Anonymous Communication and its Importance in Social Networking

Nguyen Phong HOANG, Davar PISHVA
Institute of Information & Communications Technology, APU
(Ritsumeikan Asia Pacific University), Japan
Corresponding Author: dpishva@apu.ac.jp, Fax: +81 0977 78 1001, Tel: +81 0977 78 1000

Abstract— **Digital information has become a social infrastructure and with the expansion of the Internet, network infrastructure has become an indispensable part of social life and industrial activity for mankind. For various reasons, however, today's networks are vulnerable to numerous risks, such as information leakage, privacy infringement and data corruption. Through this research, the authors tried to establish an in-depth understanding of the importance of anonymous communication in social networking which is mostly used by ordinary and non-technical people. It demonstrates how the commonly used non-anonymous communication scheme in social networking can turn the Internet into a very dangerous platform because of its built-in nature making its users' identity easily traceable. After providing some introductory information on internet protocol (IP), internal working mechanism of social networking and concept of anonymity on the Internet, Facebook is used as a case study in demonstrating how various network tracing tools and gimmicks could be used to reveal identity of its users and victimize many innocent people. It then demonstrates working mechanism of various tools that can turn the Facebook social networking site into a safe and anonymous platform. The paper concludes by summarizing pros and cons of various anonymous communication techniques and highlighting its importance for social networking platforms.**

Keywords— **Security, Privacy, Network Tracing Tools, Anonymous Communication Tools, Social Networking, Facebook**

I. INTRODUCTION

We live in the era of Information and Communication Technology (ICT) and the Internet has become a dominant means of communication and an indispensable part of modern life. Adoptions of cloud computing, mobile applications and virtualized enterprise architectures have led to an expansion of applications that are connected to Internet resources [1]. Just to mention a few examples, we use Internet for various sorts of communication like VoIP and email, multimedia services like Online Music and Online Movie, business transaction like e-Banking and e-Business, administrative work like e-Governance and e-Administration, networking activities such as Online Advertising and Social Networking. Furthermore, along with the development of Internet, e-Commerce has become an efficient marketing tool for many companies and Social Networking with Facebook is an emerging market which has recently become the most visited website in the world.

Nevertheless, it is the fact that privacy is implicated in e-Commerce because of the risk involved in disclosing personal information such as email addresses or credit card information, which is required for most electronic transactions. Specific privacy concerns in this realm include use of customers' information by companies for electronic surveillance (e.g., 'cookies'), email solicitation (e.g., 'spam'), or data transfer (e.g., when customer database information is sold to third parties or stolen) resulting in identity or credit card theft [2-3]. As such approaches could unconsciously victimize both technical and non-technical users, anonymous communication is becoming more and more important on Internet environment since it can protect people's right to online privacy and reduce the possibility of getting recognized and thus victimized.

In recent years, because of dramatic increase in the use of social networking platforms by many non-technical people, social-engineering technique is also being widely exploited to victimize users. According to the 2013 Data Breach Investigations Report [4], cyber threat derived from social-engineering technique is increasing dramatically as shown in Figure 1:

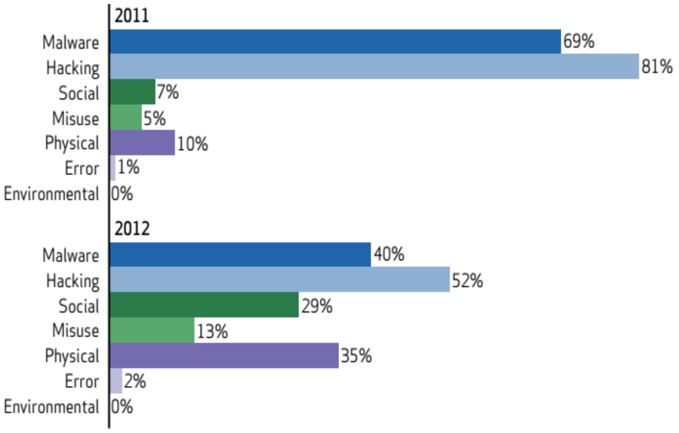


Figure 1. Threat action categories in 2011 and 2012 [4]

Although its percentage is still low compared to “Malware” and “Hacking”, threat caused by social-engineering intrusion has increased by more than 4 times within the past one year. Considering the rapid development of social networks, it can be foreseen that social engineering intrusion will continue to increase in the coming years, thus necessitating appropriate countermeasures.

The underlying factors behind all these issues are operating nature of the communication protocol used in the Internet domain and availability of many free software that can carry out most of these attacks. The Internet protocol suite which is commonly known as TCP/IP (Transmission Control Protocol and Internet Protocol), is used for most Internet applications. IP serving as its primary component carries out the task of delivering packets from source host to destination host solely based on the IP addresses contained in the packet headers. In order to achieve proper operation of such transaction worldwide, this requires source and destination to have unique IP address and included it in the packet headers of their information packets. Since every IP address is associated with a unique entity, identity of IP address holders can be traced using their IP addresses contained in the packet headers. There are numerous techniques that can achieve such objective and this paper highlights some of the important and commonly used approaches.

II. Vulnerability of Facebook Users

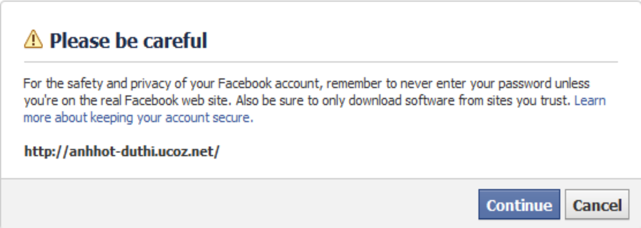
This section will briefly discuss some of the techniques that are employed to victimize Facebook users at random or in a pinpointed fashion by taking advantage of the nature of Internet Protocol (IP), built-in functions of Facebook, innocence and curiosity of Facebook users.

A. Random Facebook Phishing

Phishing is a good example of social engineering intrusion technique. About a decade ago, when email services such as Gmail and Yahoo mail were becoming more and more popular, phishing was used as an efficient mechanism to lure those innocent Internet users who easily provided their own personal information to “phishing email” that contained a link to a fraudulent web page which appeared legitimate, contained company’s logos, content and a form requesting many private information such as home address, phone number, ATM card's PIN, etc.

In recent years, Facebook not only has grown to become one of the most popular social networking platform for many people to communicate and share information, but also turned to be a productive marketing channel for a lot of companies, retailers, business entities and the Facebook itself. With an approximately 1.15 billion monthly active users as of June 2013 [5], Facebook has turned out to become a high-potential target for cyber criminals. Furthermore, with phishing Facebook, a hacker just needs to tempt the innocent users to fill in only their Facebook ID and password. The aftermaths of releasing such information can be more detrimental than the effect of those which were revealed through phishing email since huge amount of private information such as user’s address, birthday, job, education history, hobbies, friends, relationship and a bunch of other sensitive information could be accessed from the Facebook account.

Although Facebook filters all URLs which link its users to an external website and warns them of fraudulent websites, the approach does not always work. For example, after clicking to the link: *http://anhhot-duthi.ucoz.net/*, which is a fraudulent website created by a Vietnamese hacker, Facebook will warn the user about the vulnerability of the site through a dialog box shown in Figure 2. This, however, does not always happen since hackers keep on creating new fraudulent web pages in order to penetrate through loopholes of Facebook’s security. Furthermore, oftentimes, non-technical people may unconsciously press the “Continue” button instead of the “Cancel” button.



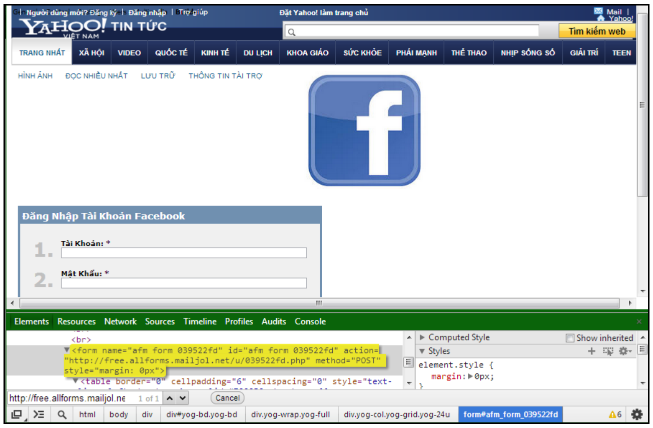
⚠ Please be careful

For the safety and privacy of your Facebook account, remember to never enter your password unless you're on the real Facebook web site. Also be sure to only download software from sites you trust. Learn more about keeping your account secure.

http://anhhot-duthi.ucoz.net/

Figure 2. Vulnerability warning of Facebook

Now let us see what happens when either Facebook’s security does not detect the above mentioned fraudulent website or a user clicks the “Continue” button. As shown in Figure 3, the control would transfer to a phishing site that has the appearance of Yahoo Vietnam website, containing Facebook Logo and a login form which resembles that of the official website. Although a technical user could easily display HTML view of the page to determine where the information would be sent, some innocents



Đăng Nhập Tài Khoản Facebook

1. Tài Khoản: *

2. Mật Khẩu: *

```
<br>
▼<form name="afm form 039522fd" id="afm form 039522fd" action=
"http://free.allforms.mailjol.net/u/039522fd.php" method="POST"
style="margin: 0px">
  ▼<table border="0" cellpadding="6" cellspacing="0" style="text-
```

```
element.style {
  margin:▶0px;
}
```

http://free.allforms.mailjol.ne 1 of 1

Figure 3. An example of a phishing website “http://anhhot-duthi.ucoz.net/”

users may just fill up the form and press the submit button. As indicated in the highlighted section of Figure 3, information content of the form would simply be sent to *http://allforms.mailjol.net/*, a site which provides free Form-to-Mail service. In other words, filling out the form and pressing "submit" button, will transfer ID and password of Facebook user directly to the email address of the attacker.

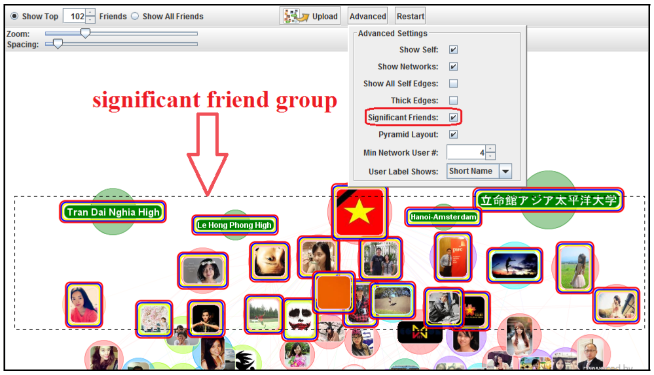
B. Targeted Facebook Phishing

After obtaining the first victim's Facebook account, the attacker can easily exploit more users in a targeted manner by taking advantage of Facebook's internal working mechanism and the victim's personal information.

1) Using "Important Friends" Feature of Facebook

Facebook has a built-in feature called "important friends" the function of which is to internally keep track of people with whom a Facebook user communicates frequently and shares some commonality (e.g., same high school, hometown, fan page, etc.). Whenever important friends write a post, or give a comment; it appears on their respective homepages as news feed. Using data mining techniques and associating Facebook users with "nodes" and time required for spread of information among them as distance, one can easily compute for the shortest path in Facebook social network in order to transfer information from a given source to a desired destination in the shortest period of time or trace source of the information at a given destination [6].

There are many data mining tools which can extract such information through a Facebook account, and for demonstration purpose the authors have used TouchGraph to show a visual image of a Facebook account's important friends. As shown in Figure 4, even an ordinary user can visually display important friends of a Facebook account by checking "Significant Friends" feature of the TouchGraph software. This implies that after victimizing a Facebook account through random Facebook phishing, the attacker can employ such technique to carry out targeted Facebook phishing attacks towards the important friends of the victim. Since in targeted phishing Facebook, the phishing link is being sent from Facebook account of an important friend, i.e., trustable and authentic source, it may easily persuade the recipient friend to click the link and supply the requested information. The chain reaction of such approach will enable the attacker to easily victimize many Facebook users in a short period of time.



● Show Top 102 Friends ○ Show All Friends

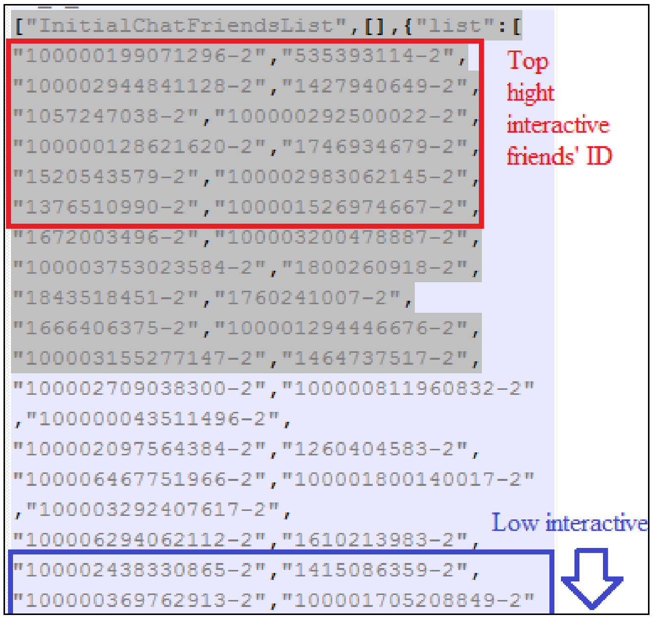
Advanced Settings

Show Self: ☑
Show Networks: ☑
Show All Self Edges: □
Thick Edges: □
Significant Friends: ☑
Pyramid Layout: ☑
Min Network User #: 4
User Label Shows: Short Name

Figure 4. Mining of Facebook data with TouchGraph

2) Using "Initial Chat Friends List" of Facebook

By examining HTML source code of a victim's Facebook, which can easily be done by most web browsers, an attacker can easily access "InitialChatFriendsList" of the account as shown in Figure 5. The list contains Facebook ID of friends with whom the account holder interacts, arranged in descending order of the interaction frequency rate. Using the ID information, targeted Facebook phishing can again be carried out by incorporating ID of high-interactive friends from this list into http://www.facebook.com/[ID] to contact vulnerable friends of the victim. This is another example of successful Facebook phishing as it appears to come from trustable source and has chain reaction effects.



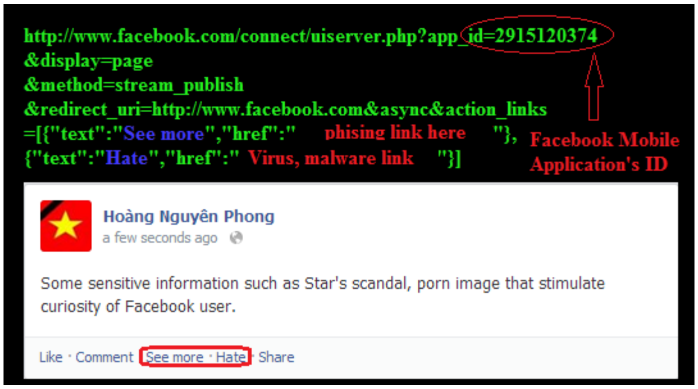
```
["InitialChatFriendsList",[],{"list":[
"100000199071296-2","535393114-2",
"100002944841128-2","1427940649-2",
"1057247038-2","100000292500022-2",
"100000128621620-2","1746934679-2",
"1520543579-2","100002983062145-2",
"1376510990-2","100001526974667-2",
"1672003496-2","100003200478887-2",
"100003753023584-2","1800260918-2",
"1843518451-2","1760241007-2",
"1666406375-2","100001294446676-2",
"100003155277147-2","1464737517-2",
"100002709038300-2","100000811960832-2"
,"100000043511496-2",
"100002097564384-2","1260404583-2",
"100006467751966-2","100001800140017-2"
,"100003292407617-2",
"100006294062112-2","1610213983-2",
"100002438330865-2","1415086359-2",
"100000369762913-2","100001705208849-2"
```

Figure 5. Viewing Facebook's HTML source code

3) Employing IP Address Extraction Techniques

Personal information can also be extracted from IP address of a destination host as explained earlier. This section shows how an IP addressed can be extracted from its data request packet headers and type of personal information recoverable from the IP address. As a demonstration, we will use Facebook Mobile Application to easily generate a post that has more buttons than usual on Facebook to tempt other Facebook users click on it and lead them to a phishing page, a malware-embedded link or an IP-spy link. The trick here is to stimulate curiosity of other

Facebook users so that they feel inquisitive and click on the buttons. The idea is shown in Figure 6 wherein a hot content encourage viewers to click the encircled “See more” or “Hate” buttons and consequently direct them to malicious side as shown in red on its source code.



```
http://www.facebook.com/connect/uiserver.php?app_id=2915120374
&display=page
&method=stream_publish
&redirect_uri=http://www.facebook.com&async&action_links
=[{"text":"See more","href":"    phising link here    "},
{"text":"Hate","href":" Virus, malware link    "}]
```

Hoàng Nguyên Phong
a few seconds ago

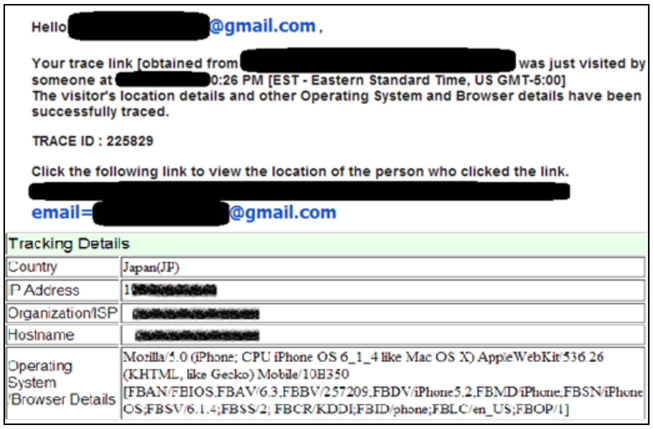
Some sensitive information such as Star's scandal, porn image that stimulate curiosity of Facebook user.

Figure 6. Code to generate a phishing post on Facebook

There are many freely available IP logger software which take advantage of the operating nature of Internet Protocol (IP) to extract IP address from the packet headers and show the associated private information. Figure 7 shows some examples of such IP logger software and their associated URLs. Even an ordinary hacker can easily created an IP-spy link using any of the IP-spy software shown in Figure 7 and insert the IP-spy link in the “See more” or “Hate” links of Figure 6. Most of these IP-spy software are designed in such a way that make it difficult for victims to even know that they are being spied and enable attackers to generate invisible URL which can be encoded to an image, or redirect the access to another trusted website by the time a victim click on it.

Figure 7. Freely available IP logger software

Figure 8 shows an example of personal information retrieved by IP-spy software. Using the above information, the attacker can penetrate into victim’s PC by means of various IP-attack tools contained in Kali or Backtrack which are Linux based penetration tools.



Hello [redacted]@gmail.com ,

Your trace link [obtained from [redacted] was just visited by someone at [redacted]0:26 PM [EST - Eastern Standard Time, US GMT-5:00]
The visitor's location details and other Operating System and Browser details have been successfully traced.

TRACE ID : 225829

Click the following link to view the location of the person who clicked the link.
[redacted]
email=[redacted]@gmail.com

Tracking Details	
Country	Japan(JP)
IP Address	1[redacted]
Organization/ISP	[redacted]
Hostname	[redacted]
Operating System /Browser Details	Mozilla/5.0 (iPhone; CPU iPhone OS 6_1_4 like Mac OS X) AppleWebKit/536.26 (KHTML, like Gecko) Mobile/10B350 [FBAN/FBIOS;FBAV/6.3;FBBV/257209;FBDV/iPhone5,2;FBMD/iPhone;FBSN/iPhone OS;FBSV/6.1.4;FBSS/2; FBCR/KDDI;FBID/phone;FBLC/en_US;FBOP/1]

Figure 8. Victim’s information spied by IP-spy tool

III. Anonymous Communication

Considering the above examples, it is clear that Internet users in general and social network application users in particular are vulnerable to numerous personal information leakage. Therefore, the concept of anonymity on Internet, which has been introduced in recent years to help Internet users protect their privacy from getting disclosed, is quite important. This section examines numerous anonymous communication techniques which are available on Internet, identify their advantages and disadvantages, and recommend a particular method that is most suitable for social networking.

A. Anonymous Mode of Internet Browsers

Recently almost all Internet browsers have added a built-in anonymous mode such as “Incognito” in Google Chrome, “Private Browsing” in Firefox and “InPrivate Browsing” in Internet Explorer. In order to determine extent of their reliability, the authors conducted some simple tests. The investigation showed that anonymous surfing mode of the above browsers did not leave any trace when anonymous modes were utilized. However, by means of an embedded IP-spy URL at the server side, one could still trace IP information of the user. Furthermore, even though anonymous browsing mode cleans cookies, the cleaning is done after the browser is closed. In other words, while surfing in anonymous mode, tools like Wireshark can capture the cookies and use them for real time attacks.

B. Anonymity via Proxy

Proxy is a step forward to prevent the Server side from logging IP address and other relevant information of Internet user. As shown in Figure 9, when Proxy is used the only thing that server can see is just the IP address of Proxy Server and not that of the real IP address of client. Hence, Proxy has become a popular method, particularly to access websites that have put some geographic or governmental access restrictions on certain clients or countries. However, even with the use of Proxy Server,

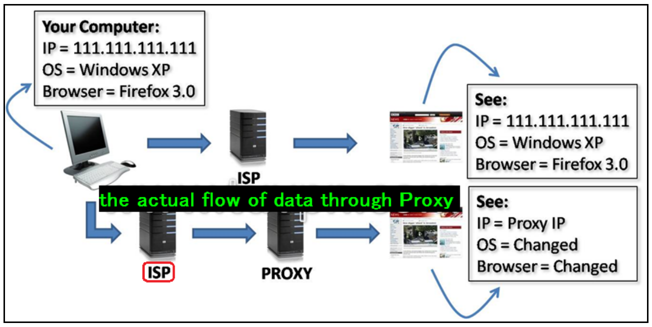


Figure 9. Data flow through proxy server

the data has still to pass through user's Internet Service Provider (ISP) first as indicated in Figure 9. This means that though with the use of Proxy Server, a client can hide their IP address from the final destination, the address is still available to the ISP. In other words, the ISP itself or an attacker along the route to ISP can capture packets sent out from a particular IP address by means of traffic analysis methods to discover private information.

C. *Anonymity via Virtual Private Network (VPN)*

In order to solve the key problem of Proxy, VPN is introduced with a higher level of security. As shown in Figure 10, VPN encrypts all of the packets sent out from client's PC and send it to VPN server through a tunnel called "Secure VPN Tunnel" which is established between the client's PC and the VPN server by the VPN software installed in client's PC. The strength of VPN lie in the fact that once the environment is established, all packets that are sent out from the client's PC are encrypted, regardless of the type of application they use. This way, even if ISP or hackers retrieve transferred packets, they will have difficulty of decrypting them in order to extract private information. The only way to decrypt those packets is to obtain the secret key from the VPN server. Nevertheless, if a VPN server gets hacked, controlled by an organization that makes business out of users' private information or make them available to government entity upon request, privacy can be leaked.

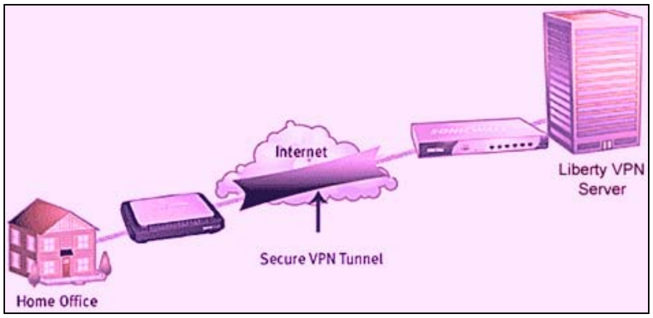


Figure 10. Data flow through VPN server

D. *Anonymity via The Onion Router (TOR)*

Finally, we will discuss The Onion Router (TOR) as an ideal anonymous communication method for social networking environment which employs asymmetric cryptography and use multiple layers of encryption. In this approach, when transmitting data from a source to a destination, a random path consisting of multiple nodes are selected and original data including its destination are encrypted and re-encrypted using public key of the selected nodes. This results in an onion ring wherein each layer is a re-encrypted version an encrypted data by the public key of the node. In the transmission process, each node decrypts a layer of encryption to reveal the next layer, a process similar to an onion-peeling-off process. The final node decrypts the last layer of encryption and sends the original data to its destination without revealing or even knowing its sender. Figure 11 shows a pictorial representation of the working mechanism of TOR between Alice and her TOR clients [7].

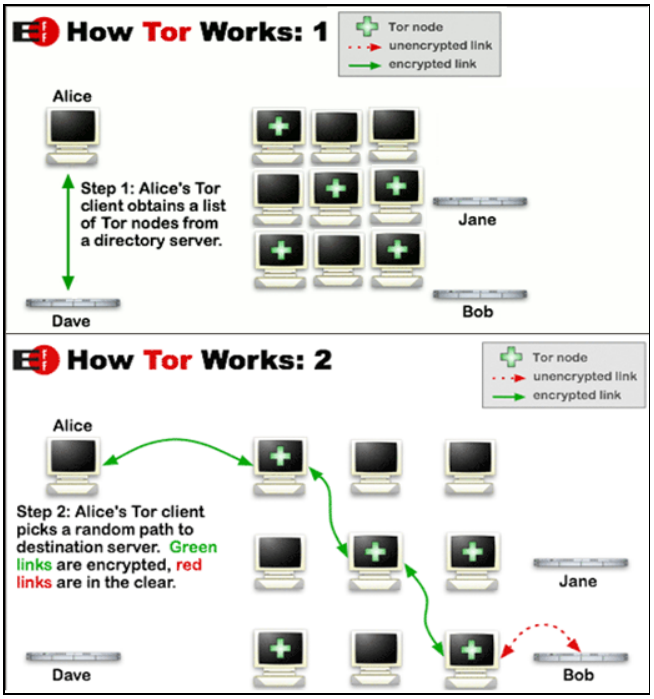

How Tor Works: 1
Tor node
unencrypted link
encrypted link
Alice
Step 1: Alice's Tor client obtains a list of Tor nodes from a directory server.
Jane
Dave
Bob
How Tor Works: 2
Tor node
unencrypted link
encrypted link
Alice
Step 2: Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.
Jane
Dave
Bob

Figure 11. The Onion Router working mechanism [7]

This protocol is more robust than Proxy and VPN because of its multiple encryption layer and protection of the anonymity of the sender at the destination from IP logger tools like IP-spy URL. Although some researcher have pointed out vulnerability of TOR at the exit node as professional attackers could target the node, it is not considered a big issue since TOR makes use of the dynamic IP address to prevent attacker from continuous monitoring of the exit node. Furthermore, by using tools like Vidalia, a cross-platform graphical controller for the TOR, TOR user can easily change the transmission path of data-packets. As shown in Figure 12, just by clicking the "*Use a New Identity*" button on Vidalia interface, user can get a new IP address and setup a new data transmission path. This makes TOR an ideal technique for anonymous communication since in procedures like VPN, users cannot change their IP address frequently due to limited availability of IP address.

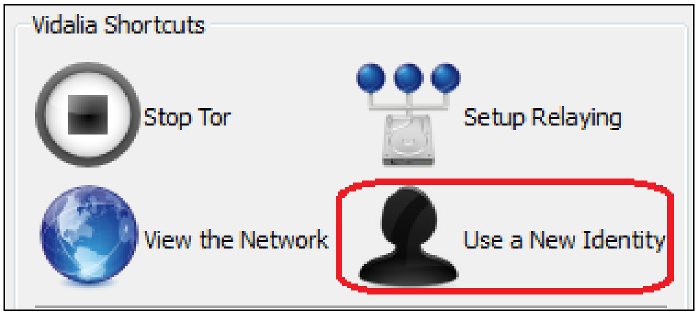
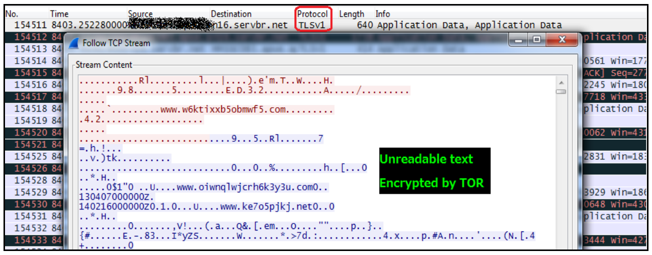


Figure 12. Getting new IP address and changing data-sending path

Another attractive characteristic of the TOR is its free cost. While full-featured VPN services are charged annually, TOR is totally free thus making it more popular in Internet world. The cost free nature of TOR, however, does not compromise its high security level. Granting that attackers capture transmitted packets, they will have difficulty comprehending them since the packets will be in encrypted form as shown in Figure 13. On the contrary, as more users join the TOR network, the higher becomes its anonymity level because of increased routing options. Furthermore, TOR also provides Internet users an opportunity to protect their privacy from the client side instead of waiting for solutions from the ISP or the social network service provider side.



```
No.     Time            Source      Destination      Protocol  Length  Info
 154511 8403.252280000[redacted]n16.servbr.net  TLSv1       640 Application Data, Application Data
```

```
...........Rl.........l...|....).e'm.T..W....H.
.......9.8.......5.........E.D.3.2...........A...../.........
.....
.....`.........www.w6ktixxb5obmwf5.com.........
.4.2...................
.....
...........................9...5..Rl.......7
=.h.!...
..v.)tk.........
.............................0...0..%.........h..[...0
..*.H..
.....0$1"0 ..U....www.oiwnqlwjcrh6k3y3u.com0..
130407000000Z.
140216000000Z0.1.0...U....www.ke7o5pjkj.net0..0
..*.H..
.........0.......,V!...(.a...Q&.[.em...o....""....p..}..
{#......E.-.83...I*yZS.......W.......*.>7d.:.............4.x....p.#A.n....'....(N.[.4
+.......0
```

Figure 13. Packet capture by Wireshark is encrypted by TOR

IV. Results and Conclusion:

This paper showed numerous risks that Internet users in general and social network application users in particular face. It showed how penetration tools like Wireshark, IP-spy URL and others can be used to capture private information of innocent users and victimize them. It proposed anonymous communication as an effective tool to help Internet users protect their private information actively and examined numerous anonymous communication scheme a summary characteristics of which is shown in Table 1. The table can be used as a reference by Internet users in selecting a particular anonymity tool based on the desired level of anonymity and features of the tools. The authors recommend TOR as the most secured anonymous communication scheme and foresee its popularity to further increase in the future. TOR seems to be the king of the anonymous communication scheme since activity of its users are really difficult to be traced even by TOR developers themselves because of its complex internal working mechanism. Nonetheless, attackers are oftentimes one step ahead, hence it is necessary to extend TOR development to a higher level of anonymous communication so as it could cope up with the evolution of attack technology. Furthermore, educating common Internet and social network users are also very important since no amount of anonymity could help when a user starts releasing private information in response to phishing schemes.

TABLE 1. Anonymous Tools Comparisons Table

Testing tool		**Private Browsing Function**	**Proxy**	**VPN**	**TOR**
IP spy URL		fail	pass	pass	pass
Wire shark	capture	fail	fail	fail	fail
	decrypt	fail	fail	pass	pass
Trace-back		fail	fail	fail	pass
Dynamic IP and Data Path changing		Do not support	Do not support	Limited	Support
Cost		free	flexible	flexible	free
Anonymous Level		Low →			High

References

[1] Chris Drake, *FireHost Detects Surge in SQL Injection for Q3 2013 and Cross-Site Scripting is Rising*. Retrieved 22 October 2013. Available: http://www.firehost.com/company/newsroom/press-releases/firehost-detects-surge-in-sql-injection-for-q3-2013-with-cross-site-scripting-also-rising/

[2] Metzger, Miriam J., *Communication Privacy Management in Electronic Commerce*, Journal of Computer-Mediated Communication, volume 12, Issue 2, January 2007, pages 335–361, ISSN 1083-6101. Available: http://dx.doi.org/10.1111/j.1083-6101.2007.00328.x

[3] Angelia, D. Pishva, "Online Advertising and its Security and Privacy Concerns", The 15th International Conference on Advanced Communication Technology (ICACT 2013), Vol. 1, pp. 372-377 (January 2013).

[4] "Threat Actions", *The 2013 Data Breach Investigations Report*, Verizon Enterprise, page 25, Retrieved 2013. Available: http://www.verizonenterprise.com/DBIR/2013

[5] *Facebook Reports Second Quarter 2013 Results*. Facebook. Retrieved 24 July 2013.

[6] M.E. J. Newman, "A measure of betweenness centrality based on random walks", *Social Networks*, Volume 27, Issue 1, January 2005, Pages 39-54, ISSN 0378-8733. Available: http://dx.doi.org/10.1016/j.socnet.2004.11.009

[7] "The solution: a distributed, anonymous network", Tor: Overview. TOR project. Available: https://www.torproject.org/about/overview.html.en#thesolution