Security Protection Mechanism for Social Networking Websites Based on Real-Time Proxy

Komal Navale¹, Rajendra Pisal², Vishal Suravase³, Santosh Reddy⁴

¹(CSE, JCEM/ Shivaji University, India)
²(CSE, JCEM/ Shivaji University, India)
³(CSE, JCEM/ Shivaji University, India)
⁴(CSE, JCEM/ Shivaji University, India)

ABSTRACT

During the last two decades Information technology has grown tremendously and became the main source of knowledge. In past few years the world getting closer and closer this is only because of Social networking websites such as Facebook, Twitter etc. Yet with usefulness and the popularity, the misuse and cybercrime are more evident. So prevention and detection of these threats is become a major challenge

To minimize this risk of accessing social networking applications we proposed an application. The idea is to integrate many commercial software and online security services into a security module, simultaneously execute webpage security threat scan, then scan the information sent by the web server with security module before sending to the client. If security threats were found in the webpage, the system will add this web page to the blacklist and issue a warning to the client side to prevent attack. Later on, as long as the client is to receive the webpage in the blacklist, a warning will be issued to the client side. Through this mechanism, we can lower the security risk of the clients using social networking websites.

Keywords - Information security, personal data, social networking website, Facebook, proxy

I. INTRODUCTION

A social networking service[1] is a platform to build social networks or social relations among people, for example, share interests, activities, backgrounds or real-life connections. Social networking is web-based services that allow individuals to create a public profile, to create a list of users with whom to share connection, and view and cross the connections within the system. Although young generation is fond of these applications, social networking websites also encounter a number of privacy threats. These threats reveal the information security risk of social networking websites such as internet fraud, identity theft, virus and phishing.

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 transfers scams. For this reason, the security threats of social networking websites, such as Facebook, needs to be investigated and ameliorated.

This paper declares that proposed application is divided into four modules namely Social networking application, Security Module, Sample Attacks, Proxy. Social networking application is a sample social networking application which includes the some basic functionality such as add friends, remove friends, search friends etc. Security module uses the some security software’s and online security services to prevent and detect security threats. The module proxy is from where client side requests are diverted to the web server of requested website. Proxy server downloads the data of the requested website and analyses that data against the threats. And if the website was found as threaten then the warning message is sent to the client side. The next time whenever the client side request for the same website then the proxy send warning message to the client side directly instead of analyzing that website.

II. METHODOLOGIES

This paper declares that proposed application is divided into four modules namely Social networking application, Security Module, Sample Attacks, Proxy. Social networking application is a sample social networking application which includes the some basic functionality such as add friends, remove friends, search friends etc. Security module uses the some security software’s and online security services to prevent and detect security threats. The module proxy is from where client side requests are diverted to the web server of requested website. Proxy server downloads the data of the requested website and analyses that data against the threats. And if the website was found as threaten then the warning message is sent to the client side. The next time whenever the client side request for the same website then the proxy send warning message to the client side directly instead of analyzing that website.

Fig. Represents the process of the entire service.

It consists of five steps:

1. Client uses a browser to request for particular social networking website.

2. Instead of crawling the requested webpage, the 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. And if the requested website were found threaten the proxy then add the URL to
blacklist and respond a 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.

III. SCOPE

The system 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. If the requesting webpage threatening the warning message is sent to the client and scanning result is stored in the black list.

Whenever the next time user wants to browse the same webpage in the list the blacklist used to raise warning.

IV. LITERATURE SURVEY

IV.1 THREAT

A threat to a computer system is defined as any potential occurrence, either accidental or malicious, that can have an undesirable effect on the assets and resources of the organization. The most common threats to an individual or organization involving the Internet or Web include the following:

- Virus
- Trojan Horse
- Worm
- Scams
- Malware

IV.2 WEB THREAT

Web threat is any threat that uses the internet to facilitate cybercrime. Web threats use multiple types of malware and fraud, all of which utilize HTTP or HTTPS protocols, but may also employ other protocols and components, such as links in email or IM, or malware attachments or on servers that access the Web.

- Phishing
- Web browser exploit
- Third party add-ons
- Download
- Hybrid Attack

IV.3 MECHANISMS IN MALICIOUS WEBSITES

The victims who visit the malicious websites will be redirected and exploited by the Web-based Trojans, implemented in scripting languages including JavaScript.

IV.3.1 STRATEGIES FOR REDIRECTING VISITORS TO WEB-BASED Trojans

To redirect the visitors to the actual Web-based Trojan, attackers are typically using one of the following three categories of strategies.

V. EMBEDDED HTML TAGS

Embedded HTML tags such as iframe, frame, and others, are used to embed the Web-based
Trojan into the source code of the website. The aim of this HTML element is to create an inline frame that displays another document. When that page is opened, the included document is displayed in the inline frame. Thus attackers take advantage of this to include the Web-based Trojan directly, setting the iframe to be invisible by setting the height or width of the iframe to zero or a very small value, for example:

```html
<iframe src="URL to Trojan" width="0" height="0" frameborder="0"></iframe>
```

V.1 TROJAN HORSE

Trojan horse attacks are accomplished by inserting malicious code into other people’s programs. When the user executes their program, they unintentionally execute the Trojan horse program. Many current web sites insert a small piece of code like a cookie into your browser file, which may contain a Trojan horse.

V.2 MALICIOUS SCRIPTS

The second category uses the script tag to include Web-based Trojan scripting or redirector scripting, which are often XSS (Cross-Site Scripting) vulnerabilities.

V.3 EMBEDDED OBJECTS

The third category of strategies is based on the embedded object tag for activating third-party applications like Flash or Baofeng media player or Browser Helper Objects to display the embedded object. When vulnerabilities in these applications and BHOs are found, attackers then use this strategy to inject the objects to the vulnerable applications, which exploit them in order to remotely execute code on the victim’s machine.

V.4 ARP SPOOFING

This is another advanced strategy to build malicious websites when the attackers cannot gain control of the target website. The attacker uses ARP spoofing in order to act as a Man-in-the-Middle, and hijacks all of the traffic from and to the victims in the same Ethernet subnet. The attacker then injects malicious code into the HTML responses from the target website, or all of the web traffic, to achieve virtual malicious websites.

VI. MODULES

VI.1 SOCIAL NETWORKING APPLICATION

Now-a-days social networking websites have become a popular networking culture. It has been proven that people can keep in touch and share feelings, as well as collaborating research and network marketing through social networking websites. We design a simple sample social networking application which is used to set profile, add and ignore friends requests, send messages to friends, search etc.

VI.2 SECURITY MODULE

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.

VI.3 PROXY

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.

VI.4 SAMPLE ATTACKS

We are using some sample attacks such as Fragmentation Attack, size Of Attack etc. application to make attack over sample social networking.

VII. CONCLUSION

We have designed architecture for mitigating the privacy risks of using a social networking site. Our design strikes a balance between protecting the users' privacy and maintaining Facebook's usability. We argue that, although some privacy and security risks remain, the threat of privacy compromise is greatly reduced because our architecture raises the cost of technical privacy attacks and shifts the communication medium to one in which a user may hold a reasonable expectation of privacy and thereby enjoy an accompanying legal framework for privacy protection.

VIII. REFERENCES

Books: