A Case Study on Clickjacking Attack and Location Leakage

Lim Chin Nei, Loo Yow Cherng, Manmeet Mahinderjit Singh

Abstract— The advanced in technologies such as mobile devices, GSP, WIFI, and 3G has encourage the information sharing using social media. The large amount of information shared on social media often lead to security issues which are unaware by the users. This information may include sensitive information such as a person's name, location, relationship status and many more and can be dangerous if is put in a wrong hand. In this research, we provide a review on the type of social media ad what are the current threat in social media. We then focus on two specific threat namely clickjacking and location leakage, and proposed a solution for each of it as well as the evaluation of the solution.

Index Terms—*Security; Social media; Attack; Defense Machine, Clickjacking, Location leakage*

1 INTRODUCTION

This rapid shift of technologies in this era of information and communication has dramatically boosted the usage of the social media. With the advanced in technologies such as smart mobile devices, GPS, WIFI, and 3G services, user were able to connect to the internet regardless of time and location and hence allowing them to use application or services of social media anywhere, anytime. This is especially true for social media such as online social networking sites (OSN) which has received excellent response from the users. The use of social media has provided a virtual meeting place for people across to world, which hence has ease the effort in sharing information and communicating. Such convenient technologies, hence received a great response from users of all social and age levels. OSN such as Facebook and Twitter has hundreds of millions of daily active users, which hence causing a tremendous amount of information sharing happening across the world. Facebook, for example, has more than 1.23 billion active users per month, reaching an amount of 945 million active mobile users in the end the year 2013 [4].

Social media is important because the users spend a large amount of time on performing activities on the internet using it, including updating their information, interacting with other users, and browsing other user's profile, statistics shows that the young generation is the large share of users in social media [23]. Social media is very useful because it removed the geographical and economical borders in interacting with people, allowing people with the same interest across the world to interact with each other. Moreover, social media can also be used as a tool for entertainment as such as provided by YouTube, or for other purposes such as educational, advertisement, job finding and many more.

The concern is that most of the users of social media are unaware of the potential threats that may occur in the social media. With this large amount of information shared online, the social media actually has become a perfect platform for hackers to find their victims. The information shared using social media often contain sensitive and private information which can be easily compromised by the hackers. Furthermore, most of the social media user have low awareness on how security attack is performed and hence often fall into the traps of hackers such as clickjacking and phishing attack. As a result, a lot of social media user's account has been compromised, causing a loss in sensitive data.

In this research paper, we perform a study on the current available threats in social media, and the corresponding security mechanism that can be applied on it, by focusing on the threats namely clickjacking attack and location leakage. The rest of the paper is organized as follow: Section II Background Study provide a study on the definition and the types of social media, Section III Related Work presents the current threats in social media as well security mechanism applied on the two of the threat, which is clickjacking and location leakage. Section IV Case study 1: Clickjacking, present a research on the threat clickjacking, including the real life example, the way that it is performed, and our proposed solution to encounter clickjacking. Section V Case study 2: Location leakage provides a study on the threat location leakage, including a real life example, the way that user location information can leak, and our proposed solution to encounter the threat. In Section VI we evaluate our proposed solutions by comparing it with the X.800 security services standard. Finally, we conclude our research and future work in Section VII.

.

International Journal of Scientific & Engineering Research, Volume 5, Issue 7, July-2014
ISSN 2229-5518

2.0 BACKGROUND

When talking about social media, most of the people will be thought about the online social networking such as Facebook and Twitter. However, social networking sites only consider as one of the classification of social media. According to Kaplan and Haenlein, there are six different types of social media [1], which are collaborative project, blog, social networking sites, content communities, virtual game-worlds and virtual social world. Before further discussing the types of social media, a definition of social media is needed to know.

Definition of Social Media

According to Jacka and Scott [2], there are many definitions of social media. Hence, let's see about some of the definition that state by researchers before.

Oxford Dictionary, 2011: Social media is a dedicated websites and applications that enable users to communicate with each other, or to find people with the similar interest to one's own.

Andreas Kaplan and Micheal Haenlein[1]: Social media is a "group of internet – based application" which allows the creation and exchange of the user – generated content.

In a short word, social media is an online web application which allows the people to communicate or share the information and resource with others.

Classification for Social Media

As mention is the earlier section, there are six types of social media in today's world.

Collaborative projects: A type of social media which allows the joint and simultaneous creation of content by many users. The content modification level is depended on the setting of the website's admin. Some of the website, such as Wikipedia allows user to add, remove and change the content; however, some of the websites only allows the group based collection or user rate. The example of collaborative projects is Wikipedia.

Blogs: A type of social media is a personal website which allows individual to publish their information and others come to comment or give the opinion on his information. The example of blog is Blogspot.

Social Networking Sites: A type of social media which allows individual to interact with their friends or others by inviting them to have the access to the profile, send emails and instant message. The example of social networking site is Facebook and Myspace.

Content communities: A type of social media which focus on the sharing of media content between users. The difference of content communities and social networking sites is individual are not allowed to create a personal profile page. The examples of content communities are Bookcrossing (share text), Flickr (share photographs) and Youtube (share video).

Virtual game world: A type of social media that replicate a three – dimensional environment and user (player) appear as a personalized avatars (character). In virtual game worlds, user can interact with others (fight or discuss the strategy) according to the rules and setting of the game. An example of virtual game world is World of Warcraft.

Virtual social world: A type of social media which allows individual to choose the behavior more freely and live in a virtual world which similar to the real life. Same with the virtual game world, individual appears as a personalized avatars and the different things is virtual social world create a environment which is similar to real life (sleep, eat and others) while virtual game world create a fight or gaming environment which is totally different with real life. Second Life is one of the examples of virtual social world.
In today world, as the technology continues to be improved in order to satisfy the user, the boundary between the different types of social media has increasingly blurred. For example, Shi et.al [3] argue that Twitter is a combination of the broadcasting service (blog) and social networking sites and hence introduced a new classes which known as "social broadcasting technology".

3.0 RELATED WORKS

In this section, we discuss the existing attacks and defenses on online social media which has been proposed by researcher.

Online Social Media: Threats

With the increasing usage of online social network, attackers start to use online social network as a platform to perform their attacks. Those attacks can cause several threats such as stealing user's personal data (bank account information) or installing software application on the user's computer to perform another backend attack. Hence, a few of study is make in order to protect social network's user.

According to the study, those attacks basically can be divided into two main categories: active attack and passive attack and then divided into two more classes which are classic threats and modern threats. [4]

Active attacks is a type of attack that attackers may transmit the message or modify or delete the message/data during the transmission whereas passive attack is the intruder eavesdrop the message/data only without modify any message during the message transmission. The definition of classic threats and modern threats will be discussed with their examples first before showing a table which classify the threats into active attack and passive attack.

Classic threats, a category of threat that not only threatens online social network but it also normally used by attackers on others website which is not social network as well. The examples of classic threats are malware, cross-site scripting (XSS) attacks, internet fraud and phishing attacks.

International Journal of Scientific & Engineering Research, Volume 5, Issue 7, July-2014
ISSN 2229-5518

We can found those classic threats on other website such as banking website as well.

On the other hand, **modern threat** is the additional current threats that unique to online social network environment. Modern threat uses the online social network infrastructure to perform attacks such as collect and expose the personal information of a user and then lured users to click on malicious link. The examples of modern threat are inference attacks, de-anoymization attacks, clickjacking and location leakage. A briefly introduction of various modern threats is shown in rest of this section.

De-anoymization attacks: Wondracek et al. [5] who introduced this attack uncover the user's real identity by using the network topology and user group membership in online social network.

Clickjacking attacks: A very common malicious techniques that used to trick online user click on something that they unintended to click and then manipulate user to post spam message on their timeline. For example, an attacker web page tricks the victim to click on a Facebook "Like" button without acknowledge victim that he actually did unintended action (post that he "likes" the attacker web site). And, victim's friend will just click on that link because of their curiosity and then the attack is spread out.

Location leakage. A type of information leakage that can expose the user's location. With the increasing use of mobile devices and technologies such as GPS and 3G, user may unknowingly share their location when they sharing private and sensitive information using social media, which can then, led to loss of properties such as burglary as home [4].

Category of threats	**Threat's name**	**Attack's type**	**Reason**
Classic threats	Cross-site scripting	Active attack	Can cause web client run malicious code
	Internet fraud	Active attack	Used to scam or take the advantage of victim
	Phishing attack	Active attack	Used to take the advantage of victim (take all the money or invite friend to click on malicious link)
Modern Threats	Inference attacks	Passive attack	Eavesdropping the information and then predict victim's personal
	De-anoymization attacks	Active attack	Uncover the user's real identity
	Clickjacking	Active attack	Trick user to click something that they unintended to do
	Location Leakage	Active attack	Analyze victim's location from their social media information then perform physical crime

In today world, a more sophisticated attack is created by attackers by combining these two types of attacks in order to prevent being detected by security machine. Hence, it makes user more difficult to detect and prevent the attack in online social network.

Online Social Media – Solutions

As we know, it is always hard to make an application that has high security level and much function. The number of vulnerability of an application is increased with the increasing amount of the functionality in an application. In order to protect online social network from attackers, several of defense machine is introduced. Several of the defense machines are described below.

Authentication mechanisms: a type of technique that used to make sure that the user that log into the social network is a real person and not a socialbot. The common technique that used in this authentication machine is photo-of-friends identification or multi- factor authentication (verification code from mobile devices and password). [4]

InContext: A type of defense model which proposed by Huang et al. [6] to use to prevent clickjacking attack in online social network. His team mentions that most of the existing clickjacking defense has their shortcoming and the most widely deployed defense; *framebusting* is incompatible with embeddable third – party widget (Facebook Like button). Hence, it is not applicable well in most of the online social network. The table below shows a summary of existing defenses that used to prevent from clickjacking attacks.

Type of context that protect	**Attack Name**	**Attack Description**	**Challenge**
Protecting visual context (include pointer integrity)	User Confirmation	Confirmation dialog is displayed to user whenever request come from blacklisted domains	• Degrades user experience • Vulnerable to double click timing attack
	User Interface Randomization	UI layout (element's position) is randomized	• Attack still can be perform by asking victim to keep clicking until successfully

International Journal of Scientific & Engineering Research, Volume 5, Issue 7, July-2014
ISSN 2229-5518

			guessing the location of target UI element
	Opaque Overlay Policy	Removes all the transparency from all cross – origin element	• Making inconvenience to some developer • Break the flow of other legitimate websites
Protecting pointer integrity	Visibility Detection on Click	Transparent frames is allowed but mouse clicks is block if frame that being clicked is detected not fully visible	• Return false positive is some site • Must declare that all cross – origin frames need clickjacking protection, or else just protect a particular element
Protecting temporal Context	UI delay for cross – origin	Impose a delay after displaying a dialog	• UI delay making users feel annoy • Clickjacking attack still able to perform by using whack – a – mole attack

The defense model, **InContext** which proposed by Huang et al. protect all the integrity (visual integrity, pointer integrity and temporal integrity).

To protect visual integrity of online social network, Huang et al. checks target visual integrity by comparing the OS – level screenshot and the bitmap of sensitive element rendered in isolation at the time of user action. Firstly, a screenshot of browser window based on element's position and dimensions is taken in order to do the comparison. On the other hand, reference bitmap, the position and dimensions of the sensitive element should be looks like when rendered in isolation is determined by browser. After that, the referred bitmap and screenshot of browser is compared to determine whether the sensitive element in referred bitmap is same with what user see and hence detects potential clickjacking attack by using this technique.

To protect pointer integrity of online social network, various techniques is introduced by Huang et al. The technique that used by Huang and his team are screen freezing around sensitive element, no muting and no lightbox around sensitive element so that victim will not get attract by those fake element. In addition, no programmatic cross – origin keyboard focus is allowed to prevent victim from getting strokejacking attacks (change the keyboard focus in online social network).

UI delay technique with some improvement is used to protect temporary integrity of online social network. As mention in the table above, UI delay for cross – origin are still vulnerable for whack – a – mole attack, which tricks user to click fake target element for many times. Hence, a advanced UI delay, UI is delayed whenever the pointers enters the sensitive elements in order to let victim have enough time to realize that they going to click fake target element and respond it before being attack by whack – a-mole attack.

Landon et al. [19] introduced a system called Smokescreen which provides flexible privacy control related to the presence sharing. The system provide flexible information sharing by allowing broadcasting of clique signals that can be activated or deactivated depending on the user choice. Such system hence allows the user to limit the information shared with strangers and hence reduce the risk of location leakage while still remain the full benefit of presence sharing.

While Smokescreen solved the problem of how to flexibly sharing presence between friends and stranger while preserving location privacy, Wei et al. [20] claim there are no similar scheme that were introduced for mobile online social networks (mOSNs). Hence, the authors proposed a system called MobiShare which provides flexible privacy-preserving location sharing in mOSNs. It enables location sharing between both trusted social relation and un-trusted strangers by separating user identity information and location information into two separate servers. This feature hence required the both server to be compromised by the same adversary in order to identify the specific user's location. A similar system is proposed by Liu et al [21], which are modified from MobiShare by simplifying the system architecture and adding encryption to the data. The proposed system, N-MobiShare removed the third-party that operate user's location information and protect user privacy by performing cryptography, this hence simplified the effort required to perform maintenance on the system architecture.

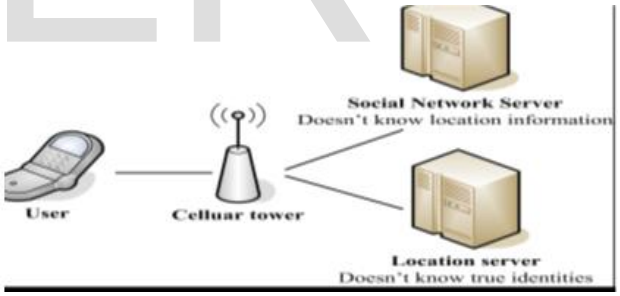

Figure 1: System architecture of MobiShare [21]

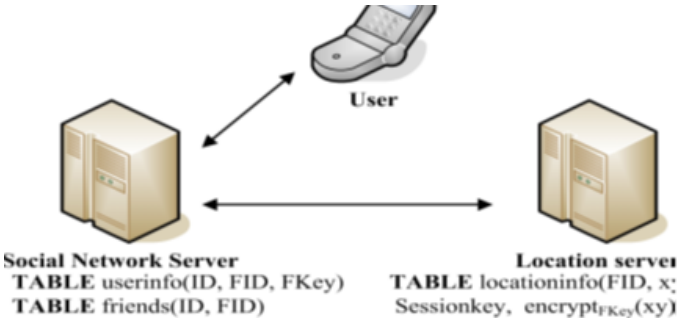

Figure 2: System architecture of N-MobiShare [21]

International Journal of Scientific & Engineering Research, Volume 5, Issue 7, July-2014
ISSN 2229-5518

On the other hand, SnapMe services is introduced by Henne et al. [22] which can notify a user if a photo of the user is posted nearby, even though the user is not tagged. The services are performed by utilizing face-recognition and co-location check technique. This service hence can help the users in managing the flood of media, avoiding the picture of the user being used without notifying the user, and hence reducing the risk of privacy leakage.

In a paper published by Friedland et al. [13], the authors believe that educating the users is the key in preserving location privacy and two ways that location data should be handling in order to avoid location leakage. The authors thinks that location sharing should be acknowledge at a per application basic, suggesting that capturing/recording of photo/video should include a control on the degree of location information that can be stored. Another suggestion is that instead of restricting the location information at the time of capture or record, the information can be restricted at the time of sharing. This can be done by implementing the same control, however on the time of sharing, which the browser will provide a dialog box on the location privacy control..

4.0 CASE STUDY 1: CLICKJACKING ATTACKS

Clickjacking, which also known as UI redress attack is a malicious technique that attract users to click on an element of a web page which different from what they intended to click. After that, users are routed to the web page which is designed by attackers and then attack is performed.

An example of clickjacking attacks which occurred recently at Facebook in 2011 is fake news about Lady Gaga found dead is spread in Facebook and Tweeters and then lures Lady Gaga's fans to malicious web page [7]. In this case, legitimate BBC site is replicated in the malicious website which done by attackers and it successfully make some social network's user believe that the website that they visited is BBC site. A survey dialog is pop out and prompt user to complete a survey form before they could play the video. In the backend part, their respective accounts were being set to "Like" and the news of "Lady Gaga found dead in hotel" is post on victim's timeline in order to attract more curious user to come this malicious website and it allows attackers to earn money from every user visit.

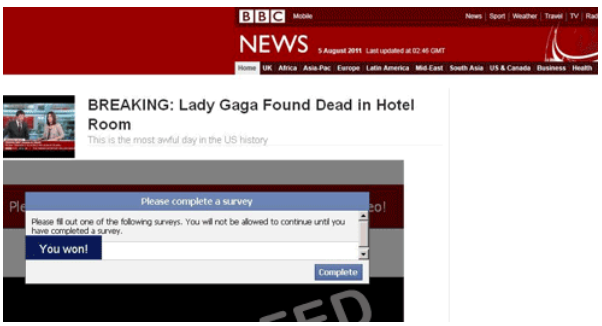

Figure 3: Screenshot of survey prompt

Figure 4: "Like" wallpost of affected user

According to Paul Pajares, a Fraud Analyst [7], clickjacking attack is performed because Facebook does not display any warning site when the site is redirected and the site's SSL/HTTPS feature is bypassed. Hence, attackers take this vulnerability to perform their attack.

4.1 Vulnerability of social network on clickjacking network

However, there are still many ways to perform clickjacking in online social network. For example, cursor spoofing attack, double- clicks attack and whacks a mole attack. Based on study, basically there are three ways to lure user by using clickjacking attack. [6]

1. Compromising target display integrity (visual integrity)
2. Compromising pointer integrity
3. Compromising temporal integrity

1. Compromising Display Integrity

Website developer normally use HTML and CSS styling features in order to make their website (include online social network) attract more user. This styling feature lets the attacker has the opportunity to perform clickjacking attack by visually hide the target element (which redirect user to malicious site) in the legitimate online social network. Technically, the target element is covered by the original button in legitimate website so that victim does not notice anything go wrong in the website. Then, the original button is changed to become unclickable or cannot function and hence when victim clicks on the original button, it actually fall through the decoy (original button) and land on the invisible target element. Lastly, it makes victim perform unintended action in the online social network and being redirect to malicious website. In a short word, the vulnerability which allows the developer to change the display or visual of the website or hide the target element makes attackers able to perform clickjacking attack.

4.2 Compromising Pointer Integrity

To make the clickjacking attack more successful, some of

International Journal of Scientific & Engineering Research, Volume 5, Issue 7, July-2014
ISSN 2229-5518

the attack change both display and pointer which also known as cursor to make victim unaware of the attack. Pointer integrity is violated by displaying a fake cursor icon instead of the real cursor and it makes the victim misinterpret the click's target and then perform the unintended click. This attack is known as cursorjacking. Another ways to compromising pointer integrity is keyboard focus stroke jacking attack. Most of the browser allows developer to manipulate its keyboard focus. Attackers use this vulnerability to perform attack by switching the keyboard focus to target element while asking victim to input text on the fake attacker- controlled input field. The vulnerability of current website which allows developer to change or hide cursor by using CSS cursor property and change the focus of keyboard element allows the attackers trick the victims into sending input to the target element.

4.3 Compromising Temporal Integrity

According to study, human require a few hundred milliseconds to react to visual changes [8] and attackers take this advantage (our slow reaction) to manipulate the User Interface element. For example, the target element is moved on the top of decoy via CSS position proprieties after victim hover the pointer or cursor over the decoy or decides to click on the target User Interface element. Victim hard to respond to the changes that made by attackers as our slow reaction and some of them even didn't notice the user interface is changed. Another example is victim is asked to click the object in a malicious game repetitively and then attacker moves the target elements over the decoy immediately after the first click by victim. In addition, as most of the web browsers do not protect temporal integrity for web sites, it gives the chance for attackers to perform clickjacking attacks through this method.

4.4 Proposed Solution

As mention in the earlier section, most of the existing defense machine for clickjacking attack still faces some security challenge. Hence, after studied about current existing defense machine and its security challenge, we decided to propose a defense model which take most of the advantage of existing defense machine and improve it by changing the security challenge that face by that machine. In this paper, we decided to take *InContext* defense machine as a reference as it has more strength if compare with another defense machine, *FrameBusting*.

As mention in earlier section, *InContext* determine whether clickjacking attack is performed in online social network by comparing the referred bitmap and the screenshot of current browser (what victim see). However, it will be better if there is an server or database that support by all browser to save the targeted malicious website URL or its pattern. The basic concept is we proposed is almost same like the concept of intrusion detection system. There are two types of detection that we proposed in this paper, signature detection and anomaly detection.

Signature detection is a type of detection approaches that determine whether the attack is detected by comparing them against a database of signatures or their pattern from known malicious site. By using this technique, browser can have higher performance as browser do not needs to screenshot the browser interface and then compare with the referred element everytime. Malicious website or sensitive elements can be detected by comparing the website that being redirect on online social network with the database. However, it needs to be support by all browsers (Google Chrome, FireFox) in order to get more malicious website database.

If the browser cannot determine whether clickjacking attack is exist in online social network by using signature detection, then next type of detection machine, anomaly detection is used to determine. The detection technique of this proposed solution is totally same with the solution which proposed in InContext. Once the clickjacking attack is detected by using this technique, the malicious site and its expected pattern is then documented in database for signature detection use.

The most common hijacking attack is compromising visual integrity. Traditionally, user confirmation technique or Opaque Overlay Policy is implemented to avoid from clickjacking attacks. However, those solutions meet some security challenges which mention in the earlier section. Developer is the person who understands their application the most and knows their website's security level until which extend. Hence, it will be better if web developer is asked to decide whether their website is allowed to render page in <frame> or <iframe> or JavaScript to run in the page on browser. An additional function or browser plug in that allow developer to set their security extends (whether allow <iframe> or javascript) is proposed. After that, depend on the security settings that decide by developer, browser can detect the clickjacking attack in a more effective ways. For example, if the developer mark certain section has the chance to be attacked, the browser can check that target section more frequent to avoid clickjacking attack. However, it requires developer mark the security setting honestly in order to prevent from clickjacking attacks.

5.0 Case Study 2: Location Leakage

One of the less obvious security issues arise from the increasing use of social media is location leakage, which potentially lead the social media users to physical property loss such as burglary or even endanger the life of the users as it can exposed the user's current location to stalkers or robbers. With the increasing use of smart mobile devices which possess technologies such as GPS and WIFI as the criterion functionalities of the device, users were encourage to use social media anywhere, anytime, and hence enable users sharing information globally regardless of time and location. The security issues arise as the users often unaware that the information that they shared using social me-

International Journal of Scientific & Engineering Research, Volume 5, Issue 7, July-2014
ISSN 2229-5518

dia may contain private and sensitive information including the location of the users, especially with the use of online social network (OSN) application such as Twitter and Facebook.

An example of the potential threats of location leakage lead by usage of social media is showed in the case of an Arizona man named Israel Hyman. Israel claimed that his Twitter message has led to the burglary at his house while his family is out of town. Having approximately 2,000 followers in Twitter, Israel posted tweets that reveal his family is having a vacation in Kansas City. As a result, as he returned from the vacation he found that his home were burglarized and over thousands of dollar worth video equipment were stolen These video equipment is used by Israel for his video business in his Twitter account. He believe that the Tweet about his family going out of town has tell the world including that his home is unoccupied at the specific time, indirectly telling the thieves to visit his house [10].

In this paper, we will present the way that location leakage may happen in social media by organizing it into two types, namely "*Content based leakage*" and "*Geotagging*", which is showed in the following section.

5.1 Security Risks and Challenges

5.1.1 Content Based Leakage

As mention previously, the advanced in technologies such as GPS and WIFI has encourage the use of social media as users can access to it by using their mobile devices anywhere, anytime. For example, the Twitter has experience a outstanding response from the users since the date of its creation in year 2006, reaching a total amount of 232 million active users in the year of 2013 [11]. These users actively posted short messages ("tweets') of 140 characters to their followers. As in the case presented in the section A, these users may share private and sensitive through these tweets, as most of the users has low awareness on the potentially threats in exploring their location to their followers. Other social media such as Facebook also potentially create security issues as it allows users to "check in" upon reaching a destination, showing the users current location to his/her friend's news feed. Moreover, Facebook timeline also contain a feature called "Places", which upon clicked, will shows all the places that the user has been tagged, pictures tagged in different location, etc [12]. This location tracking feature expose the user activity area and could be a threat in exposing the user physical location if the user Facebook account were compromised by hackers.

Similar cases can happen in all other social media such as Craiglist or Youtube. In a paper published by Gerald [13], the authors shows that a person activity area can be traced from the contain of social media such as Craigslist, Twitter, and Youtube. The authors wrote a script using Youtube API, which was able to trace the activity of a user by using data such as location, radius, keyword, and user name. The experiment shows that the script was able to track the user's activity, including where the user is playing with his kid near their home.

A more obvious example of location leakage threat can be found from the website pleaserobme.com [14], where the website was able to indicate the location of empty homes based on the contain of social networking's post especially Twitter. The website perform Twitter search on a Twitter account by using HTML and Javascript, which can than reveal the user's location if the user has posted message related to their location. The developers of this website claim that the website was created in order to raise the awareness among the users regarding the potential threat in sharing their information on social media. Another example can be found in a paper published by Mao [16], where the authors has train classifier that can determine whether the user is on a vacation or not, based on the content of their tweets. The authors claim that they can determine who will go on vacation, where, and when, this hence can provide an opportunities for burglars to know the exact time to visit their victim's house.

Furthermore, the information shared in social media may lead to location leakage even though the user did not purposely post their location or use any tagging services provided by the social media. Researchers have shows that a user location can be revealed by purely analyzing the content of the information they shared even though the information does not contain any geospatial cues [15]. The concept is build based on the intuition that a user's post may include some location- specific content, meaning that a certain words or a certain name will more likely to appear in a specific region. For example, the word "howdy" is used by people from Texas, and the word "rockets" will appears more frequently in Houston, the home of NASA and the NBA basket ball team Rockets.

5.1.2 Geotagging

The previous section has demonstrate how a user location may leak based on the contain of their post, which may include the exact location name, or even without any geospartial cues, which purely based on the terms that only occur in a specific location. If a user were aware of the sensitivity of the data they shared, they might avoid sharing information that can reveal their location. However, most of the users are not aware that even if their post does not contain information mentioned above, their location can still leak because of the technology of Geotagging.

Geotagging is the process of adding geographical information to various media in the form of metadata [17]. These media might include photo, video, websites or even

International Journal of Scientific & Engineering Research, Volume 5, Issue 7, July-2014
ISSN 2229-5518

SMS messages. The metadata consists of various information such as latitude and longitudes coordinate, bearing, altitude, distance and places names. This information is very useful for photographer to record the exact location of a beautiful picture were taken and hence allows them to organize their picture better or revisit the location for another shoot. One may also search for pictures that were taken at a location by providing the coordinate of that location.

The security issues arise when most of the users are not aware that the Geotagging technology is also including in the mobile devices that have GPS functionalities. When a user take a photo using their smart phone, the exact location of the picture is actually also recorded in the EXIF data of the JPG photo, if the GPS function is on. Moreover, some of the mobile devices have the Geotagging function activated on default, and hence recorded the picture's location automatically without the user's conscious. For example, iPhone have the Geotagging function activated by default while Android phone have the function off by default.

Figure 6: A photo that doesn't shows location trait

The figure 5 shows a photo that does not tell the exact location of the photo taken, we can't identify where the photo is taken just by looking at the image provided. Hence, a user may post this photo using social media such as Facebook, Cragslist, or Flickr. The problem arises as this photo actually is Geotagged and contains the location information in the EXIF data. These data can be easily view by using various tools such as Exif Viewer add-on of Mozilla Firefox, or any online EXIF viewer tools such metapicz [18]. As a result, the coordinate of the photo taken can be found easily from the EXIF data as shown in the figure 6, and hence anyone who intended to perform crime can easily locate their victims. For example, if a person posted a photo of jewelry on Cragslist which he intended to sell, then burglary can happen as the thieves can easily obtain the address.

5.2 Proposed Solution

Various mechanisms have been introduced for preserving user's location privacy, these mechanisms normally varied according to the application or services that are using the location information. System such as MobiShare or N-MobiShare is specifically designed for mobile social networking site and required a change in the system architecture design. In this paper, we want to propose solution which is simpler and can be applied widely without restricting to a single application.

The idea of notifying the user as mentioned by Henne [22] and Friedland [13] is the key in preserving the location privacy because human is the biggest threat in security issues. Users often unconsciously expose their sensitive information when they use social media. The proposed idea is to acknowledge the user every time that the user shared information that potentially led to location leakage. The acknowledgement can be done by using add-on or plug-in on the browser that create a dialog box that notify a user if they post a location information. The location information can be detected by using technique that is introduced by Pleaserobme.com [14] or Cheng at al. [15], which it analyze the content of the post and identify terms that is representing a location. This solution is performed using add-on or plug-in of browsers and hence is not restricted to only one application.

The proposed solution above can solve the problem of location leakage in term of the content based leakage, for the Geotagging issues, we want to preserve the location privacy as well as utilizing the benefit from the Geotagging technologies which was useful in recoding the location that a photo or a video is taken or recorded. Friedland [13] has proposed that when a photo is taken or shared, the user should have a control mechanism to determine the degree of location information to be recorded. However, in our proposed solution, we do not want to notify the user for the control for every time that the user takes or share a photo or video. This is because a user such as a photographer may take a thousand of photos per day and prompting for control mechanism every time will be very tedious for the users. In our proposed solution, we suggest that cryptography should be applied to the metadata of the media by the devices that is taking/ recording the photo/ video. Application for mobile devices can be developed and use which once installed will perform encryption on the EXIF data at the time that the photo is taken. These hence allowed the photos to be shared freely because the EXIF data cannot be analyzed as it is encrypted. The encryption can be performed by using simple symmetric key encryption algorithms, which can only decrypt by the owner of the device that own the secret key of the encryption. The security strength of the encryption need not to be too high because the location leakage mostly leads to burglary, which the criminal often does not possess the knowledge in decrypt-

International Journal of Scientific & Engineering Research, Volume 5, Issue 7, July-2014
ISSN 2229-5518

ing the ciphertext.

6.0 EVALUATION OF PROPOSED WORK

Since no experiment is carried out in this paper, hence the evaluation of our proposed solution is done by adopting X.800 Security Service. X.800 is security architecture for OSI which is used to define the requirement for security and characterize the approaches to satisfy those requirements. X.800 focuses on security attacks, security mechanism and security services. In this section, a briefly explanation of security service is discussed before moves to evaluation of proposed solution.

X.800 defines the security service as a service provided by a protocol layer of communicating open system. It is used to ensure the appropriate security level of the system or of the data transfer. X.800 divides security service into five main categories. [9] Five categories of security service in X.800 are shown as below:

Authentication: The function of the authentication service is to assure that the message is from the communicating entity that is the one claimed. There are two aspects of authentication involve in the case of an ongoing interaction. First, two entities' authentication is assured by service at the time of connection initiation. Second, during the connection, the service must assure that the connection between two entities is not interfered by third party for the purpose of unauthorized transmission or reception.

Access Control: The function of access control service is to prevent or limit the unauthorized user access to resource. To achieve this, every user that trying to gain access must be first identified or authenticated first, so that access right can be tailored to them.

Data Confidentiality: Data confidentiality is used to protect the data or resource from unauthorized disclosure.

Data Integrity: Data integrity is used to assure the data or resource that received is exactly same as sent by authorized entity. Integrity can be apply to a stream of message, single message or selected fields within a message. Of course, the most useful approach is total stream protection, which assure the data that received is totally same with the data which sent by authorized entity.

Nonrepudiation: Nonrepudiation is used to protect against transmitted message denial by one of the parties (sender or receiver) in a communication. Hence, when a message is sent, the receiver can prove that so-called sender sent the message and vice versa.

6.1 Proposed solution for case study 1: clickjacking attack

The solution for clickjacking attack that proposed in this paper achieves all the security services that propose in X.800. This is because actually the solution that we suggested is an enhancement for *InContext* and *InContext* actually fulfill all the security service's categories in X.800.

For **authentication**, the browser is proposed to determine whether transparent layer exist or there are JavaScript that designed to be run in a website so that the third party (attackers) wouldn't interfered during the message transmission and hence perform clickjacking attack.

For **access control** part, this proposed solution is designed to prevent the unauthorized user (attackers) to access to the resource (user's confidential data) by enable user only click on the link or do the action that they intended to do. Hence, user will not be redirect to malicious website to enable the attack to gain the access to their confidential information.

For **data confidentiality** part, the proposed solution is target to protect user's confidential information from exposure to attackers.

For **data integrity part**, as mention in earlier section, there are three types of integrity that this proposed solution protecting to prevent attacker from modify the visual and pointer of the web application.

For **nonrepudiation** part, basically it occurred during the message transmission from user to the website. UI delay function is designed to enable user ensures that the action that he intended to do is exactly same with what the system did (message is transmitted to the correct person).

6.2 Proposed solution for Case Study 2: Location Leakage

For the solution of location leakage, it is hard to be justified by using X.800 security services because it is more on educating the user on the security risk rather than securing the data transfer, nevertheless, it still fulfilled some of the X.800 security requirement as show at below:

For **authentication,** the content of the user's shared information is what lead to the location leakage, our solution focused on notifying the user when sharing information, but not authenticating the user's identity when sharing information, hence, this security services is not achieved in this proposed solution.

For **access control,** we proposed encryption to be performed on the EXIF data of the media, and hence only authorized users (the owner of the device that performed the encryption) that have the secret key can access the data, therefore, this security services is achieved.

For **data confidentiality,** user was alert by the browser when they try to share confidential information such as location. This hence can prevent sensitive data to be compromised by unauthorized party that have harmful intention. Metadata of a photo or video is encrypted and hence ensure the data confidentiality is protected.

For **data integrity,** the proposed solution does not involve in ensuring the data transferred is the same as sent, hence this security mechanism is not fulfilled.

For **nonrepudiation,** the proposed solution also does not ensure that a message sender cannot deny the message is sent by him or her.

The proposed solution in the security issue of location leakage is more in a form of enhancing the available services or application security level, hence the security level also varied according to the application. For example,

International Journal of Scientific & Engineering Research, Volume 5, Issue 7, July-2014
ISSN 2229-5518

the add-on or plug-in for browser is proposed in order to increase the user's awareness of potentially sensitive data that may be dangerous, out solution is more in a form of enhancement to the browser functionalities, hence the security level also varied according to the browser used by the users. If the browser achieved all of the security criteria in X.800, then our solution also achieved the criteria. Nevertheless, the most important key feature in countering the problems in location leakage is to raise the user's awareness on the potential danger of sharing information using social media, because in this case users themselves is often the highest risk in exposing their location data.

7.0 Conclusion & Future Works

The use of social media created a lot of potential threat in security issues of preserving the user information, which is often unaware by the users. Our research work has exposed the different type of security risk in social media including classical threats and modern threats. A review on different type of defense mechanism has provide the reader a brief understanding on what are the available countermeasure against the security threat in social media. By presenting two case studies, we have successfully given a deeper review on two specific security threat which is clickjacking and location leakage. We also proposed solutions to encounter the two security threat mentioned, which is positively evaluated by using the X.800 security services standard. These proposed solutions reworked on the current defense mechanism and provide a better protection mechanism.

In conclusion, this research paper has exposed the potential threats in social media which may be used to raise the awareness among the users, and we have proposed solutions for two specific threats. In our future work, we can focus on providing more detail and technical implementation of our proposed work. Furthermore, more case studies can be review to expose the potential threat to the social media users.

References

[1] *Social Media and its Origin, Review of Social Media and Defenc.* [Online]. Available: http://www.defence.gov.au/pathwaytochange/docs/socialmedia/1.%20Social%20media%20and%20its%20origins%20SM.pdf

[2] Jacka JM and Scott PR, *Auditing Social Media – a governance and risk guide*, 2011.

[3] Zhan Shi, Huaxia Rui and Andrew B. Whinston, *Content Sharing in a Social Broadcasting Environment: Evidence from Twitter,October 2013*

[4] Micheal Fire, Roy Goldschmidt and Yuval Elovici, *Online Social Networks: Threat and Solutions*, Unpublished

[5] G. Wondraeek, T.Holz, E. Kirda and C. Kruegel. *A pratical attack to de-anonymize social network users, In Security and Privacy (SP)*, 2010 IEEE Symposium on, pages 223-238, IEEE,2010

[6] Huang, L.S., Moshchuk, A., Wang, H.J., Schechter, S., Jackson, C.: *Clickjacking: Attacks and defenses:* In: Proceedings of the 21st USENIX conference on Security symposium (2012)

[7] *'Lady Gaga Found Dead in Hotel Room' Facebook Likejacking scam leads to Malware*, September 20,2011 [Online] Available: http://www.spywareremove.com/lady-gaga-found-dead-in-hotel-room-facebook-likejacking-scam.html

[8] Ubaid Ur Rehman, Nazar Abbas Saqib, *On Detection and Prevention of Clickjacking Attack for OSNs* 2013 11th International Conference on Frontiers of Information Technology, pages 160-165

[9] *Introduction of X.800* [Online]。Available: http://www.deic.uab.es/material/26118-capitol1.pdf

[10] Elinor Mills, *Twitter user says vacation tweets led to burglary*, June 8, 2009, [Online] Available : http://www.cnet.com/news/twitter-user-says-vacation-tweets-led-to-burglary/

[11] Jim Edwards, *Twitter's 'Dark Pool': IPO Doesn't Mention 651 Million Users Who Abandoned Twitter*, Nov 6, 2013 [Online]. Available: http://www.businessinsider.com/twitter-total-registered-users-v-monthly-active-users-2013-11?IR=T&

[12] Andy O'Donnell, *Facebook Places Location Tracking Creeping You Out? Turn it OFF!*, December 29, 2012 [Online]. Available: http://netsecurity.about.com/b/2012/12/29/facebook-places-location-tracking-creeping-you-out-turn-it-off.htm

[13] Gerald Friedland, Robin Sommer, *Cybercasing the Joint: On the Privacy Implications of Geo-Tagging*, '10 Proceedings of the 5th USENIX, CA, USA, article no. 1-8, 2010

[14] Barry Borsboom, Boy van Amstel, Frank Groeneveld, *Please Rob Me: Raising awareness about over-sharing*, [Online]. Available: http://pleaserobme.com/

[15] Zhiyuan Cheng,James Caverlee,Kyumin Lee, *You Are Where You Tweet: A Content-Based Approach to Geo-locating Twitter Users*, CIKM'10, , Toronto, Ontario, Canada, pp. 759-768, October 26–30, 2010

[16] Huina Mao, Xin Shuai, Apu Kapadia, Loose Tweets: An Analysis of Privacy Leaks on Twitter, WPES'11,, Chicago, Illinois, USA, pp1-12, October 17, 2011

[17] Cory Janseen, *Geotagging*, [Online] Avalaible: http://www.techopedia.com/definition/86/geotagging

[18] Marco Rucci, Roberto Scatena, Laura Jeanne Hornbake, *Metapicz* [Online] Availaible: http://metapicz.com/#landing

[19] Landon P. Cox, Angela Dalton, and Varun Marupadi, *SmokeScreen: Flexible Privacy Controls for Presence-Sharing*, MobiSys'07, New York, USA, pp 233-245 June 11-14, 2007

[20] Wei Wei, Fengyuan Xu, Qun Li, *MobiShare: Flexible Privacy-Preserving Location Sharing in Mobile Online Social Networks*,INFOCOM, 2012, Orlando, FL, pp 2616 - 2620, 25-30 March 2012

[21] Zheli Liu, Jin Li, Xiaofeng Chen, Jingwei Li, Chunfu Jia, *New Privacy-Preserving Location Sharing System for Mobile Online Social Networks*, P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), 2013, Compiegne,pp. 214 - 218, 28-30 Oct. 2013

[22] Benjamin Henne, Christian Szongott, Matthew Smith, *SnapMe if You Can: Privacy Threats of Other Peoples' Geo-tagged Media and What We Can Do About It*, WiSec '13, New York, NY, USA, pp. 95-106, 2013

[23] Amirmohammad Sadeghian, Mazdak Zamani, Bharanidharan Shanmugam, *Security Threats in Online Social Networks*, ICICM'13, Kuala Lumpur, Malaysia, pp. 254 - 258, 4-6 Sept. 2013

International Journal of Scientific & Engineering Research, Volume 5, Issue 7, July-2014
ISSN 2229-5518

International Journal of Scientific & Engineering Research Volume 5, Issue 7, July-2014
ISSN 2229-5518