by sheer luck. For the latter case the OSNs do not take any precaution measures, neither do they offer any kind of notification mechanisms to their users.

The watermarking scheme proposed by Zigomitros et al. is mainly focused on images, but can be applied to other multimedia content such as audio and video. The scheme uses two watermarks, a robust and a semi-fragile, both explained previously, for storing user's multimedia content. A use-case scenario can clarify the need for the dual watermark scheme. We assume that user A provides to OSN an original multimedia. Then the OSN starts the embedding process and embeds a robust watermark, which identifies the multimedia content uniquely and associates it with the user. A semi-fragile watermark can be embedded in the host media at the same time or afterwards, since the robust watermark can tolerate this kind of process. The dual watermarked media is stored in OSN servers and becomes available to users of the OSN according to privacy settings defined by its owner. The robust watermark is used to identify the media and the owner of it uniquely, and can be recovered even if the watermarked media has been processed.

Meanwhile, the semi-fragile watermark enables the detection of alterations, malicious or not. The scheme is illustrated in Fig. 1.

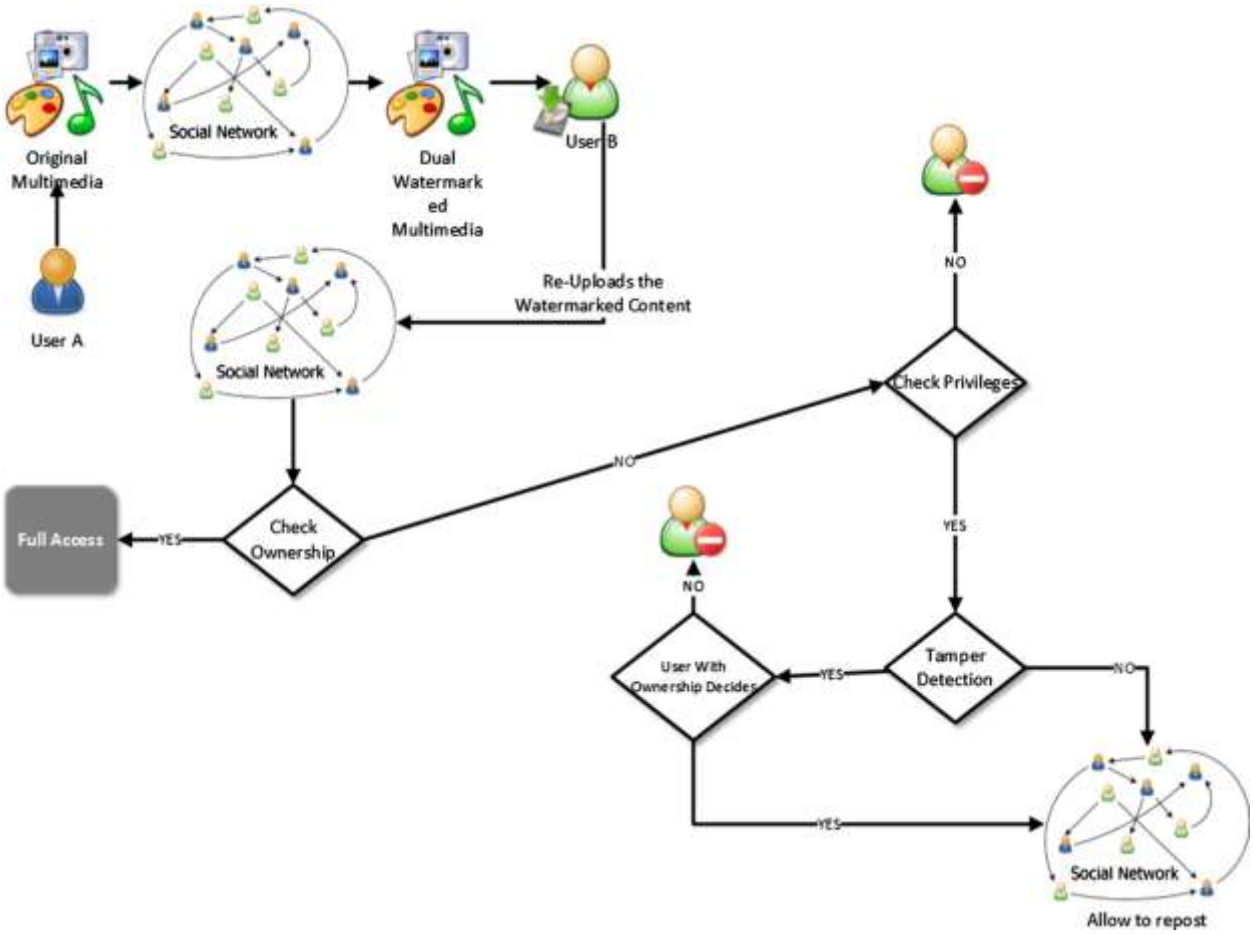

Fig.1. The Zigomitros et al. scheme.

Experiments

1. The process

The lack of detailed reference manuals on how the shared information is managed, processed and stored from most OSNs, due to their closed source code notion, has led us to conduct several experiments in order to test the possible existence of image watermarking schemes. The experiments that where conducted were repeated to test if there is any change in the policies. The original tests were made on the two most widely used OSNs, namely Facebook and Google+. However, we decided to include in our experiments a fast growing OSN, VK (vk.com), which

claims to currently host more than 100 million active users. For our experiments we used two groups of images, which are going to be referred as Test Set 1 and Test Set 2, using two user accounts, user A and B respectively. The concept was to upload both sets of images on the two accounts and then download again the images from each users' profile and perform some comparisons. Firstly, we downloaded the images from the profile of user A and compared them against their originals. Then, the same procedure was executed for user B. Then, we compared the downloaded images of the two users, trying to trace possible differences. The same procedure was repeated for each OSN, from different PCs and at different time frames. These steps allowed us to avoid computer fingerprinting and exclude the time factor from our experiments. Two groups of images were created. Test Set 1 includes 40 computer generated and grayscale images from TESTIMAGES.

RESULTS

Since the results vary on the three OSNs, we group their results accordingly. Therefore, firstly we present some general remarks and then we discuss our findings for Facebook, Google+, and finally, for VK.

The results for VK presented more differences. The main difference is that VK has three resolution thresholds for uploaded images, beyond these thresholds; images are resized to fit these boundaries. Therefore, only 30 cases (20 for Test Set 1 and 10 for Test Set 2) fit these boundaries and could be compared against the original ones, all of them being identical. Testing the downloaded images from the profile of user A to the respective from user B, showed again that they are identical, even in the case of size reduction.

CONCLUSION

The privacy of the multimedia content which is a significant ingredient for the success of OSNs, has not drawn the proper attention yet. The OSNs so far only deal with metadata of multimedia content by erasing them or by letting users set privacy settings for the geolocation of the content if available. As OSNs affect more and more our daily lives, the development of new security and privacy policies for multimedia content becomes essential. Towards this end, this work introduces a scheme that allows users to enforce their privacy policies not only on multimedia shared in the OSN that they belong to, but among others to which they are not registered. This is achieved by the use of watermarks on the multimedia with either public encryption algorithms or public watermarking techniques. The major contribution of this work is the unification of privacy policies across multiple OSNs in a distributed way without the use of trusted third parties.

REFERENCES

1. Sonia Jahid, Prateek Mittal, Nikita Borisov, Easier: encryption-basedaccess control in social networks with efficient revocation, in: Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, ACM, 2011, pp. 411–415.
2. Randy Baden,Adam Bender, Neil Spring, Bobby Bhattacharjee, Daniel Starin, Persona:an online social network with user-defined privacy, ACM SIGCOMM Comput. Commun.Rev.vol.39, ACM, 2009,pp. 135– 146.
3. Julian Backes, Michael Backes, Markus Dürmuth, Sebastian Gerling, Stefan Lorenz, X-pire!-a digital expiration date for images in social networks, arXiv preprint arXiv:1112.2649, 2011.
4. Distributing privacy policies over multimedia content across multiple online social networks Constantinos Patsakis b,⇑, Athanasios Zigomitros b,c, Achilleas Papageorgiou b, Edgar Galván-López