

Privacy of Facebook's Native Chat Application

Vikrant Agarwal

Francis Gbormittah

Mike Hanley

Devon Rollins

Abstract

In this paper, we have analyzed the Facebook chat application. We implemented a Man in the Middle (MITM) attack on the same. Our analysis indicated that if users A and B are chatting, the MITM can redirect A's messages to a third friend, C. The MITM can also edit these messages. Hence, C will think that A is chatting with him/her and A has no knowledge of the same. This was accomplished by capturing the Facebook chat packets and analyzing/editing them.

The paper also contains detailed comments on this situation from the policy, privacy as well as managerial aspects of the Facebook chat application's security.

1. Introduction

Instant Messaging (IM) is increasingly popular among members of the online community. A survey in 2004 by Pew Internet & American Life revealed that more than four in ten adults online use instant messaging. This amounts to approximately 54 million American adults. The survey indicated that 24% of adult instant messengers utilize IM more frequently than e-mail. Six percent indicated they use IM as much as they use e-mail. Moreover, approximately 11 million of these adults IM during work and "...[are] fond of its capacity to encourage productivity and interoffice cooperation" (Eulynn Shiu 2004). IM is becoming a ubiquitous form of communication adopted by people of all ages. This less formal channel of communication encourages people to divulge information they would not typically during any physical interaction.

As a result, there has been a proliferation of IM programs. Some of these programs require a client download; others are web-based while the rest come integrated into an already existing service (e.g. Gmail chat).

2. Facebook

On March 18, 2008, Facebook declared its intention to include IM capabilities. A *CNETNews.com* article, ironically titled “Facebook fires up IM, ratchets up privacy”, pointed out that “Social networking site Facebook will roll out more extensive privacy controls as well as an instant messaging service soon after that.” The report highlighted Facebook’s concerns with privacy on its site and indicated that, “...the new Facebook friend-adding interface, will be integrated with privacy controls and Facebook members will also be able to include or exclude certain friends from having access to information”. (McCarthy 2008).

According to the report, Facebook company executives are attaching a lot of importance to privacy as a result of the “ongoing evolution of the social network” and explained that “changes to the site's privacy controls are necessary given its rapid growth and increasingly diverse user base” (McCarthy 2008). Moreover, Matt Cohler, vice president of strategy and business operations, reiterated that the social network is designed to facilitate better, more-personal ways to share and communicate information. Essentially, “Facebook's product allows users to have control over their personal information.”

However, the report clearly underscored the importance that Facebook attached to the privacy of user information on its social networking site with respect to both native and non-native applications. This importance is hardly misplaced in view of recent trends within the online social networking community. However, it seems that the continued emphasis on user privacy may have created a set of expectations regarding the privacy of communications on Facebook. We believe this trust and set of expectations can be exploited using technical measures such as a man-in-the-middle attack, to be discussed shortly.

According to anti-spam firm Cloudmark, “in six months leading up to March 2008, 30% of new accounts created at several major social networking sites are

automated fraudulent “zombie” accounts, designed to be used for spam and other malicious attacks” (CyberInsecure.com 2008). According to another online report, “social networks like Facebook and MySpace are perfect models for the three D's of insecurity: insecure by design, insecure by default and insecure in deployment” (Roiter 2008). The report quotes security consultants who spoke at the 2008 Black Hat briefings, as saying that “security is clearly not part of the business model for owners of these wildly popular Web properties and that when sharing something on a social network, assume it’s going to be public” (Roiter 2008). This trend gives serious cause for concern considering the growth in the usage of IM as well as the typical habits of IM users. Another online article titled. “Popularity for instant messenger on social utility Facebook grows” reports that in less than 30 days after the launch of Facebook’s IM, “users have sent over one million messages to each other in real-time conversation with thanks to a month old instant messenger application” (Hawkes 2008). One key concern that arises from this is the attackers’ ability to intercept and misuse sensitive, private information. A fair amount of research has been carried out in this area with respect to non-native or third party applications on a number of social networking sites like MySpace and Facebook.

Security consultants at the black hat briefings demonstrated “a series of all-too-easy MySpace attacks, which combine social engineering and technical hacks against an end-user population hungry for peer interaction and imbued with trust.”⁴ Moreover, the consultants claim that, “MySpace, Facebook and other social networking sites offer wide-open APIs. These not only allow unrestricted data exchange with any application, but also permit attackers to tap into user applications and exploit site code that's wide open to cross-site scripting and other attacks.”⁵

Adrienne Felt’s research in July 2007 at University of Virginia looked into the privacy protection of Facebook Users with respect to third party applications. Contrary to her work, we will explore Facebook’s native chat application and the

level of privacy protection that it provides it's more than 110 million active users (Facebook site statistics n.d.) who exchange all kinds of information on this social networking site. There are expectations to privacy and our research will showcase how this property is not guaranteed.

In our studies, we will illustrate that the Facebook chat application is vulnerable to many different types of attacks. Data can be gleaned from these attacks by a malicious third party.

3. Experimental Configuration and Tools

In our research, we devise a proof of concept detailing how a man in the middle attack can occur when using the IM technology along with the Facebook platform. Wireshark, formerly known as Ethereal, is the network packet analyzer we selected for this research. Our goal was to see if Wireshark would allow us to identify the underlying communications of the Facebook native chat application. Wireshark "is a measuring device used to examine what is going on inside the network cable." The data would be stored in a *.pcap (standing for "packet capture") file for further investigation. The methodology entailed "sniffing" the network, while two users communicated via Facebook native chat. This would give insight as to what data was enveloped with the message to the recipient. It would also highlight how the data was sent and what privacy implications could be extracted. Wireshark was set to sniff the network in promiscuous mode, which implies that all data would be captured through the interface card whether it was meant for the sniffing machine or not. In hindsight, this analysis served as a microscopic view of the data flow harnessed through the communication channels of the chat application embedded into every Facebook user's profile.

The environment was a typical computing environment for most end users. It consisted of a local area network comprised of three machines. Each machine represents a user who will be referred to as *Alice*, *Bob*, and *Eve*. Alice and Bob both

access Facebook to communicate through the native Facebook chat application. Eve inconspicuously sniffs all traffic on this network, and will be our “attacker” [for the purposes of this paper]. As data is transmitted, Eve is able to gather all the information between the nexus of Alice, the Facebook server, and Bob. With each user a strategically placed “man in the middle” attack was constructed. (See Figure 1 for an illustration.)

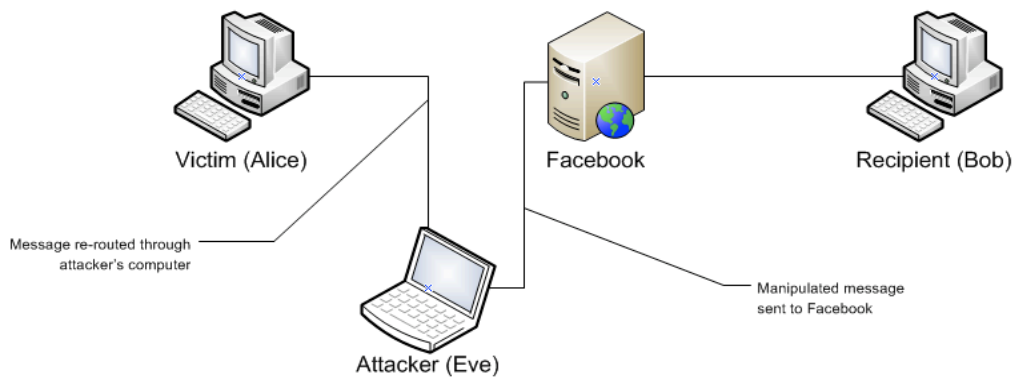


Figure 1 - “Man-in-the-middle” with message manipulation

According to Bruce Schneier, “In a man-in-the-middle attack, the attacker inserts himself between two communicating parties. Both believe they're talking to each other, and the attacker can delete or modify the communications at will.” (Schneier 2008) As data was transferred between Alice and Bob, it was captured for further analysis. The data uncovered the results as shown below.

attack degrade the integrity of the user identities in the social networking space. This alludes to other issues that can be exposed with data collected from Facebook chat. For instance, the email address of the sender is captured and could be subjected to spamming or spoofing. This will impair network effects as users of the site are interacting with an expectation that the “online identity” matches the “offline identity” (Acquisti 2002).

Other information identified in the network capture log indicates that other variables can be seen and modified. As mentioned by Cody Rester, Facebook is vulnerable to several attacks, which make use of POST requests, information submitted to be processed through a form on a webpage. Information transmitted from the native chat application makes use of this method, thus leaving the door open for our attack vector. Rester explains, “The problem with POST requests is when the requests are allowed to be submitted without being checked for unauthorized uses. One such method to curb, if not completely stop unauthorized requests, is to include a random ID string that is sent with the rest of the data submitted to the server” (Rester n.d.). This intrusion allows full access and authorization as they masquerade as a legitimate user.

These issues are evidence that innocuous data is easily aggregated to harm end users and others in their social networks. Facebook should take further initiative in protecting this data and adhering to the privacy policies they have set forth. The problem is momentous because gathering data is relatively simple, and it is used to thwart an enjoyable user experience. The information is deployed to friends on a native application that explicitly allows users to state their privacy preferences. This is very misleading and serves as a major indicator that privacy standards are not being subjected to extended applications. As we traverse the attack vector, the implications become larger.

4. Manipulation and Redirection Attacks

As we know that there is data of interest to a third party being sent out, we can now explore some different types of attacks. The attack vector is modified as Eve attempts to modify the message sent from Bob to Alice. This part of the experiment was done using Paros, a tool to analyze the security of web based applications. According to the documentation, “through Paros’s proxy nature, all HTTP and HTTPS data between server and client, including cookies and form fields, can be intercepted and modified” (Paros Proxy – Web Application Security Tool n.d.). With this tool, we looked to simulate the systematic process a hacker would follow in order to compromise the integrity of the message, redirect the destination, and assume the identity of the sender.

With Paros, the data captured was very similar to the results of Wireshark. The Paros interface provided a detailed view of the POST and GET methods used to request information from the Facebook server and its corresponding response to the client. This information is vital to the assessment as information is channeled through the Paros proxy, which has a feature to trap the message before it is forwarded to the server. Consequently, the contents of the chat message were captured, modified and forwarded to the intended recipient as depicted in *Figure 3* and *Figure 4*.

```
for (,):{"f":"msg","c":"p_668340166","ms":[{"type":"msg","msg":{"text":"I'm going to try and change this message","time":1223062907176,"clientTime":1223062906588,"msgID":"2798031445"},"from":11200214,"to":668340166,"from_name":"Devon Rollins","to_name":"Vikrant Agarwal","from_first_name":"Devon","to_first_name":"Vikrant"}]}
```

Figure 3: Original message sent by Alice intended for Bob

```
for (,):{"f":"msg","c":"p_668340166","ms":[{"type":"msg","msg":{"text":"I'm going to try and change this message TO SOMETHING NEW","time":1223062907176,"clientTime":1223062906588,"msgID":"2798031445"},"from":11200214,"to":668340166,"from_name":"Devon Rollins","to_name":"Vikrant Agarwal","from_first_name":"Devon","to_first_name":"Vikrant"}]}
```

Figure 4: Message being modified by Eve

The message is sent in verified by Wireshark, along with metadata associated with the message. This flaw poses severe implications to the validity associated with the chat application available to every end user of the social network. Interestingly

enough, the message is forwarded and displayed in the chat interface. Bob would have no indication the message has been changed.



Figure 5: The Facebook chat interface displays the modified message with no alert to Bob.

We verified the capability to modify both messages on their way to Facebook from a user, and messages Facebook sends to the receiver. Now, taking this a step further, we tried to redirect a message to a third person Joe, when Alice and Bob were chatting. The scenario is as follows: Alice sends a message to Bob, is the intended recipient, yet Eve is able to intercept the message and redirect it, contents intact, to a chosen third party, which we will call Joe.

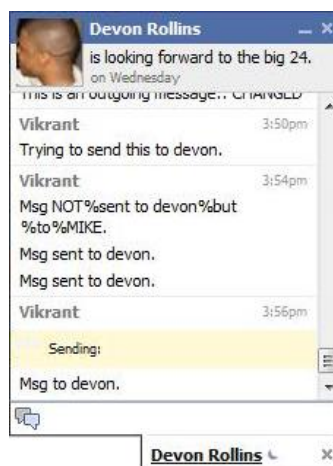


Figure 6: Alice sending the original message to Bob.

The MITM (Eve) catches the message from Alice to Bob and changes the message to redirect it to Joe as depicted in Figure 7 and Figure 8.

```
msg_text=Msg%20to%20devon.&msg_id=477902068&client_time=1223063802147&to=11200214
&popped_out=false&num_tabs=2&pvs_time=1223063712952&post_form_id=9da7880bdc595961de605496898dafd5
```

Figure 7: The original message that Alice was sending to Bob.

```
msg_text=Msg%20to%20devon%NOW%MIKE.&msg_id=477902068&client_time=1223063802147&to=529219218
&popped_out=false&num_tabs=2&pvs_time=1223063712952&post_form_id=9da7880bdc595961de605496898dafd5
```

Figure 8: The original message being sent by Alice as changed and redirected to by Eve.

A sample outcome of a scenario combining our modification and redirection attacks is illustrated using the screenshot below. Alice saw both messages, the original one to Bob and the changed one to Joe. This is the top half of the screenshot. On the bottom left is Bob's chat, which shows the original message from Alice. On the bottom right is Joe's screen, which shows the altered message from Alice. Figure 8, displays the chat screens for Alice, Bob and Joe and provides a holistic view of the scenario.

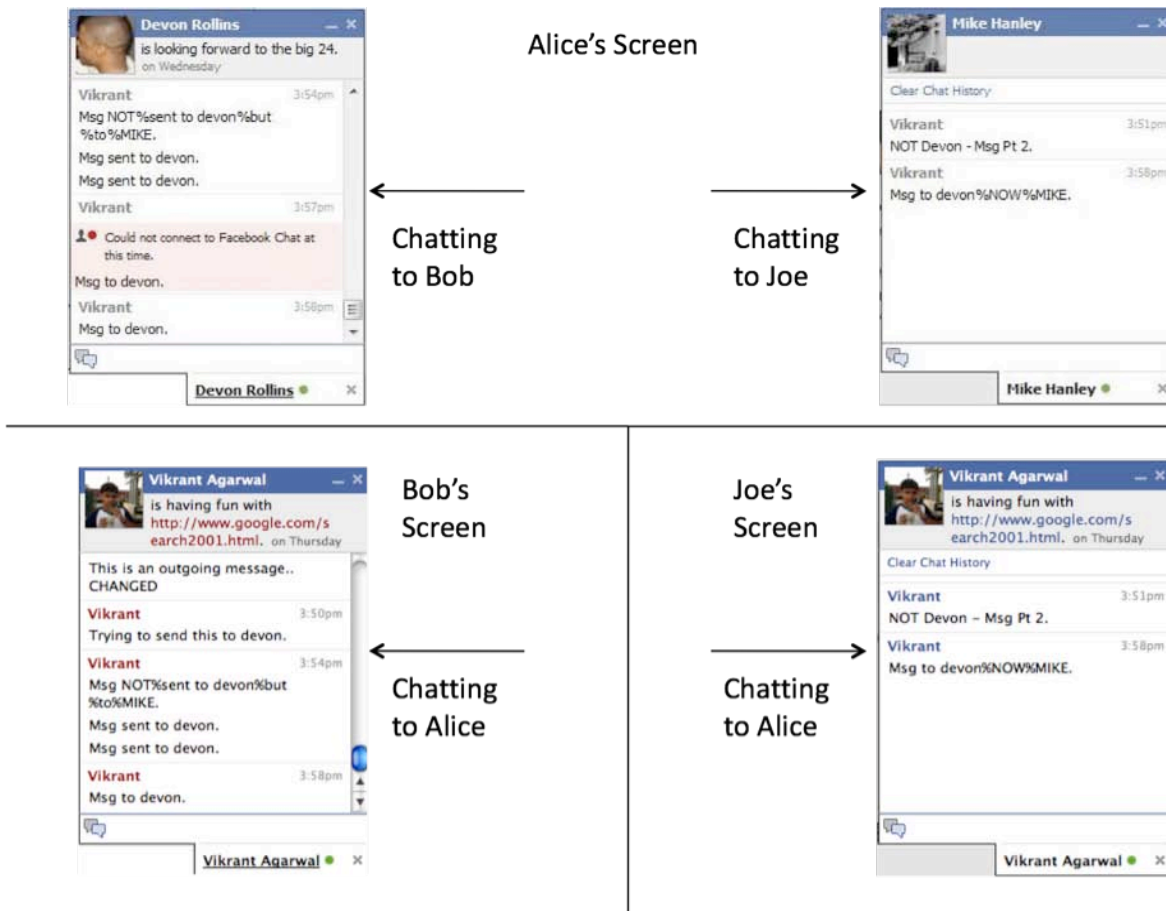


Figure 9: Alice chatting to Bob and Eve. Bob receives the original message as sent by Alice but Eve receives the altered message by the MITM.

The extent of potential data disclosure does not stop here. For example, as shown in Figure 10, a summary of the last several messages exchanged between Alice and Bob is sent with each new message. This history shows the UIDs of Alice and Bob, as well as the exact timestamps of the messages exchanged. Hence, the MITM could not only snoop on the current conversation, but by using packet capturing with a tool like Paros, Eve could also see the previous messages exchanged. This has the potential to seriously impact the security policies of Facebook. On one hand they claim to give the user control of what data they want exchanged yet they send out details of previous chats, without any user knowledge or consent.

```
for ({});{"error":0,"errorSummary":"","errorDescription":"No error.,"errorsWarning":false,"payload":{"history":[{"msg":{"text":"hey"},"from":668340166,"to":11200214,"time":1222707414594,"type":"msg"},{"msg":{"text":"whats going on"},"from":11200214,"to":668340166,"time":1222707431458,"type":"msg"},{"msg":{"text":"nm"},"from":668340166,"to":11200214,"time":1222707468757,"type":"msg"},{"msg":{"text":"u tell me"},"from":668340166,"to":11200214,"time":1222707474752,"type":"msg"},{"msg":{"text":"are u going to be able to make it today"},"from":11200214,"to":668340166,"time":1222707477022,"type":"msg"},{"msg":{"text":"oh ya"},"from":668340166,"to":11200214,"time":1222707481683,"type":"msg"},{"msg":{"text":"I'm in the library now"},"from":11200214,"to":668340166,"time":1222707482656,"type":"msg"},{"msg":{"text":"okay cool"},"from":11200214,"to":668340166,"time":1222707485054,"type":"msg"},{"msg":{"text":"i skipped the session"},"from":668340166,"to":11200214,"time":1222707485802,"type":"msg"},{"msg":{"text":"alright, well get to the library...lol"},"from":11200214,"t
```

Figure 10: A part of the chat transcript leaked by Facebook.

The other data that Facebook ‘leaks’ are Alice’s Facebook friends who are online when Alice is chatting to Bob. It leaks their Unique UID, Name, Profile photo link, Status and Status last updated as shown in Figure 11. This data is also sent in the clear to “Eve.” Now the attacker also gathers some secondary information used to target future attacks.

```
usTimeRef":"","514081384":{"name":"Saaniya Abbas","firstName":"Saaniya","thumbSrc":"http://profile.ak.facebook.com/W225V248V78Vq514081384_589.jpg","status":"acts like summer and walks like rain, listens like spring and talks like june.,"statusTime":1223020255,"statusTimeRef":"12 hours ago"},"577456236":{"name":"Chinmay Bijwe","firstName":"Chinmay","thumbSrc":"http://profile.ak.facebook.com/vprofile5V1420V101Vq577456236_4073.jpg","status":"is longing for a long weekend! (this 1 finished before I realised it started!),"statusTime":1222647878,"statusTimeRef":"on Sunday"},"583443973":{"name":"Shreesh Mangrulkar","firstName":"Shreesh","thumbSrc":"http://profile.ak.facebook.com/W224V1883V51
```

Figure 11: The details that were sent out about all of Alice’s friends who ~~happened to be~~ were online at the same time.

We also conducted a mini-study on Gtalk, {Google’s Instant Messaging application}, in comparison with Facebook. We discovered interesting results there as well. Gtalk sends out messages in the clear but also sends out reset packets every few seconds, which makes it a little harder to change messages on the fly. Also, the length of the message is constant, so one cannot change the message length, just the message content within the same length.

Hence, we can conclude, that the chat data is susceptible to attack not only on the Facebook chat application, but on other major IM platforms as well.

5. Concerns

Our “attack” demonstrations depict some clear concerns relating to Facebook users privacy. First, we can look at our basic observation of user communication with Wireshark, or a related network analysis tool kit. Content of user communications

is transmitted in clear text between the user and Facebook's servers, and vice versa. Anyone skilled with network capture can read the message content with a high probability of translating the UID strings in the messages back to an actual user by inputting the UID string into a URL in the following format:

```
http://www.new.facebook.com/profile.php?id=<UIDstring>
```

Where <UIDstring> is set equal to the user's UID, this should allow you to at least display a user's picture, name, and their network affiliations. Given that network affiliations also give you some idea of whether or not the user is a student, what class level they are, and a general idea of their geophysical location, an attacker can obtain a wealth of information about this user even if the above URL does not allow you one to browse the full profile due to the user's privacy settings. A perfect example of this particular exploit stems from user of UID = 4. If we craft the URL:

```
http://www.new.facebook.com/profile.php?id=4
```

we are taken to the search results for Facebook's founder, Mark Zuckerberg. Regardless of whether we can read his entire profile, we know Zuckerberg's place of employment, educational background, and regional location from the network affiliations displayed. Furthermore, we have a name and a photograph of the user (in this case, Mark), two incredibly valuable pieces of information to reconstruct the observed conversation. Since we noted that most IM system users disclose information via IM that they would not normally say in person, the attacker can reconstruct valuable information to use for blackmail. Additionally, the information can be used to discredit someone's reputation, or attempt identity theft.

Another primary concern involves the manipulation of message content between two users. If in the message modification scheme described earlier, we have Alice and Bob exchanging information, and the messages that Bob receives from Alice have been intercepted and modified by Eve (our attacker), there is an asymmetry

created in the information flow. Since Alice is unaware that her messages have been modified, responses from Bob might be written under a completely different context and with entirely different content depending on the degree to which Eve elected to tamper with the conversation. Since Eve has a choice to make few modifications with no change in overall meaning or to change the message to something completely unrelated and potentially damaging to Bob and Alice's online conversation, this attack can be incredibly versatile. The degree with which Bob can be offended, feed misinformation, or otherwise manipulated is entirely up to Eve.

More important is combining message manipulation with message redirection. If Alice and Bob are exchanging private information via the chat, and Eve has the capability to redirect the messages to the user of her choice by changing the target recipient UID, then by extension, Eve also has the ability to disclose sensitive information from at least one side of the conversation to a third party.

These issues raise the question of message repudiation with respect to redirected or modified messages. If Alice intends to send an innocuous message to Bob, but it is modified en route by Eve, Bob has no idea that Alice intended to send anything other than the manipulated message that is displayed on his screen. Alice also has no idea that anything other than what she intended was delivered to Bob. Thus, we may have the problem where Bob is now under the impression that Alice is of some opinion X on a topic, when actually she was of opinion Y. Assuming the conversation stops here, this may impact future exchanges. Bob now has false information that he has incorporated into his knowledge of Alice, potentially limiting future conversations. This creates communication inefficiency via the spread of false or damaging information.

Combining the message redirection and manipulation attacks with Wireshark observation acts as a force multiplier for these attacks. If Eve were sufficiently motivated to observe Alice and Bob's chat sessions over a time frame, Eve may be able to find patterns in the conversation. These patterns would assist Eve in

executing a highly sophisticated social engineering attack against Alice and Bob. The potential for personal data interception and disclosure has been amplified with only minimal reconnaissance.

6. Future Work

Given additional time and the results of our basic attack mechanisms, it may not only be possible to redirect and modify communications, but it may also be possible to forge messages to either mask the real sender or to attempt to discredit a user by forging and sending a message that appears to be from them. The availability of such an attack strikes at the core of the application's integrity, because it opens up the possibility that users may have no control over messages that appear to come from them. Additionally, they have practically no means by which to repudiate whether or not the message was sent by them. In the absence of security mechanisms such as digital signatures or other identity-verification measures, leaves the system vulnerable to a wide range of compromising attacks.

However, our initial findings indicate that message forgery is beyond the degree of difficulty that most attackers will be willing tackle. Unlike the key fields we used for our redirection attacks and message manipulation attacks, the traffic leaving Facebook and getting sent to message recipients has some key parts encrypted, such as sender ID. The ease with which we were able to construct the first sets of attacks suggests that with sufficient time and a sufficiently large sample size of captured messages, this system can be exploited at will.

Furthermore, we see a great deal of value in exploring the economics of false personal information spread via instant message forgery. We asked the question during our research of what differs between the attitudes of users with respect to protecting their privacy on Facebook and the attitudes of users toward the spread of false information or of their impersonation on Facebook. We suspect that there may

be certain incentives for attackers to engage in this type of malicious activity, and also believe that there may be certain measures by which users might choose to defend against this type of misinformation campaign. Again, given additional time, this is something that merits further exploration.

At the present time, we recognize that there is little we can do to change the way users communicate via instant message. That said, there may be ways for Facebook to make good on their promises of privacy through various technical countermeasures to the attacks we have detailed in this paper. Using SSL to encrypt traffic between users and the Facebook may be one way to help deter all but the most highly motivated attackers from attempting to exploit this vulnerability. This, however, has its own issues, including the added overhead required to encrypt and decrypt communications that may create some delay in communication between users. Though this does not completely address the attack vector, it does provide Facebook with improved credibility with respect to their privacy claims.

7. Source List / Bibliography

Bibliography

Acquisti, Alessandro. "Privacy and Security of Personal Information: Economic Incentives and Technological Solutions."

www.heinz.cmu.edu/~acquisti/papers/acquisti_eis_refs.pdf, 2002: 4-7.

CyberInsecure.com. *30% of new major social networking accounts are fraudulent*. May 14, 2008. <http://cyberinsecure.com/30-percent-of-new-major-social-networks-accounts-are-fraudulent/>.

Eulynn Shiu, Amanda Lenhart. "How Americans Use Instant Messaging."

www.pewinternet.org. September 01, 2004.

http://www.pewinternet.org/~media/Files/Reports/2004/PIP_Instantmessage_Report.pdf

Facebook site statistics. <http://www.facebook.com/press/info.php?statistics>.

Felt, Adrienne. "Defacing Facebook." July 2007. <http://www.cs.virginia.edu/felt/privacy/>.

Hawkes, Rachel. *Popularity for Instant Messenger on Social utility Facebook grows - Social Media Portal*. February 12, 2008.

McCarthy, Caroline. 'Facebook fires up IM, ratchets up privacy'. *CNET News*. March 18, 2008. http://news.cnet.com/8301-13577_3-9896860-36.html.

"Paros Proxy." *Web Application Security Tool*. <http://www.parosproxy.org/index.shtml>.

Rester, Cody. "Demonstrating the Insecurity of Facebook."

Roiter, Neil & Westervelt, Robert. *Black Hat roundup, Social Networking sites insecure by design*. August 11, 2008.

Schneier, Bruce. "Schneier on Security: "Man-in-the-Middle Attacks"." July 2008. http://www.schneier.com/blog/archives/2008/07/maninthemiddle_1.html.