New Directions in Social Authentication

Sakshi Jain
sjain2@linkedin.com

Neil Zhenqiang Gong
neilz.gong@berkeley.edu

Sreya Basuroy
basuroy@princeton.edu

Juan Lang
juanlang@google.com

Dawn Song
dawnsong@cs.berkeley.edu

Prateek Mittal
pmittal@princeton.edu

***Abstract*—Web services are increasingly adopting auxiliary authentication mechanisms to supplement the security provided by conventional password verification. In the domain of social network based web-services, Facebook has pioneered the use of *social authentication* as an auxiliary authentication mechanism. If Facebook detects a user login under suspicious circumstances, then users are asked to verify information about their friends (in addition to verifying their passwords). However, recent work has shown that Facebook's social authentication is insecure.**

In this work-in-progress, we propose to rethink the design of social authentication. Our key insight is that online social network (OSN) operators are privy to large amounts of private data generated by users, including information about users' online interactions. Based on this insight, we architect a system for social authentication that asks users to verify information about their social contacts and their interactions. Our system leverages information protected by privacy policies of OSNs to resist attacks, such as questions based on private user interactions including exchanging messages and poking social contacts.

We implemented our system prototype as a Facebook application, and performed a preliminary user study to evaluate feasibility of the approach. Our initial experiments have been encouraging; we find that users have high rates of recall for information generated in the context of OSN interactions. Overall, our work provides a promising new direction for the secure and usable deployment of social authentication.

I. Introduction

Web services today such as Facebook rely on user provided passwords for authentication. However, a critical security issue in this paradigm is the compromise of passwords [1]. For example, passwords could be compromised because of password database leakage, phishing attacks, dictionary attacks, or password reuses across multiple websites. To supplement the security provided by conventional passwords, websites are increasingly deploying *auxiliary authentication* mechanisms. Auxiliary authentication aims to prevent attackers from taking over user accounts despite having access to their correct passwords.

In the domain of social network based web services, Facebook has pioneered the use of *social authentication* as an auxiliary authentication mechanism. Facebook monitors user accounts for suspicious activity. For instance, if a user logs into Facebook from very distant locations within a very short span of time, then in addition to requiring the user password, Facebook verifies the user by presenting a friend photo and challenging the user to name the friend [2]. Indeed, Facebook's approach has been inspired by similar proposals from the academic community [3]. Interestingly, most deployed and proposed systems have primarily focused on the paradigm of users identifying their friends in depicted photos. A critical vulnerability in this paradigm is the use of fast improving face recognition algorithms. In fact, recent works have demonstrated the successful attacks on photo-based social authentication through theoretical modeling as well as empirical evaluation [4], [5]. *Thus, an open question facing our community is whether social authentication in the current form can provide a strong foundation for supplementing the security of password based authentication.*

Our work: We propose to rethink the design of social authentication based on the insight that online social network (OSN) operators are privy to large amounts of private data generated by users. We believe that the space of social knowledge is much larger than photographs of friends. For instance, users in online social networks are associated with rich *node attributes* such as users' schools, employments, faces, and locations. Moreover, users interact with each other in online social networks. Such interactions include poking friends and exchanging private messages with friends. In this work-in-progress, we aim to study how to leverage the rich space of social knowledge to design mechanisms for social authentication that are both secure and usable. Towards this end, we introduce a general architecture and a system for social authentication that is is able to incorporate the social knowledge available to OSN operators. Our system challenges users to verify information that is dynamically generated in the context of OSN usage, such as information about users' social contacts and their interactions. Note that our approach does not rely on users to preselect static "security questions" and can thus be leveraged on demand.

We propose to group the challenges that can be generated using social knowledge into three categories: *node*, *pseudo-edge*, and *edge* questions. They are constructed from node attributes specific to a single user, common node attributes of linked users (friends), and attributes of user interactions, respectively. Under this categorization of social knowledge,

USEC '15, 8 February 2015, San Diego, CA, USA
Copyright 2015 Internet Society, ISBN 1-891562-40-1
http://dx.doi.org/10.14722/usec.2015.23002

Facebook's photo-based authentication mechanism is an example of a node question since faces are users' node attributes. Moreover, questions based on private user interactions such as exchanging private messages are examples of edge questions. To resist attacks against social authentication, our approach relies on privacy policies applicable on user data that are enforced by OSN operators.

One of the key challenges in generalizing the concept of social authentication is usability, *i.e.*, are users able to recall information that is organically and dynamically generated with their OSN usage? To study this question, we implemented a preliminary prototype of our architecture as a Facebook application. We performed a user study by recruiting 90 participants from Amazon Mechanical Turk to test our prototype. Our initial results have been encouraging; our study provides preliminary support to the idea that users have a non-trivial ability to recall information pertaining to their interactions on online social networks.

As a part of future work, we plan to (a) conduct a larger-scale user study to further our understanding of the usability of social authentication, (b) develop theoretical models to quantify the security of the approach, and (c) engage with OSN operators to impact system design. Overall, our work opens up promising new directions for research in secure and usable social authentication mechanisms.

II. Motivation

Facebook designed and implemented an auxiliary authentication mechanism called *social authentication* [2] for its users using photos of friends posted on the social network. When Facebook detects suspicious activity on a user's account, e.g., if a user logged into Facebook from very distant locations within a small span of time, in addition to the user's password, it presents photo challenges to the user. In these photo challenges, Facebook shows 3 tagged photos of a friend with 6 options and the user has to select the correct friend name that corresponds to the tags in the photos shown. If the user accurately answers at least 5 out of 7 instances of photo challenges, he or she is allowed access to the website.

However, recent works [4], [5] have discussed various security issues with photo-based social authentication. For instance, Kim et al. [4] pointed out that photo-based social authentication is not secure against the user's friends who could also recognize the person in the photo. Polakis [5] designed an automated attack which exploits face recognition techniques, to demonstrate the feasibility of carrying out large-scale real-world attack against photo-based social authentication. As a defense, Polakis et al. [6] recently proposed to transform faces and show distorted faces in the photos. They showed that these distorted friend faces, while easy for a user to recognize, are robust against face recognition attacks and image comparison attacks where attackers collect publicly available photos to compare and identify the individuals in displayed photos. In conclusion, photo-based social authentication constantly finds itself in arms race with face recognition algorithms, which are fast improving. In this work, we ask the question, can we leverage information from a user's social network other than the photos?

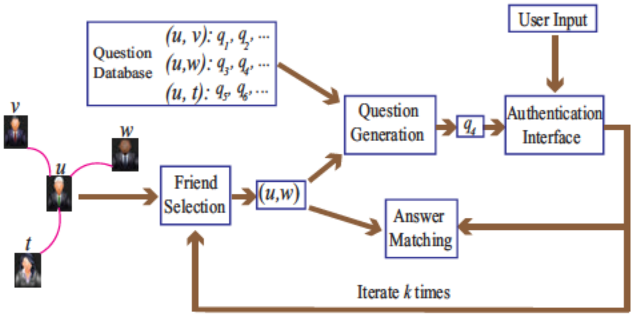


Fig. 1: Proposed architecture for social authentication systems

Indeed, the space of social knowledge is much larger than just photos. For instance, users in OSNs usually create profiles which include diverse information types such as education, age, employment, and location. Moreover, OSNs offer various modes of interaction amongst users, for example, users could poke their friends and exchange private messages on Facebook, Twitter allows a user to follow another user, Google+ allows its users to create circles and categorize their connections, and LinkedIn allows users to write recommendations and endorse their social contacts for some skills. Can these social data be leveraged to design social authentication? How difficult or easy it is to generate challenges based on these data? How secure and usable would such systems be? Would it be more secure than photo-based social authentication? Would it have implications on users' privacy? Can we categorize the plethora of information available in social networks in some way in order to perform a security analysis of them?

We believe that photo-based social authentication is one aspect of knowledge based social authentication mechanisms and there lies a large space of social knowledge yet unexplored. In this work-in-progress work, we lay the basic framework of exploring the use of other social knowledge and take the first step towards answering some of the questions asked.

III. Architecture of Social Authentications

We denote an OSN as a graph $G = (V, E)$, where each node corresponds to a user registered on that OSN and an edge corresponds to two users being *friends* on the social network. OSNs store various types of personal information about users themselves as well as their activities on the website. We divide these information types into two categories, i.e., *node attributes* and *edge attributes*. Node attributes correspond to details specific to each user independent of their interaction with others. Some common node attributes across social networks include user's name, photo, education, and location. Edge attributes on the other hand include data corresponding to interactions among various users. The schema of this information type largely depends on the various platforms provided by the social network for user engagement. Some examples of such data include messages exchanged between users, pokes by friends, and posts written on a friend's wall.

Architecture Overview: A social authentication system comprises of challenges or questions posed to the user. We propose a schematic architecture for a social authentication system as follows. The system iterates over k trials to authenticate a user u. In each trial, a question is selected from the question database and is displayed to the user via an *authentication interface*. All questions follow a common schema, where the user is provided information about an attribute, node or edge, and is asked to identify the associated friend. The user u inputs his/her answer (i.e., name of a friend) to the question; and the *answer matching* module checks if the user provided answer can be matched to the correct friend.

Question Database: The questions in the database are generated using the node and edge attributes available for the specific social network. We divide the set of questions into three main categories.

Node questions: Questions where the user is provided data about some node attribute of a friend and is asked to recognize the corresponding friend. For instance, "Name your friend in the displayed photos" or "Name a friend who is currently studying at UC Berkeley".

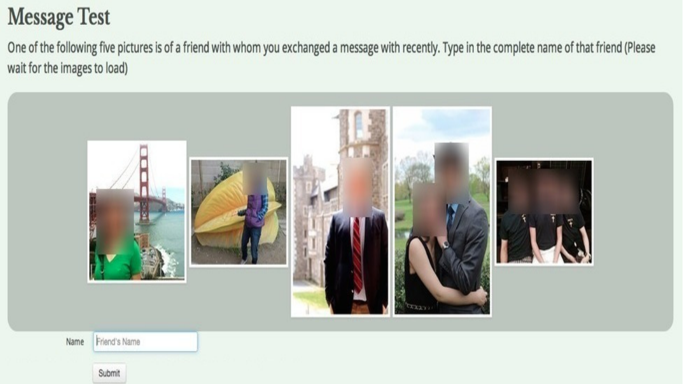
Pseudo-edge questions: Questions where the user is provided information about some node attribute which is common between the user and a friend. The user is then asked to recognize the friend. For instance, "Who went to the same school with you?" is a pseudo-edge question because it involves the school (node attribute) common to the user and his/her friend.

Edge questions: Questions where the user is provided information about some interaction with a friend and the user is asked to recognize the friend. For instance, "Name a friend you recently exchanged a message with" is an edge question.

Facebook's face-recognition challenges fall under node questions category since faces are node attributes.

Authentication Interface & Answer Matching: The authentication interface displays the challenges and receives the user's inputs. There could be multiple ways of obtaining answers from the user, each providing varied usability and security trade-offs. For example, one way is to show n options of friend names as radio buttons and the user chooses the correct one amongst them. Facebook's current photo-based social authentication system receives the answers in this way, where $n = 6$. Another way is to ask the user to type in the name of the correct friend by providing just the photos of both correct and incorrect friends as options. The user in this case needs to recognize the correct friend from the photos and write the selected friend's name in the textbox. The name entered by the user in this case can be matched to the correct one using fuzzy matching, to account for spelling mistakes for improved usability. One can also imagine providing a dropdown menu of friends' names to select from, with or without providing any photo options. Each of the above techniques have their pros and cons when evaluated against security and usability metrics. We suspect that the first method is very usable since it allows the user to click on an option, however, the security of such method is lower bounded by $\frac{1}{n}$. Although we compromise on usability for the second method, its security is strictly better than providing radio buttons, since the attacker would have to recognize the correct friend and type in the name. Quantitatively evaluating the security is however quite tricky in this case.

Model Selection and Evaluation: Given the proposed general model for a social authentication system, there are multiple parameters that need analysis. For example, how difficult is it to come up with the question database for a particular social network? Is such a model feasible? Would users remember answers to such questions? How should the answer choices look like? Do any particular category of questions provide better security or usability to users? In order to answer some of these questions and to test the feasibility of such a system, we build a prototype authentication interface for Facebook and perform a user study to perform preliminary analysis of the proposed system. We particularly chose Facebook as our platform since it is the most popular online social network (OSN) with more than 1 billion users worldwide [7]. Also Facebook provides an API to build apps using information from a user's social graph.



Message Test

One of the following five pictures is of a friend with whom you exchanged a message with recently. Type in the complete name of that friend (Please wait for the images to load)

Fig. 2: Example of an edge question from our prototype for Facebook.

In the following two sections, we detail our analysis of the feasibility and usability of the proposed system. We also briefly discuss the security implications of the various types of questions in Section V.

IV. User Study Design

A. Preliminary Study

We designed a user study to understand the usability of our new proposed model, to measure how well users perform when posed with questions about their social network and to help design a more extensive authentication mechanism model. To this effect, we recruited 90 participants to take a survey and performed a quantitative study based on the observations.

1) Methodology: We invited participants via Amazon Mechanical Turk to take a survey about their Facebook account. Any participant above 18 years of age owning a Facebook account was allowed to take the survey. Each participant is directed to a Facebook application URL and asked to login with his Facebook credentials. Once logged in, Facebook takes the participant to our application, called 'Soc-auth'. Soc-auth requests the following permissions to the user before proceeding: $\{$user-groups, user-photos, friends-about-me, friends-education-history, friends-photos, read-mailbox$\}$. Once the participant provides the required permissions, Soc-auth poses the participant with 4 different questions followed by a survey about basic personal information and a feedback form. For each question, client-side Javascript queries Facebook for

TABLE I: Questions used in the Facebook prototype for user study and their corresponding categories

Question schemas	Description	Category
Q_1	Type in the complete name of the person with a square box around his/her face in the following picture	Node
Q_2	Given the following 5 Facebook friends as options, type the complete name of the friend you went to same school with	Pseudo-edge
Q_3	Given the following 5 Facebook friends as options, type the complete name of the friend who poked you on Facebook	Edge
Q_4	Given the following 5 Facebook friends as options, type the complete name of the friend with whom you exchanged a message on Facebook	Edge

appropriate user information and checks the correctness of the answer provided by the user. We chose to implement all the logic at the client side to protect the confidentiality of user information since the above mentioned permissions provide the app access to sensitive data including inbox. To protect the privacy of the user, we only store whether the user answered a question correctly. Each participant was compensated with $5 paid via Amazon Mechanical Turk. We recruited 90 participants in total from Amazon Mechanical Turk over a course of 7 days. These participants had a wide range of ages (18 - 45+). 42% of the participants fell in the (18-24) bracket, 39% in the (25-34) bracket, and the remaining 18 % were above 35. We also saw a wide range of educational background. About 19% had or are pursuing high school degrees, 57% had or are pursuing bachelor degrees, and 24% had or are pursuing advanced degrees.

Our goal of this experiment is to understand the feasibility of a model which uses the user's social network to generate authentication questions. To this effect, we chose 4 different questions to ask each user. Questions were selected based on most popular sources of activity on Facebook and security of the question. We first inspected the Facebook Graph API[1] which is a tool provided by Facebook to represent the nodes and edges of its social graph. By analyzing a node or user, we determined the most common interactions or edges they share with other nodes and designed the questions to ask about these attributes. Furthermore, according to a survey about people's Facebook activity conducted by the Pew Research Center [8], the top 3 most frequent activity are commenting, liking, and exchanging messages. While users may post statuses or comment on friends' posts frequently, this behavior is easily viewable by both known and unknown attackers and does not constitute a secure question. Hence, we ask questions about the next most frequent set of activities that are not public, such as private messages and pokes exchanged.

The questions and their corresponding categories are shown in Table I. Question Q_1 presents a user with a photo from his album and asks the user to type in the name of the tagged person. This is a node question since answering this question correctly would require the user to recognize a friend's face (a node attribute) correctly. Question Q_2 presents a user with profile photo of five of his friends and asks the user to type in the name of the friend with whom he went to the same school. This is a pseudo edge question since the question requires the knowledge about the node attributes (i.e., school) of both the user and the correct friend. Questions Q_3 and Q_4 are edge questions, each of which presents a user with five options and asks the user to type in the correct name. Specifically, Q_3 asks the user to choose the friend who *poked* him recently on Facebook and Q_4 asks who recently exchanged a message with the user on Facebook. Questions Q_3 and Q_4 are asked only when the user has at least one friend who poked/ messaged him in last one year. This design choice is made to ensure that the interaction is recent enough for the user to remember the friend. Figure 2 shows an example of Q_4.

TABLE II: 95% confidence intervals of applicability and reliability of the four question schemas shown in Table I.

	Applicability	Reliability
Q_1	77%±8%	28%±9%
Q_2	51%±10%	54%±10%
Q_3	48%±10%	71%±9%
Q_4	98%±2%	66%±10%

To generate options for each question, we randomly choose one correct option and 4 incorrect options. Note that the user is not just asked to select the correct friend but to type in the name of the friend in a text box, thereby increasing security. To match the answer provided by the user with the correct friend's name displayed on Facebook, we adopt Dameru-Levenstein edit distance for fuzzy matching. The input answer is considered correct if the edit distance is no more than 12%, which roughly means that we tolerate one out of 8 characters to be removed or replaced or added.

2) Findings: In order to capture the feasibility of our model, we evaluate it using two metrics, *applicability* and *reliability*. Notice that some or all the four questions might be inapplicable to some users. For instance, Q_3 is inapplicable to a user who has not been poked by any friend and Q_2 is not applicable to a user who has not mentioned his school on Facebook. To quantify this, we define *applicability* of each question Q_i as the fraction of users to which Q_i was applicable. In order to measure how easy it is for a user to answer the questions, we define *reliability* of each question Q_i as the fraction of users for whom this question was applicable and who correctly answered the question. We use well known Wilson method to compute 95% confidence interval for both applicability and reliability of the four questions.

Table II shows the 95% confidence intervals of applicability and reliability of the four questions obtained from our user study of 90 participants. We find that the variation in the applicability of the questions we chose is quite large. Only about 51% of the participants had a page associated with their school on Facebook. While about 52% had not been poked

[1] https://developers.facebook.com/docs/graph-api/

in last one year, around 98% had exchanged a message with a friend during the time span of a year. The photo question has a 77% of applicability, since the photos selected were chosen from the user's albums, instead of any and all images of the individual. While a friend may have many images on Facebook, not all will have albums.

Similarly large variation is seen in the reliability of our four questions. We find that the users were able to correctly answer the two edge questions more easily than the node question, which fared quite low on reliability ($\sim 28\%$). We believe that this gap is because an interaction with a friend in the form of a message or a poke would make it more likely that the friend is a close friend implying it would be easier for the user to remember his/her name. On the other hand, a user might not be familiar with friends or acquaintances (but friends on Facebook) tagged in some photos,[2] resulting in low reliability of Q_1. Note that from these observations, we cannot firmly deduce that edge questions are more reliable than node or pseudo-edge questions since we have used specific examples for each category of question. It is possible that some instances of node questions perform better than a poorly chosen instance of edge question. However, since there is no universal set of edge, node, and pseudo-node questions, this is difficult to evaluate at this point.

B. Next Steps

Based on the observations from the first study, we are designing a more extensive and larger scale study to quantitatively evaluate the benefits of the proposed model as a part of future work. Since the previous study only asked 1 node, 1 pseudo-edge, and 2 edge questions, the results are limited to the specific question asked within each category. Instead, we plan to design and analyze a broader set of questions per category. Examples of node questions other than face-identification could include asking the user to identify a friend from his hometown, college, employer, or Facebook groups that he is a member of. The pseudo-edge category can be expanded to questions like “Name a friend who attended the same high school or college as you.”, or “Name a friend who is going to a given Facebook event with you.” Similarly, the edge questions can be expanded to more than exchanging pokes and messages. For example, users can be asked to identify a friend who sent them a friend request or tagged them in a photo recently. Each question may have a different memory recall time and applicability based on the user's engagement of Facebook; it would be interesting to examine whether one particular type of questions are more usable.

Furthermore, we want to quantify the usability and security of the existing face-based authentication model used by Facebook and compare with our model. The photo test question in the previous study was similar to the one used by Facebook, except for the number of images of the friend displayed in the question and the answering matching mode. Thus to create a more direct comparison, we plan to design a separate question to simulate the photo-based challenge as shown by Facebook. Finally, we'd like to evaluate the ease of use of various answering methodologies while maintaining their security properties. We plan to compare the radio button option, vanilla text box with no options, and text box with photos of friends without their names shown as options. Moreover, we plan to construct a formal security model to quantify the security of different categories of questions and different answering matching modes, and compare them quantitatively.

V. Discussion

In this section, we briefly discuss the security and privacy implications of the proposed model.

Security: Online social networks often provide users with fine-grained privacy settings. We assume a user u sets his/her node attributes (e.g., users' faces, schools, and employers) to be accessible to at least his/her friends. The incentives for users to do so could be to let their friends know who they are. In fact, Dey et al. [9] showed that 47% of Facebook users leave their such node attributes publicly accessible by default. However, we consider edge attributes (e.g., pokes and private messages exchanged between two users) of an edge (u, f) are set to be accessible only to user u and the linked friend f. Indeed, such edge attributes in Facebook are only accessible to the two involved users.

Under this privacy setting, the set of users who can access the attributes that are core to the three types of questions (i.e., node, pseudo-edge, and edge questions) are different. Specifically, let u be the user and f be the selected friend about whom a question q is being asked. If q is a node question, the node attribute used in q is at least accessible to all the friends of f and f. If on the other hand q is a pseudo-edge question, the common node attribute involved in q is only accessible to the common friends of u and f if they set their node attributes to be only visible to their friends in their privacy settings. Lastly, if q is an edge question, the corresponding edge attribute is accessible only to u and f. The different privacy setting for node and edge attributes is the fundamental reason why the three types of questions manifest different levels of security.

We will take the Sybil attack [10] as an example to further illustrate the security levels. In an Sybil attack, the attacker creates fake accounts on the social network and tries to befriend the victim and its friends to get access to their information. If the authentication challenge is a node question like the Facebook's photo based challenge, the attacker has all the necessary information to solve the challenge once he has connected himself to the victim's friends on the social graph. If the authentication challenge is a pseudo-edge question, the attacker needs to befriend the victim's friends and the victim, which succeeds with a lower probability. Edge questions are robust to this kind of Sybil attack because interactions are private to the victim and the friend involved.

We believe edge questions can be significantly more promising in providing security and worth exploring in the new versions of social authentication services. Theoretical modeling of the three types of questions and performing security experiments on publicly available social graphs is left for future work.

Privacy implications: Social authentication mechanisms might also raise concerns around leakage of private user information. For each of the three types of questions, some information about the node or edge attributes is revealed to be

[2] These tags could be provided by other users.

able to frame the challenge. An example from our prototype is the message question; the attacker without answering the question would know that the user exchanged private messages with one of the friends from the options. Similarly, in the Facebook's photo-based questions, user's friends and their photos are revealed during the challenge. One can argue against the privacy leakage since these challenges are only used when the user has been confirmed via primary authentication interface (passwords). Moreover, we plan to evaluate users' privacy concerns in social authentication via user studies.

VI. Related Work

In this section, we review prior work on social authentication mechanisms, which we divide into two categories: *trustee-based* social authentication and *knowledge-based* social authentication.

In trustee-based social authentication [11], [12], [13], [14], [15], the user or the service provider pre-selects a few friends of the user as trustees, who aid the user in the authentication process. Knowledge-based social authentication [3], [2], [4], [5], [6] utilizes a user's friends' information for authentication, and thus knowledge-based social authentication relies on the user's knowledge about their friends. The friends are not directly involved in knowledge-based social authentication. Knowledge-based social authentication mechanisms are mainly used as auxiliary authentication mechanisms while trustee-based social authentication mechanisms are used as backup authentication service. Our work belongs to knowledge-based social authentication.

Trustee-based social authentication: Brainard et al. [11] proposed to use *somebody you know*, i.e., friends of users, in authentication systems. Originally, Brainard et al. combined trustee-based social authentications with other authenticators (e.g., passwords) as a two-factor authentication mechanism. Later, trustee-based social authentication was adapted to be used as a backup authenticator [13], [14], [12]. For instance, Schechter et al. [12] designed and built a prototype of trustee-based social authentication system which was integrated into Microsoft's Windows Live ID system. Facebook announced its trustee-based social authentication system called Trusted Friends in October 2011 [13], and it was redesigned to be Trusted Contacts [14] in May 2013. Gong and Wang [15] proposed a probabilistic security model to quantify the security of trustee-based social authentication, and their security model can guide the design of more secure trustee-based social authentication.

Knowledge-based social authentication: Yardi et al. [3] were the first to propose a photo-based authentication system called *Lineup*, to test if the user belongs to a group (e.g., interest groups in Facebook) that he/she tries to access. Specifically, when a user tries to access a group, Lineup presents a photo and asks the user to input the names of subjects in the photo assuming that if the user has the permission to access the group, he/she should know the subjects. To determine if the answer given by the user is correct or not, Lineup uses tagged photos to obtain ground-truth answers. Furthermore, Yardi et al. discussed *Denial of Service (DoS)* and *network outlier* attacks. In DoS attacks, an attacker could spam the system with a large number of photos with wrong tags, and thus legitimate users input "incorrect" answers even if they know the subjects. The network outlier attacks represent that an attacker can recognize his/her friends that are in the group and whose tagged photos are presented. Later, Facebook adopted and implemented this photo-based authentication mechanism [2] to verify users when a suspicious user activity is detected.

VII. Conclusion and Future Work

In this work, we propose to revisit the design space of social authentication challenges by exploiting the vast amount of data generated on social networks. Specifically, we present a general architecture for social authentication that incorporates a large space of social knowledge and makes it possible to compare different design strategies under the same framework. We introduce a categorization of the design space of questions that can be generated from a social graph, i.e., *node*, *pseudo-edge*, and *edge* questions.

As a proof-of-concept for our proposed model, we implement a prototype as a Facebook application and perform user study on 90 Amazon Mechanical Turk workers. The results of the study are encouraging and prove the feasibility and usability of such a model. Our work thus opens up promising new directions in knowledge-based social authentication by exploiting a larger design space.

Acknowledgement: This work is supported by the NSF under Grant No. 1409915 and 1409415.

References

[1] D. Balfanz, R. Chow, O. Eisen, M. Jakobsson, S. Kirsch, S. Matsumoto, J. Molina, and P. van Oorschot, "The future of authentication," *IEEE Security & Privacy*, 2012.

[2] Facebook's Knowledge-based Social Authentication., "http://blog.facebook.com/blog.php?post=486790652130."

[3] S. Yardi, N. Feamster, and A. Bruckman, "Photo-based authentication using social networks," in *WOSN*, 2008.

[4] H. Kim, J. Tang, and R. Anderson, "Social authentication: Harder than it looks," in *FC*, 2012.

[5] I. Polakis, M. Lancini, G. Kontaxis, F. Maggi, S. Ioannidis, A. D. Keromytis, and S. Zanero, "All your face are belong to us: Breaking facebook's social authentication," in *ACSAC*, 2012.

[6] I. Polakis, P. Ilia, F. Maggi, M. Lancini, G. Kontaxis, S. Zanero, S. Ioannidis, and A. D. Keromytis, "Faces in the distorting mirror: Revisiting photo-based social authentication," in *CCS*, 2014.

[7] Facebook Company Info, "http://newsroom.fb.com/company-info/."

[8] Keith Hampton and Lauren Sessions Goulet and Cameron Marlow and Lee Rainie, "http://www.pewinternet.org/2012/02/03/part-2-facebook-activity/."

[9] R. Dey, Z. Jelveh, and K. Ross, "Facebook users have become much more private: A large-scale study," in *SESOC*, 2012.

[10] J. R. Douceur, "The Sybil attack," in *IPTPS*, 2002.

[11] J. Brainard, A. Juels, R. L. Rivest, M. Szydlo, and M. Yung, "Fourth-factor authentication: Somebody you know," in *CCS*, 2006.

[12] S. Schechter, S. Egelman, and R. W. Reeder, "It's not what you know, but who you know," in *CHI*, 2009.

[13] Facebook's Trusted Friends, "https://www.facebook.com/notes/facebook-security/national-cybersecurity-awareness-month-updates/10150335022240766."

[14] Facebook's Trusted Contacts, "https://www.facebook.com/notes/facebook-security/introducing-trusted-contacts/10151362774980766."

[15] N. Z. Gong and D. Wang, "On the security of trustee-based social authentications," *IEEE Transactions on Information Forensics and Security (TIFS)*, vol. 9, no. 8, 2014.