A Step towards a Solution to Information Privacy Problem on Online Social Networks

Sirapat Boonkrong

Abstract— **Online social networks, such as Facebook and Twitter, have gained popularity in recent years. With that popularity, come security problems, especially problems with information privacy. This paper provides an overview of information privacy issues for online social networks. One way to solve this problem is to use cryptography. However, cryptography on online social networks has not been studied exclusively. Most works have been done on access control. The main issue with cryptography is the number of keys needed to encrypt and decrypt the information. The most obvious number of keys would be to use one key for every user in our group of friends. This is not needed or entirely true as we show here. This paper, therefore, gives an attempt to show that the number of keys needed to achieve secure sharing among friends can in fact be much smaller than the number of friends. The number of keys can actually be reduced by approximately 500% on average, using the method presented here. We also provide proofs of correctness and security to confirm our claim.**

Index Terms— **Cryptography, Key, Security, Social Networks**

I. Introduction

NOWADAYS, online social networks such as Facebook and Twitter have gained a lot of popularity. They have become an essential tool for communicating with family and friends. The number of active users has increased more and more in the past years, with Facebook having over 1 billion users [1]. When the network grows, there are always concerns over security, whose problems have been stated in [2, 3]. Having said that, to the best of our knowledge, there has not been a paper discussing how cryptography can be used to improve security on online social networks. Most of the works that we have come across appear to focus on access controls [4, 5, 6, 7] or collaborative watchdog [8]. That is, they apply similar mechanisms that can restrict access to contents being shared online. By restricting access, we mean that only friends will have the permission to see the contents.

However, as we have shown in [9] that the existing mechanisms only restrict access on the Web interface. That is, even though the restrictions have been set, users without permission can easily capture messages and read them. Therefore, we say that information privacy is still an issue of concern. One way to ease the privacy problem is to use cryptography. By applying cryptography, messages can be encrypted and only be read by the people, who are authorised to do so.

Cryptography is not without its problems, though. One of the problems that can be foreseen when applying to online social networks would be the number of keys needed to be held by each user. This paper provides a way to look at online social networks and work out the number of keys needed. We show that the number of keys need not be the same as the number of friends we have. Rather, it could be smaller than that by the way the social networks are looked at. Proofs of correctness/security by the GNY logic [10] are also summarised here. It has to be stressed here that we do not attempt to design a new algorithm for key establishment since there are already many [11, 12]. The purpose of our research for the paper is to show and prove that the number of keys does not have to be as many as the number of friends we have.

The structure of this paper is as follows. Section II contains an overview of the work related to this paper. Section III gives an overview of how we chose to look at our network of friends. Section IV shows the number of keys needed for a group of friends using a naïve method, with a proof. Section V presents the actual number of keys needed for a group of friends together with proofs. Section VI concludes our findings.

II. Related Work

A. Social Graph

Many sociologists and computer scientists now look at a social network as a graph [13, 14, 15]. That is, a social network contains users as vertices and relationships between them as edges. This can be put in mathematical term as $G = (V, E)$; where G is a graph or a social network, V is the vertices or users in the graph and E is the edges or relationships connecting the vertices.

Due to the growth of online social networks, many have studied the structure and properties of those social graphs, with the work of Ugander et al. [14] being the most up to date and probably the most complete. Ugander at al. [14] studied the

Manuscript submitted November 9, 2012. This work was supported by the Faculty of Information Technology, King Mongkut's University of Technology North Bangkok, Thailand.

Sirapat Boonkrong is with the Faculty of Information Technology, King Mongkut's University of Technology North Bangkok, Bangkok, Thailand. (Phone: +66-81-2555073; email: sirapatb@kmutnb.ac.th)

DOI: 10.5176/2251-3043_2.4.221

structure of the social graph of active Facebook users, which the authors claimed that it is "the largest social network ever analysed." Their study showed that the average Facebook users had around 190 friends, with the median friend count of 99. The authors also found that the average distance between any pairs of users (not necessarily friends) was 4.6, which confirmed the "six degrees of separation" theory. Furthermore, within a graph of friends, [14] discovered that, on average, 14% of individuals formed a connected subgraph. This means that those users are friends among themselves, too. The notion of a connected subgraph or friends within a graph of friends had previously been introduced in [16]. It was known as a *clique*.

The idea of cliques or connected subgraphs would be an important component in our attempt in reducing the number of keys needed for each user within a group of one-hop friends.

In graph theory, there are many types of graphs. However, only two types are of our interests here. They are undirected graph and directed graph. Let us give the definitions of the two types of graphs here.

An undirected graph is a graph in which edges have no orientation. That is, the edge *(a, b)* is identical to the edge *(b, a)*. Figure 1 is a simple example of an undirected graph.

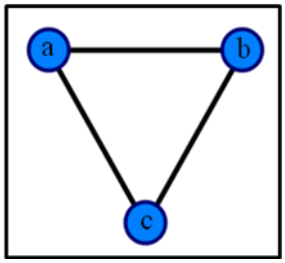

Fig. 1. An undirected graph. The graph shows that the edges have no orientation. That is, the edge (a, b) is identical to the edge (b, a).

A directed graph, to put it simply, is the opposite of an undirected graph, i.e., it is a graph in which edges have orientation. That is, the edge *(a, b)* is not the same as the edge *(b, a)*. Figure 2 shows a simple example of a directed graph.

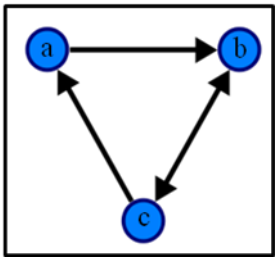

Fig. 2. A directed graph. The graph shows that the edges have orientation. That is, the edge *(a, b)* is not the same as the edge *(b, a)*.

These two types of graphs would also be an important ingredient to our step towards better security for the information on online social networks.

B. Gong Needham Yahalom or GNY Logic

The GNY logic is a formal tool that allows us to analyse cryptographic protocol step by step according to the rules provided in [10]. A protocol, in this context, consists of the exchange of some network messages between two or more principals. A protocol determines what and when messages should be sent, and by which particular principal. Each protocol run is referred to as a *session*.

When analysing a protocol, we begin with a set of initial assumptions. The appropriate rules (*Being-told*, *Possession*, *Freshness*, *Recognisability*, *Message interpretation* and *Jurisdiction rules*, usually in this order) are then applied to each of the received messages. Once the analysis is finished, the protocol should end up with the expected outcomes. If in any case the analysis does not terminate, or the protocol does not achieve the expected conclusions, the feature of the GNY protocol is that it allows the user to see at which step the analysis is stuck or potentially can be attacked. In other words, the analysis allows us to realise which essential components are missing from which message, or what attacks are possible at what stage of the protocol.

We refer the readers to [10] for the explanations of notations and rules.

III. Network of Friends

In order to achieve our goal in deducing the actual number of keys needed to have a more secure sharing between friends, we take the concept of social graph or a graph as a way to look at the network of friends.

Let us take an opportunity here to say a little bit more about the work of this paper. This paper, as mentioned, attempts to find a number of keys needed to be held by a person so that he or she can share messages with his friends and can read posts from his or her friends. Therefore, the easiest way to understand this is the look at one user at a time. We will try to establish a number of keys needed to be held by that person so that secure sharing with his or her friends is possible. Figure 3 shows a typical network of one-hop friends of user *A*.

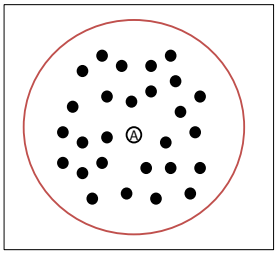

Fig. 3. A typical network of one-hop friends of user *A*. This is how a group of friends on online social network should be looked at. We can think of this network as a graph, with each node representing a person. In the Figure, all the black nodes are one-hop friends of user *A*.

By looking at a group of friends as a graph, it gives us a clearer view towards to solution of finding out the number of keys needed by user *A*. By studying extensively, [14] suggested that it is possible that among the *n* friends of user *A*, some of them are also friends with one another. In other words, within the network of friends, a *connected subgraph* or *subgraphs* can be found. Figure 4 shows a connected subgraph within a group of friends, i.e., the nodes in the dotted

perimeter.

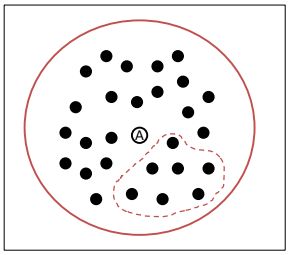

Fig. 4. A connected subgraph within a group of friends. The black nodes within the dotted perimeter are friends among themselves. This means that these nodes all know one another. In terms of graph, each node would have an edge connected to every other node in the perimeter.

Here, it seems appropriate to give a couple of definitions. In the dotted perimeter, each node, as mentioned, would have an edge connected to every other node. This is known as a connected subgraph, which would be known as a *clique* from now. Clique was first introduced in [16].

Definition 1. A *clique* is "a set of more than two people … if they are all mutual friends of one another." [16]

From Definition 1, the nodes within the dotted perimeter in Figure 2 form a clique. This would leave the other nodes (ones that are not in a clique). We think it would be appropriate to call them *isolated nodes*, which is defined below.

Definition 2. An *isolated node* is a node or a user with no mutual friends, or a node or a user that is not part of any clique.

All the studies of social graph have indicated that social networks are thought of as an undirected graph. That is, the edges represent a reciprocal relationship between nodes. However, for the purpose of using cryptography to secure message transmission, social networks cannot be looked at as an undirected graph. In our opinion, it is best to look at them as a *directed* graph. This is because when user *A* shares with his one-hop friends, one key is used for encryption (and decryption). One the other hand, when *B* (a friend of *A*'s) shares, he or she needs another key for encryption (and decryption), because *B*'s friends may not be the same as *A*'s. Hence, we claim here that when considering cryptography, it would be best to think of a social network as a directed graph, rather than an undirected one as usual.

From what we have explained, a group of friends can be thought of as a graph. It is possible, from the study in [14], for a graph to have at least one clique. This would leave the remaining nodes as isolated nodes. We claim that this is one way to look at online social networks, and is also a way towards our goal.

IV. Number of Keys in a Naïve Method

When attempting to find the number of keys needed to be help by a user, referring to Figure 3 and Figure 4, the simplest way is as follows. User *A* must possess a key for encrypting everything he shares with his friends. Moreover, the user *A* must also hold a different key for every user he is friends with, since for cryptography the graph is directed. That is, the number of keys held by user *A* is 1 plus the number of friends that user *A* has, or the number of keys is the same as the number of people in that particular group of friends.

Let *n* be the number of all the people in the group, including user A. We claim that the number of keys needed by the user is:

$$n = 1 + (n - 1) \quad \text{for } n > 1 \tag{1}$$

Proof. We say that Equation 1 is only true for when $n > 1$, because when $n = 1$ there is only one person in the group. No communications would be needed, so the number of keys would be zero.

We begin our simple proof by induction with $n = 2$. Here, it is important to keep in mind that we are trying to find the number of keys for one user, so we look at one user as a "centred" user, user *A* in this case.

Let $n = 2$. When $n = 2$, a user needs one key to share posts and one other key to read posts from the other user.

$$(2) = 1 + ((2) - 1)$$
$$2 = 2$$

Let $n = k$. When $n = k$, a user needs one key to share posts and *k-1* other keys to read posts from others.

$$(k) = 1 + ((k) - 1)$$
$$k = k$$

Let $n = k+1$. When $n = k+1$, a user needs one key to share posts and k other keys to read posts from others.

$$(k+1) = 1 + ((k+1) - 1)$$
$$k+1 = k+1$$

□

It is not difficult to see that using a naïve method a user needs to hold *n* keys, which is equal to the number of people in the group of one-hop friends of that user, including the user him/herself. The next section will try to reduce the number of keys by applying the idea of cliques and isolated nodes to our approach.

V. Number of Keys in a "Better" Method

It has been established and shown in Section II that within a group of nodes, it is possible to have one or more connected subgraphs or cliques, and the non-clique nodes are said to be isolated. It is the ideas of cliques and isolated nodes the number of keys needed to be held by any individuals can be lower than *n*, where *n* is the number of people in a particular group. By using these ideas, it can be seen that a group of nodes can be divided into two parts: cliques and non-cliques or isolated nodes. We take a look at each part in turn.

A. Part I: Cliques

By definition, a clique is "a set of more than two people … if they are all mutual friends of one another." To put this simply, everyone knows everyone in a clique, or everybody is friends with everybody in a clique. This implies that everyone *trusts* one another. Since all nodes in the clique trust each other, we claim that it is possible to achieve secure sharing within the clique using just one key. We backup this claim by carrying out the proof of correctness/security using the GNY logic.

Proof. Assume that all nodes in a clique have established a key, *K*, using such secure group key establishment protocol as

[11]. Also assume that a symmetric encryption algorithm used is secure.

For the simplicity of the proof, we say that node *A* shares a post with other members in the clique. Let us also call all other members in the clique *m*. The purpose of the proof is to show that A can share with other nodes in the clique securely.

$$A \rightarrow m: m \triangleleft *\{*Msg, *N_a, *A\}_K$$

where *Msg* is a message *A* shares with the rest of the clique;
N_a is a nonce (number used once) generated by *A*;
A is the identity of the node *A*; and
$\{x\}_K$ is the symmetric encryption of message *x* using the key *K*.

Analysis:

In carrying out the GNY analysis, we apply postulates T1, T3, P1, F1, R1 and J1 in this order to obtain $m \mid\equiv Msg, N_a, A$. We refer the readers to our work in [17] for the detailed proof.

From the proof, the GNY logic terminates at the end of the final postulate, J1. We claim that this sharing is secure. That is, at the end, the following outcomes are achieved. *m* or all other nodes in the clique believe that *A* is the one sharing a message. They also believe that the message has been encrypted and transmitted by *A*, using the key *K* known only by the nodes in the clique. (When another node within the clique shares a post, the same proof can be used with the same outcomes.)

From the proof above, we claim that using only one key *K*, all nodes in the clique can achieve secure sharing among themselves. □

B. Part II: Isolated Nodes

The second part is for the non-clique nodes, which are known as isolated nodes in this paper. By the definition given in Section III, these are the nodes that are not in any clique. It is, therefore, easy to see that for a user to be able to see a post shared by each isolated node, one key is needed. To put it another way, an isolated node needs one key to encrypt anything he or she wants to share with the individuals he or she is friends with.

From what has been stated above, we say that for a user *A*, the number of keys needed in order to see posts shared by his or her isolated friends is equal to the number of isolated friends. Moreover, the user *A* would also want to share, which means that he or she needs another key to encrypt those messages. Therefore, we get: Let *n* be the number of all isolated nodes plus user *A*.

$$\textit{The number of keys} = 1 + (n - 1) \quad \text{for } n > 1 \qquad (2)$$

It can easily be seen that the Equation 2 is the same as the one in the naïve method. Therefore, the proof showing that the number of key is true is exactly the same, too. We refer readers to Section III for the proof by induction for this equation.

It is now left to us to show that when an isolated user shares something, it is sufficient and secure enough to use just one key. Again, we prove this by using the GNY logic. However, before carrying out the proof and analysis, a couple of assumptions need to be made.

Firstly, it is assumed that an isolated node and the user *A* have established a key *K* using such secure key establishment method as [12]. Secondly, it is assumed that a symmetric encryption algorithm used when sharing is secure.

Proof. Let us call an isolated node *B* and call a user *A*. Let us also say that the isolated node *A* shares something with his or her friends, but since the node is isolated (in this particular group), only user *B* can see it in this group.

$$B \rightarrow A: A \triangleleft *\{*Msg, *N_b, *B\}_K$$

where *Msg* is a message *A* shares with the rest of the clique;
N_b is a nonce (number used once) generated by *B*;
B is the identity of the node *A*; and
$\{x\}_K$ is the symmetric encryption of message *x* using the key *K*.

Analysis:

In carrying out the GNY analysis, we apply postulates T1, T3, P1, F1, R1 and J1 in this order to obtain $A \mid\equiv Msg, N_b, B$. Again, we refer the readers to our work in [17] for the detailed proof.

From the proof, the GNY logic terminates at the end of the final postulate, J1. We claim that this sharing is secure. That is, at the end, the following outcomes are achieved. User *A* believes that the isolated node *B* shares a message. User *A* also believes that the message has been encrypted and transmitted securely by *B*, using the key *K*.

From the proof above, we claim that by using a single key *K*, an isolated node *B* achieves secure sharing with the user *A* within this group. □

C. What is the number of keys in total?

So far, it has been established that when our friends share or post, we need: one key to see each of the isolated nodes' posts and one key to see posts from any node in a clique.

This means that in our group of friends, the number of keys needed to read or see posts from our friends equals the number of isolated nodes plus the number of cliques within the group. Furthermore, we also need one key to encrypt the posts that we share with our friends. Therefore, the number of keys needed to be held is:

$$n_k = n_{iso} + n_c + 1 \qquad (3)$$

where n_k is the total number of keys;
n_{iso} is the number of isolated nodes; and
n_c is the number of cliques in the group.

From Equation 3, it is obvious that the number of keys depends on the number of cliques and the number of isolated nodes. The equation we have established here clearly shows that the number of keys is smaller than the number obtained from the naïve method. The only way that the number of keys will be the same is when there are no cliques in the group, which is very unlikely especially in a large group of friends, as suggested in [14]. In addition, [14] also mentioned that the larger the group the more mutual friendships exist. That is, when a group becomes larger, or a user has more and more friends, it is almost always the case that more than one clique exists. This, from our equation, means that *more cliques equal fewer isolated users which lead to smaller number of keys*. Furthermore, what the equation does not show is that *bigger*

cliques also equal fewer isolated users which also lead to smaller number of keys. We, therefore, claim that we have achieved our primary goal in attempting to reduce the total number of keys needed to be held by each user in online social networks.

D. The Average Number of Keys

A general equation has been formed in the previous section to calculate the number of keys. However, without knowing the exact number of cliques and isolated users, it is still difficult to work out the number of keys needed by an individual. This section will try to go a step further to assist in the calculation of the number of keys. Even though the exact number may not be found, the equations in this section should be less generalised than the previous one.

Equation 3 contains two variables. They are the number of clique n_c and the number of isolated nodes n_{iso}. Let us begin by taking a look at the number of cliques.

By definition, a clique must contain at least three nodes. That means if there are n nodes in our one-hop friend network. The number of cliques could be:

$$1 \le n_c \le \lfloor n/3 \rfloor \quad (4)$$

What this equation tells us is that it is not possible to find an equation that would give an exact number of keys. They best we could do is to form an inequality. That is, it is now possible to form an equation that would give us a range of number of keys for any number of cliques. This is explained in detail below.

Suppose there are n nodes in a typical social network. The following cases could occur.

If the number of cliques is one, it means that the number of nodes in this clique could be between three and n nodes. This suggests that the number of isolated nodes will be:

$$0 \le n_{iso} \le n - 3, \quad (5)$$

where 3 is the minimum number of nodes in a clique.

If the number of cliques is two, and the minimum number of nodes in a clique must be three, the number of nodes that are in any clique could range between six (2 cliques x 3 nodes) and n nodes. This suggests that the number of isolated nodes will be:

$$0 \le n_{iso} \le n - (2*3), \quad (6)$$

where 3 is the minimum number of nodes in a clique, and
2 is the number of cliques.

If the number of cliques is three, and the minimum number of nodes in a clique must be three, the number of nodes that are in any clique could range between nine (3 cliques x 3 nodes) and n nodes. This suggests that the number of isolated nodes will be:

$$0 \le n_{iso} \le n - (3*3), \quad (7)$$

where the first 3 is the minimum number of nodes in a clique,
the second 3 is the number of cliques.

It has been established in Equation 4 that the maximum number of clique in a social network would occur when each of every clique contains three nodes. That is, the maximum number of cliques is $\lfloor n/3 \rfloor$. We get:

If the number of cliques is $\lfloor n/3 \rfloor$, and the minimum number of nodes in a clique must be three, the number of nodes that are in all cliques combined could range between ($\lfloor n/3 \rfloor$ cliques x 3 nodes) and n nodes. This suggests that the number of isolated nodes will be:

$$0 \le n_{iso} \le n - (\lfloor n/3 \rfloor * 3), \quad (8)$$

where 3 is the minimum number of nodes in a clique, and
$\lfloor n/3 \rfloor$ is the maximum number of cliques.

What we have gained from the equations 4 to 8 is another equation that would help us work out the number of keys needed to be held by a user. Having said that, it is not possible to form an equation that would give an exact number since the actual number of cliques and isolated nodes is unknown. Therefore, the best that our equation below could do is to provide a range of possible number of keys held by a user.

Applying the above equations, when the number of nodes $n \ge 3$, the number of keys n_k could be:

$$1 \le n_k \le \lfloor n/3 \rfloor + n - (\lfloor n/3 \rfloor * 3) + 1 \quad (9)$$

After simplification of the Equation 9, we get:

$$1 \le n_k \le n - 2\lfloor n/3 \rfloor + 1 \quad (10)$$

Equation 10 allows us to find the average number of keys to be held by a typical user on an online social network. The results are depicted in Figure 5 below.

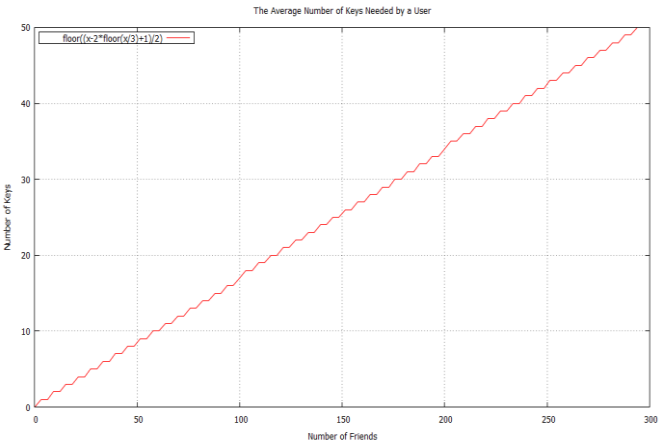

Fig. 5. Average number of keys held by a user with the number of friends ranging from 0 to 300.

It can be seen from Figure 5 that when the number of friends increases, the number of keys needed by a user also increases. In contrast, if we compare our method to the naïve method, the rate of increase is much smaller. In other words, for example in the naïve method shown in Section IV, if the number of friends is 200, the number of keys needed by a person will be 201. However, using our method, the number of keys, as shown in the graph, would only be 35. This is the decrease of more than 500%.

The graph is not a straight line, i.e., a zigzag line, because as the number of friends grows, it is more likely that those friends will join in a clique. This makes the number of keys smaller.

From everything that has been done here, it can be seen in the graph that using our method, the number of keys is much smaller than the naïve method. This, we claim, is a way to ease concerns on using cryptography on online social networks. Hence, it is a step towards better privacy of information on

online social networks.

This section has provided a different way to look at online social networks. The concept of social graphs has been applied in making a step towards securing data. That is, the idea of clique has been used and the idea of isolated nodes has been introduced. We have also scrapped the thoughts that social networks are undirected graph (users' relationship are reciprocal), because when cryptography is deployed different keys are needed to send and receive posts. That means in order to secure online social networks by using cryptography, the social networks must be looked at as a directed graph instead.

Here, it has been shown that by using a naïve method, the number of keys to be held by each user will be equal to the number of users. However, a "better" method has been introduced to reduce the number of keys. We have also proved that even though the number of keys is decreased, the security still remains.

VI. Conclusion

The growth of online social networks has led to security and privacy concerns. Many researchers have tried to improve the security mechanisms. However, their work appears to focus on access control mechanisms rather than cryptography. It has been stated in this paper that the main issue with cryptography when applying to online social networks is the number of keys needed. A naïve method has shown that the number of keys would have to be equal to the number of users in the network.

Our contributions in this research include the way we look at social networks and a method used to reduce the number of keys. First of all, as suggested by many, online social networks can be considered as an undirected graph. In other words, friendship is reciprocal on the network. However, we claim that, in order to apply cryptography, social network must be considered as a directed graph instead. This idea would lead us to bring in the concept of cliques and introduce a definition of isolated nodes, which helped us derive a formula for the number of keys in the end.

By applying the ideas of cliques and isolated nodes, we have been able to derive an equation that helps us in calculating a range and an average of the number of keys needed for an individual user. The graph shows that by using our method, we are able to reduce the number of keys approximately by a *factor of five*, which is a significant amount. Having said that, the actual number of keys still depends on how many cliques there are in a social network of one-hop friends, how many users are in each clique and how many isolated users there are.

On the whole, we have been able to make the number of keys needed much smaller than the naïve method. Even though the number of keys is smaller, the security still remains as shown in the proofs and analyses. In our opinion, this, at least, is a way towards better information privacy on online social networks.

References

[1] Facebook. "Facebook Statistics". (2012) [online] Available: http://www.facebook.com/press/info.php?statistics, 2012.

[2] Robert Gibson, "Who's Really in Your Top 8: Network Security in the Age of Social Networking", *SIGUCCS'07*, October 2007.

[3] E. Athanasopoulos, A. Makridakis, S. Antonatos, D. Antoniades, S. Ioannidis, K.G. Anagnostakis and E.P. Markatos, "Antisocial Networks: Turning a Social Network into a Botnet", *ISC 2008*, pp. 146 – 160, 2008.

[4] Barbara Carminati, Elena Ferrari and Andrea Perego, "Rule-Based Access Control for Social Networks", *OTM Workshops 2006*, pp. 1734 – 1744, 2006.

[5] Amin Tootoonchian, Kiran K Gollu, Stefan Saroiu, Yasha Ganjali and Alec Wolman, "Lockr: Social Access Control for Web 2.0", *WOSN'08*, August 2008.

[6] Barbara Carminati and Elena Ferrari, "Privacy-Aware Collaborative Access Control in Web-Based Social Networks", *DAS 2008*, pp. 81 – 96, 2008.

[7] Philip W.L. Fong, Mohd Anwar and Zhen Zhao, "A privacy Preservation Model for Facebook-Style Social Network Systems", *ESORICS 2009*, pp. 303 – 320, 2009.

[8] Neel Sundaresan, "Online Trust and Reputation Systems", *EC'07*, June 2007.

[9] Sirapat Boonkrong, "The Quest for Security on Online Social Networks", *National Conference on Computer Information Technologies 2011*, January 2011.

[10] Li Gong, Roger Needham und Raphael Yahalom, "Reasoning about Belief in Cryptographic Protocols", *In Proceedings 1990 IEEE Symposium on Research in Security and Privacy*, Seiten 234–248, IEEE Computer Society Press, 1990.

[11] Michael Steiner, Gene Tsudik, and Michael Waidner, "CLIQUES: A new approach to group key agreement", *Research Report RZ 2984 (# 93030)*, IBM Research, December 22, 1997.

[12] Whitfield Diffe and Martin E. Hellman, "New directions in cryptography", *IEEE Transactions on Information Theory*, IT-22(6):644 - 654, 1976.

[13] Alan Mislove, Peter Druschel, Massimiliano Marcon, Bobby Bhattacharjee and Krishna P Gummadi, "Measurement and Analysis of Online Social Networks", *IMC'07*, October 2007.

[14] J. Ugander, B. Karrer, L. Backstrom and C. Marlow, "The Anatomy of the Facebook Social Graph", *arXiv:111.4503v1 [cs.SI]*, November 2011.

[15] K. P. N. Puttaswamy, "StarClique: Guaranteeing user privacy in social networks against intersection attacks", *Proceedings of the 5th International Conference on Emerging Network Experiments and Technologies*, pp. 157 – 168, 2009.

[16] R. D. Luce and A. D. Perry, "A Method of Matrix Analysis of Group Structure", *Psycometrika*, Volume 14, Issue 2, pp. 95 – 116, 1949.

[17] Sirapat Boonkrong, "The Number of Keys Needed for Secure Sharing on Online Social Networks", *In Proceedings of the 3rd Annual International Conference on Infocomm Technologies in Competitive Strategies (ICT 2012)*, Bali, Indonesia, 17 September 2012.

Sirapat Boonkrong is an assistant professor and an associate dean of academic and research affairs at the Faculty of Information Technology, King Mongkut's University of Technology North Bangkok (KMUTNB), Thailand. He received his B.Sc. and Ph.D. in Computer Science from the Department of Computer Science at the University of Bath, UK. His main area of research is information and network security.

Previously, Sirapat worked as a researcher at National Electronics and Computer Technology Center (NECTEC) in Thailand. He also has experience in industry as a project manager at an IBM-partnered company. He is currently a full-time lecturer at the Faculty of Information Technology, KMUTNB and is also supervising several Ph.D. students all of whom are in the field of information and network security. He has many publications to his name, the latest of which is actually a part of this current paper, which was awarded the Best Research Paper at the ICT2012 conference in Bali, Indonesia.