IOSR Journal of Engineering
e-ISSN: 2250-3021, **p**-ISSN: 2278-8719,
Vol. 2, Issue 12 (Dec. 2012), ||V4|| PP 63-68

Real-time Protection Mechanism for Social Networking Sites Using Proxy Server

Swapnil S Matsagar [1], Abhinandan P Shirahatti [2]
[1]*Departments of CSE, St. Mary's College of engineering and Technology/ JNT University, India*
[2]*Departments of CSE, VTU Jnana Sangama, Belgaum-590014, India*

Abstract:- **In the past few years, Social Networking (SN) websites such as Face book, Orkut, twitter and MySpace become very popular.** ***SN sites are defined as interactive web-based applications that provide users with the ability to join groups, chat, share photos, and organize events and network with others in a similar-to-real-life manner.*** **In the past few years, social networking website has become a popular networking culture. It has been proven that friends can keep in touch and share feelings, as well as Collaborating research and network marketing through social networking website. Although young generation is fond of these applications, social networking websites also encounter a number of privacy threats. These threats reveal the information security risks of social networking websites such as internet fraud, identity theft, virus and phishing. We propose a real-time website security protection mechanism based on the concept of proxy. The client side transmits information to the social networking website through proxy. The main function of the proxy is to detect and determine the security threats of the website. These threats include web-based malware, phishing websites and malicious connection. The idea is to integrate many commercial protection software and online security scanning services into a security module, simultaneously execute webpage security threat scan, then scan the information sent by the web server with the security module before sending to the client. If security threats were found in the web page, the system will add this web page to the blacklist and issue a warning to the client side to prevent attack. The functionality of proxy is to segregate the client and the networking threat. Using simultaneous scan of many protection software and online services can increase the recognition rate of security threats. Later one, as long as the client is to receive the webpage in the blacklist, a warning will be issued directly to the client side. Through this mechanism, we can lower the security risk of the clients using social networking websites. Popular interactive application services such as games, psychological tests and fan communities can also be used to conduct Trojan, virus and web linked code attacks, or even money transfer scams. For this reason, the security threats of social networking websites, such as Face book, Orkut, twitter and MySpace needs to be investigated and ameliorated.**
.

Keywords - *Information security, personal data, social networking website, face book, proxy.*

I. INTRODUCTION

In the past few years, Social Networking (SN) websites such as Facebook, Orkut, twitter and MySpace become very popular. SN sites are defined as interactive web-based applications that provide users with the ability to join groups, chat, share photos, and organize events and network with others in a similar-to-real-life manner. In the past few years, social networking website has become a popular networking culture. It has been proven that friends can keep in touch and share feelings, as well as Collaborating research and network marketing through social networking website. Although young generation is fond of these applications, social networking websites also encounter a number of privacy threats. These threats reveal the information security risks of social networking websites such as internet fraud, identity theft, virus and phishing. Its browsing rate in the United States surpassed Google in March 2010. This means Social Networking is a very popular internet community service. Social networking websites gather a large amount of user data including name, picture, birthday, contact information, gender, political orientation, religion, personal interests and educational background. These data are open to the public by default; hence increase the risk of personal privacy leakage. Popular interactive application services such as games, psychological tests and fan communities can also be used to conduct Trojan, virus and web linked code attacks, or even money transfer scams. For this reason, the security threats of social networking websites, such as Face book, needs to be investigated and ameliorated.

II. FACEBOOK

A. The Origin and Website Structure of Facebook

Facebook is a global social networking website. It is founded by Mark Zuckerberg, a student of Harvard University and his friends in 2004. Anybody can become the member of Face book as long as he or she has a valid email account. Face book is a highly interactive website. Currently, there are billions of members worldwide. As shown in Fig. 1, there are three roles of Face book website structure: (1) the client side, (2) the Face book server and (3) the application server. When the client request for website application, it sends regular http request to the official server. The official server will transfer such request to the dedicated Face book Markup Language (FBML) and send the request to the application server. The application server then responds to the office server using FBML. The official server will then convert it to regular http webpage before sending it to the client. Face book uses the three-layer interactive relation to accomplish all user requests...

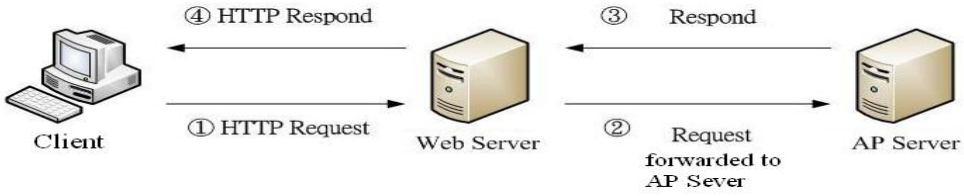

Fig. 1. Facebook website structure

All of the user's personal information is stored in the Face book social networking website. Due to high usage rate, it became the target of networking attacks. For example, after the user registers successfully, some personal data is displayed by default, including name, pictures, birthday, contact information, gender, political orientation, religion, personal interests and educational background. As long as the user enters complete and accurate information, all other users in the website can see this information. Hackers can take advantage of these information to conduct social engineering, junk mail or even telecom fraud.

B. Facebook Communities

Users of Facebook can establish community freely. Communities can gather users with similar interests or fields. Fans community establishes a common platform for certain meaningful person or object. Communities are collections of a large amount of personal information. Hackers can steal all of the user information. In addition, all users have similar characteristics. It is even easier to achieve the attack objective.

C. In-Game Virtual Currencies

The most popular applications in social networking websites are web games, which can be developed unrestrained. Both of Happy Harvest and Happy Aquarium are popular web games in Taiwan. Some items in the games need to be paid by the players with cash or credit card; other items may be acquired by questionnaire. Hackers can take advantage of these requirements to conduct fraud or steal player's personal data through questionnaire.

III. FACEBOOK WEBSITE THREATS

In practice, many cases reveal that social networking websites may encounter security threats and attacks.

1. Social Engineering: Use fake Facebook account to notify the members that for security reasons, users need to reset their account, or to open malicious email attachment to reset their account.
2. Revealing personal data: 32 millions of unencrypted personal data of Rock You Inc., a Facebook application developing company, were revealed due to hacker intrusion.
3. Drive-by Download: Hackers infringe Facebook applications and inject malicious links or codes. A fake Adobe authorization agreement window may pop up and asks users to install programs when they are using these applications.
4. Phishing: Psychological test such as "Werewolf and Vampire" uses fake webpage to ask users to answer question and enter data. At the end of the game, it asks users to enter cellular phone number to receive test result. As long as the users enter the cellular phone number, it means they also agree to pay 9 pounds every week as the membership fee.

5. Trojan: The Bredolab Trojan uses fake Facebook account to send emails to the users for password update. Users should open the attached compressed file to acquire new password. Once they do so, they will also download the Trojan and then download other malicious program automatically.
6. Criminal cases: Young girl meets Facebook friend and being killed. Terrorists recruit and liaise through Facebook.
7. Fake friendship invitation: Use false friend data to invite other people in order to steal user data.
8. Facebook Query Language (FQL): Facebook proprietary syntax used to access user data in the database. The official server uses FQL to search for user data when receiving request from the application.

IV. FACEBOOK THREAT ANALYSIS AND PROTECTION INVESTIGATION

Threat analysis can be conducted in two aspects. First, we can analyze the functional distribution of social networking website. The website functionality can be divided into three categories: Social networking service (SNS), network application service (NAS) and communicate interface (CI). The second aspect is to analyze threats through the core principles of information security , i.e., confidentiality, integrity and availability (also known as the CIA triad). We then show the analysis results with various tables.

A. Analysis Through Website Functionality

TABLE I compares the potential threats and website functionality. With this information, we can analyze which website functionality is most likely to bring security threat.

Table I : Website Functionalities That May Lead to Security Threats

Threat	Functionalities		
	SNS	NAS	CI
Social engineering	✓	✓	
Revealing personal data	✓	✓	
Drive-by download		✓	✓
Phishing		✓	✓
Trojan		✓	✓
Criminal cases	✓		
Fake friendship invitation	✓		

1) SNS: The main functionality of SNS is to establish social network or interactive relationship for people who have the same interests and activities. These services are usually based on the internet. They offer various kinds of vinculum and interaction channels such as email and instant messaging services.
2) NAS: Social networking provider offer transmission and network interaction services to the users. For example, community, fans community, psychological test and interactive web games… etc.
3) CI: Social networking provider offer platforms for user interaction and communication.

B. Analysis through the Core Principles of Information Security

1) Confidentiality: This triat is to prevent information from being accessed by unauthorized individual, entity or procedure. In terms of social networking website, confidentiality means user privacy. How to protect personal data from being accessed by unauthorized person is an important issue. Using access control can achieve clear-cut information revealing. Actually, through access control, one can segment the read and publish objects.
2) Integrity: This triat protects data from being tampered to ensure true, accurate and complete data. User identity and data must be protected from unauthorized modification or alteration. In fact, falsified account and person is not uncommon in social networking website. This could lead to security breach. Therefore, registration approval and the secrecy of login data are important and deserved further investigation.
3) Availability: This is defined as the property of data being accessible and useable by authorized individuals upon request . Some professional tools of the social networking website help users to develop their business or career. Therefore, user published data must be available continuously. Other than offering data accessibility, the system must ensure the data availability after message exchange between members.

C. Protection Investigation

Through the analysis results, we suggest the following methods to enhance the security of social networking website for both of the client side and the official server side.
1) Client side

1. Social Engineering: Use fake Facebook account to notify the members that for security reasons, users need to reset their account, or to open malicious email attachment to reset their account.
2. Refer to personal privacy protection programs and solutions offered by scholars such as Faceloak [1], NOYB [2], Flyby Night [3] …, etc..
3. Make sure each other's identify before adding to friend list. This can avoid personal data stolen by hacker with bogus identity
4. Avoid revealing too much personal information when conducting psychological tests.
5. Purchase virtual currency through legal channel.
6. Cautiously review fans groups and communities before joining them.
7. Carefully check every application before installation.

2) Official server side

1. Use https or SSL for user login. This can prevent login information being intercepted due to plain text transmission.
2. Strengthen the verification of application service developer's identity and their software security.
3. Conduct periodical security auditing to game developing vendors to avoid user information leakage from the game developing vendors.
4. Use secured channel to transmit data between servers.

V. REAL-TIME WEBPAGE SCANNING SERVICE

This paper proposes a concept of using cloud computing to construct real-time webpage security scanning module. The infrastructure shown in Fig. 2 uses proxy to collect many online anti-virus and online webpage security scanning services. In addition it combines webpage scanning software to simultaneously scan the webpage security of which user is about to browse. The scanning result is stored in the black list if the webpage is threatening. The black list is used to raise warning whenever the user wants to browse the webpage in the list.

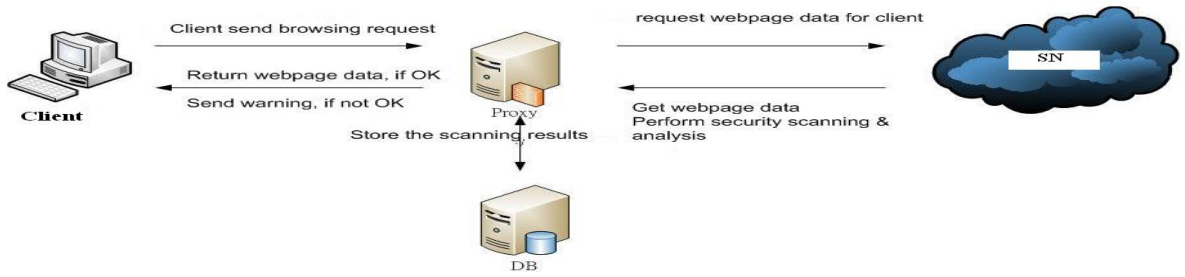

Fig. 2. Infrastructure of real-time webpage security tool

A. Service Process

Fig. 3 and 4 represents the process of the entire service. It consists of five steps:
1. User use browser to request for visiting webpage.
2. Instead of crawling the desired webpage, browser redirects the request to the proxy.
3. Proxy sends the URL to online webpage analysis service [6-10] which will then download the web content for security scan.
4. Relate online webpage service and local scanning result. Store the comparative analysis result into the database. Add the URL to blacklist and respond warning message to the user, if it potential threat exists.
5. When any user request to browse the same webpage later on, proxy will send warning message to the user directly according the black list.

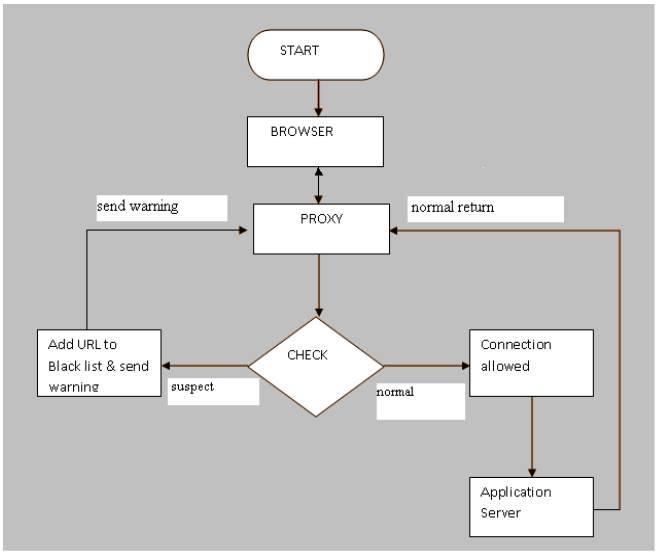

Fig. 3. Flowchart of real-time webpage security tool

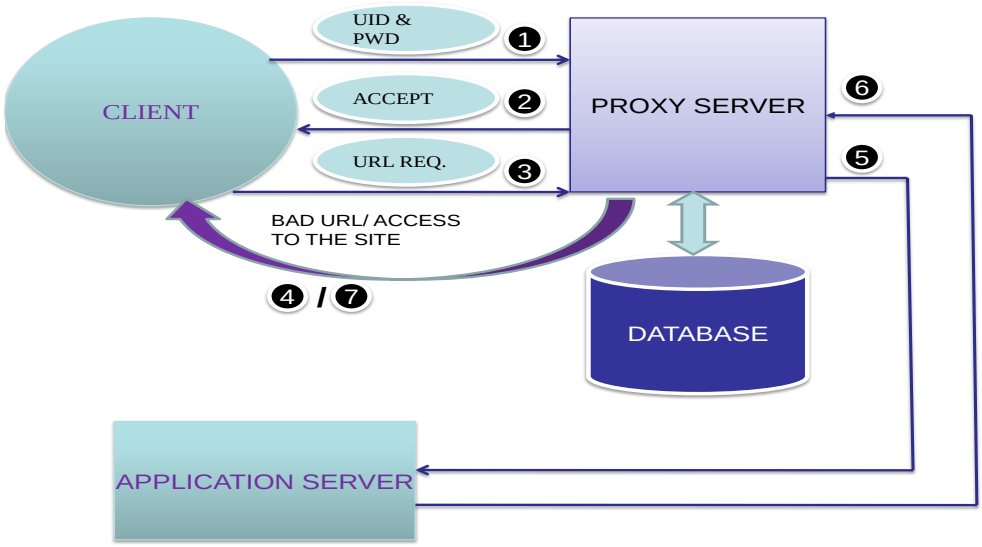

Fig.5.4. Data flow in the entire system

1) Every Client is provided with a UserID and Password. Client first enters his/her UserID and Password.
2) There is a Database maintained for Users to check weather Client is a valid user or not. A message named "Accepted" is sent back to the valid user.
3) Client sends a URL Request.
4) If the requested URL is present in the black list maintained by Proxy Server, the Proxy Server sends back a message saying "URL Banned."
5) Else forwards the request to the desired Application Server.
6) The Client can get a safe access to the site now.

Table II: Pros and Cons of Real-Time Webpage Scanning Service

Pros	Cons
● Increase scanning correction rate ● Isolate user ● Real-time scan ● Avoid contact of risky webpage repeatedly ● Warning mechanism	● Network connection needs to be maintained continuously ● Confirm service status at all time ● Periodically update service and software

VI. CONCLUSION

This paper proposes the current information security threats that may encountered by social networking website such as Facebook. We conduct cross analysis of these threats with the service infrastructure of social networking website and the CIA triad. Finally, we use TABLE I to represent the threat distribution of the Facebook social networking website. We also propose suggestions and improvement solutions for both of the user and the official website. Back to the reality, the most important issue for internet security is highly rely on the correct habit of browsing the internet. Therefore, we would like to reinforce the information security concept for all of the users using social networking websites. Finally, we introduce the concept of webpage security scanning service through cloud computing to provide internet users a more secured networking environment. Though we do not provide effective data due to the entire framework still needs to be sorted out. However once the whole real-time scanning module is completed, it should provide relatively stronger security mechanism to the user browsing the web pages.

REFERENCES

1). Wanying Luo , Qi Xie, Hengartner, "FaceCloak: An Architecture for User Privacy on Social Networking
Sites" in Computational Science and Engineering, August 2009, pp. 26-33.

2). S. Guha, K. Tang, and P. Francis, "NOYB: Privacy in Online Social Networks," in Proc. of 1st Workshop on Online Social Networks(WOSN 2008), August 2008, pp. 49–54.

3). M. M. Lucas and N. Borisov, "flyByNight: Mitigating the Privacy Risks of Social Networking," in Proc. Of 7th ACM Workshop on Privacy in the ElectronicSociety (WPES 2008), October 2008, pp. 1–8.

4). Joseph Bonneau, Jonathan Anderson , George Danezis "Prying Data out of a Social Network" in Social Network Analysis and Mining, July 2009, pp. 249-254

5). Facebook Developers, "FBML," http://wiki.developers.Facebook.com/index.php/FBML

6). The Frontline, "Facebook launches widespread UK safety campaign,"http://thefrontline.v3.co.uk/2010/04/Facebooklaunch.html

7). Online Link Scan, http://onlinelinkscan.com/

8). Browserdefender, http://www.browserdefender.com/

9). Linkscanner, http://linkscanner.explabs.com/linkscanner/avg/

. **BOOKS:**

1) ASP.NET Database Programming.
-By Jason Butler and Tony Caudill.

2) C# for building .NET Applications.
-By Eric Butow and Tommy Ryan.

3) Microsoft ADO .NET Step by Step.
-By Rebecca M. Riordan.

4) Beginning ASP.NET 3.5 in C# 2008.
-By Matthew MacDonald.

5) Professional ASP.NET 3.5 In C# and VB.
-By Bill Evjen Scott Hanselman Devin Rader