RelationGrams: Tie-Strength Visualization for User-Controlled Online Identity Authentication

Tiffany Hyun-Jin Kim, Akira Yamada, Jason Hong, Virgil Gligor, and Adrian Perrig

February 10, 2011

CMU-CyLab-11-014

CyLab
Carnegie Mellon University
Pittsburgh, PA 15213

RelationGrams: Tie-Strength Visualization for User-Controlled Online Identity Authentication

Tiffany Hyun-Jin Kim[§], Akira Yamada[†], Jason Hong[§], Virgil Gligor[§], and Adrian Perrig[§]

[§] Carnegie Mellon University
{hyunjin,jasonh,gligor,perrig}@cmu.edu

[†] KDDI R&D Laboratories Inc.
yamada.akira@kddilabs.jp

ABSTRACT

Users experience a crisis of confidence for online activities in the current Internet. Unfortunately, the *symptom* of this crisis of confidence manifests itself through online attacks, where adversaries con users to extract money or valuable sensitive information. Instead of addressing the symptom, we investigate how to address the underlying *cause*, which is that the absence of humanly verifiable information for online entities prevents user authentication.

As an initial step in this endeavor, we consider the specific problem of how users can securely authenticate online identities (e.g., associate a Facebook ID with its owner). Based on prior social science research demonstrating that the strength of social ties is a useful indicator of trust in many real-world relationships, we explore how tie strength can be visualized using well-defined and measurable parameters. We then apply the visualization in the context of online friend invitations and propose a protocol for secure online identity authentication. We analyze the robustness of the protocol against adversaries who attempt to establish fraudulent online identities, and evaluate the usability in an actual implementation on a popular online social network (i.e., Facebook). We find that a tie-strength visualization is a useful primitive for online identity authentication.

1. Introduction

Many social interactions in the real world are based on various types of trust relations derived from strong social ties[1] [18, 26, 27, 31]. For example, accepting an invitation from a stranger to a social event where personal or professional information may be revealed often relies on a good friend's or family member's knowledge of the inviter and assessment of his or her discretion. Similarly, a stranger's identity is typically taken for granted by most individuals whenever the stranger is introduced by a long-standing friend, family member, or professional colleague.

As social interactions migrate from the physical to the online world, current systems do not provide many cues upon which users can base the identity authentication. For example, consider Facebook: how can a user be certain that a Facebook invitation is really from the claimed individual? As anyone can trivially set up a Facebook page with someone else's photo, Facebook provides almost no help in ensuring correspondence between the online and physical identity [1,2,19], even fooling security-conscious individuals [33]. Furthermore, Irani et al. [23] recently propose reverse social engineering attacks in online social networks, where the attacker sets up fake accounts and lets the victim discover and contact the fake account. The emergence of SocialBot Networks, as suggested by Boshmaf et al. [3], further compounds these problems.

Although at a first glance Public Key Infrastructures (PKI) and Pretty Good Privacy (PGP) appear to enable users to link an online identity to an individual, these approaches have significant shortcomings. Despite the long existence of Certification Authorities (CAs), few users have personal certificates, which are cumbersome to obtain [10, 13]. Moreover, CAs are a single point of failure and have recently suffered from several attacks [12]. Unlike PKIs, PGP is a distributed approach based on the notion of "Web of Trust" enabling identity certification [42]. Besides the shortcomings we discuss in the related work section, PGP chains of trust are often unwieldy and offer limited security.

Personal recommendation systems may appear to address these issues, where a user would digitally sign a statement such as: "I trust that public key K_A really belongs to Alice, and I trust Alice to correctly validate other users." In the context of PGP, users could specify how much they trust others to assist validation of a chain of trust. Unfortunately, this approach suffers from scaling issues in terms of the effort required since users have to explicitly provide recommendations. Furthermore, this approach suffers from the *distrust revelation problem*, defined by Kim et al. [24], where a polite or conflict-averse user does not want to publicly admit distrusting another individual, and thus specifies the untrusted user as trusted. Avoiding the distrust revelation problem is a core challenge we aim to address.

Our goal is to study approaches that enable users to authenticate online entities in a manner that is robust against impersonation. We seek an approach that empowers the innate human ability to form trust by associating *physical world information* to virtual entities. An interesting research challenge then is to study what physical world in-

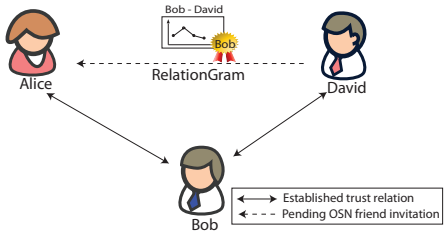

Figure 1: Our approach for online identity authentication. In an OSN friend invitation, Alice confirms David's invitation based on a ***RelationGram*** – a visual evidence of Bob's and David's tie strength.

[1] *Tie strength* is the technical term that refers to the closeness, social proximity, or propinquity of two individuals.

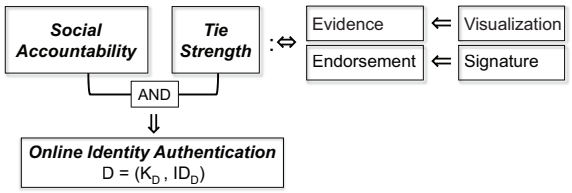

Figure 2: Our proposed online identity authentication model. User A authenticates an online identity of user D given user B's social accountability to A ***and*** the indication of tie strength between B and D, which, by definition, is satisfied given evidence of tie strength (visualization) along with its endorsement (signature).

formation can be reliably captured and communicated to provide relevant information for assisting user decisions, to enable robust authentication of online entities, to avoid disclosure of sensitive private user information, and to enable easy-to use and intuitive operation.

As an initial step in this research direction, we study how to enable users to authenticate Online Social Network (OSN) invitations to ensure that an invitation from an online individual is indeed tied to the correct physical person. Our key idea is to derive tie strength between inviters and their mutual friends to represent real-world physical interactions, and provide it as evidence to empower users to authenticate online identities. More specifically, prior research indicates that in practice, tie strength can be represented using simple proxies such as frequency, reciprocity, and recency of communication, which we believe can be feasibly acquired by smartphones using call logs, emails, OSN comments, etc. Based on the simple proxies, we propose a *RelationGram* – a visualization of tie strength between an inviter and the invitee's friend(s) from which the invitee can easily understand the degree to which her friends know the inviter before she makes her own context-dependent decisions.

We specifically examine OSNs in this paper. However, we believe that our techniques are generalizable to other situations, including:

- Business deals: recruiters can leverage a RelationGram to interview someone whom their friends know and to evaluate the level of accountability.
- Car sharing: a car owner can use a RelationGram to check if his friends have prior relationships with new candidates (and how strong their relationships are).

2. Problem Statement

In this section, we describe the online identity authentication model, and state the desired properties as well as the adversary model that we address in this paper.

2.1 Online Identity Authentication Model

In this paper, we utilize notions such as social accountability, tie strength, and identity authentication as Figure 2 depicts. Ultimately, our goal is to achieve *identity authentication*, i.e., correctly associate an online identity ID_D (along with its public key K_D) to its physical entity D.

Social accountability is a concept where people hold responsibilities for their actions as governed by social norms. For example, friends are socially accountable for their actions with other friends, and so do families and colleagues. In this paper, we utilize social accountability in the following manner: user A holds user B accountable for his actions such that B does not deceive A by creating or certifying bogus online identities. If B signs a bogus identity, the signature provides a non-repudiable statement, which may result in informal sanctions (e.g., loss of respect from family, relatives, friends, and colleagues) and shame (e.g., loss of self-esteem and feeling of guilt) for B. Preliminary evidence shows that social accountability has a much stronger deterrence effect than formal/legal punishment [21]. Furthermore, B has no strong incentives to intentionally harm A, but rather, B's correct authentication of ID_D can boost his friendship with A; when A learns that B correctly authenticated ID_D, A trusts B to a greater extent to carefully validate the identities of others. We stress that this is a considerably limited form of trust.

Tie strength measures the social distance between two individuals, with respect to kinship, interactions, workplace, etc. More specifically, we define tie strength as follows: a strong tie from user D to user B is given through *evidence of close social distance* and *endorsement by B of D*. In particular, the evidence we consider in this paper consists of communication frequency, recency and reciprocity of communication, and length of relationship. In the online world, our evidence is at least as strong as that commonly used in social sciences for measuring strength of ties in the physical world [16] (see Section 3.1). With the existence of at least 1 socially-accountable endorser, our system provides the evidence of social distance through a simple visualization that is endorsed in the form of a digital signature.

2.2 Scenario

Armed with the above concepts, we now describe the steps that Alice takes to authenticate David's online identity as shown in Figures 1 and 2. First, Alice personally knows Bob, and some level of social accountability exists between them. Second, David has sent a friend invitation to Alice and claims that Bob is a mutual friend. Before accepting the invitation, Alice wants to validate that Bob has a strong tie with David. Thanks to the RelationGram, visualizing tie strength between Bob and David, along with Bob's digital signature of the visualization and David's public key, Alice gains evidence and endorsement implying the strong tie. Hence, the combination of Bob's social accountability to Alice and the strong tie between Bob and David results in Alice authenticating David's online identity.[2]

2.3 Desired Properties

Our goal in this paper is to help users correctly authenticate online identities using endorsed visualizations of social tie strength. A challenge then is to accurately capture aspects of tie strength among OSN users and visually represent it to convey social proximity to other OSN users. Properties for our approach include:

Relevance with respect to social parameters. Every individual is unique and has different criteria in judging social distance. Hence, it is important to carefully select *relevant* parameters which accurately convey tie strength.

Robustness. Tie strength represented using social parameters must be robust against active attackers who attempt to claim close social proximity to others. Also, tie strength must be difficult to inflate due to social pressure, which Kim et al. [24] refer to as the *distrust revelation problem*, because users do not want to publicly admit that they do not trust another user.

Privacy preservation. Tie strength must be presented while protecting OSN users' privacy. In essence, it is de-

[2]As we will discuss in Section 5.1, little effort is required from Bob as the process can be automated.

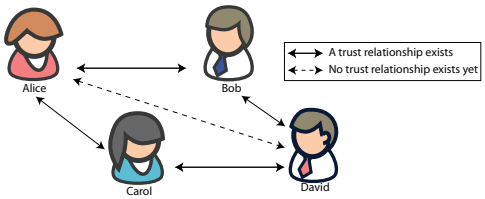

Figure 3: An example of a trust graph. David wants to be Alice's online friend, and Bob and Carol are their mutual friends.

sirable that the visualization does not leak users' sensitive personal information. However, the approaches to represent social ties must be *non-subjective* such that users can derive fair, unbiased trust relations.

Usability. It is crucial that OSN users can correctly interpret the visualization of relevant social parameters and understand social tie strength without difficulties.

2.4 Adversary Model and Assumptions

We consider an adversary whose goal is to manipulate social parameters for measuring tie strength (i.e., such that he can claim to have a strong tie to a victim's friend). When the adversary deceives the victim who accepts the friend invitation, he can successfully gather sensitive personal information of the victim and possibly her friends.

We assume that trusted friends of a user do not misbehave due to their social accountability. Furthermore, we consider an attacker who compromises a user's account to be orthogonal to the issues we address in this paper.

3. Interpersonal Tie Strength Visualization

In this section, we discuss prior studies from the field of social science that suggest both theoretical and practical parameters to depict social proximity. We then explore how the parameters can be visualized while satisfying the desired properties discussed in Section 2.3.

3.1 Background: Social Science Research

The parameters for tie strength have been studied by social science researchers. Theoretical studies suggest at least seven parameters as follows [16]: amount of time spent together [18, 26], intimacy [18] or affection [26], emotional intensity [18], reciprocal services/interaction [18, 26], structural factors (e.g., network topology and informal social circles) [6], emotional support (e.g., offering advice on family problems) [40], and social distance (e.g., socioeconomical status, education level, political affiliation, race and gender, etc.) [29]. Among multiple dimensions, Gilbert and Karahalios show that the following four relatively simple proxies are sufficient for determining tie strength in practice [16]: communication reciprocity [14, 18, 26], existence of at least one mutual friend [35], recency of communication [28], and interaction frequency [17, 18].

3.2 Visualization of Tie Strength

In this section, we formulate the details of visualizing tie strength with the following practical parameters as mentioned above: communication reciprocity, existence of at least one mutual friend, recency of communication, and interaction frequency. According to Shneiderman, disclosing patterns of past performance and providing rich feedback about content are best practices for increasing trust online [36]. Based on this suggestion, we use length of the relationship as an additional parameter. In particular, long relationships are a valuable strength indicator, since it increases accountability by adding a significant degree of moral responsibility to reporting a valid identity.

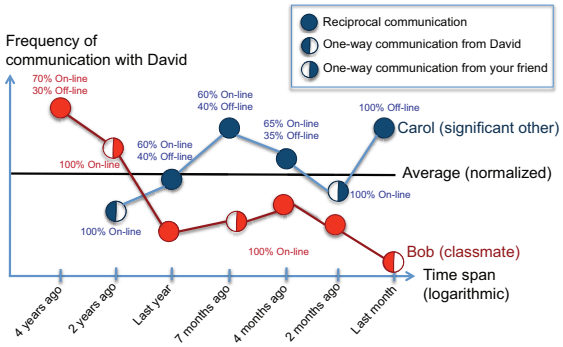

Figure 4: An example tie-strength visualization from a trust graph.

To explain the context of an online friend invitation, we consider the scenario of David who wants to be Alice's online friend. David has already established close social proximity with Alice's trusted friends. In this scenario, rather than verifying any evidence provided by David (since Alice has not met David in person), we want to help Alice make a decision based on evidence provided by her mutual friends who are socially accountable to Alice. In Figure 3, these mutual friends would be Bob and Carol.

Using this scenario, Figure 4 depicts a RelationGram, a visualization from which Alice can deduce appropriate social relationships between David and her friends, Bob and Carol. In this RelationGram, the x-axis represents a logarithmic timeline which captures the length of David's social relationships with Bob and Carol with an emphasis on recent communication. The y-axis represents the frequency of communication.

We define the frequency of communication between users U_i and U_j at a given time window τ as Eq. 1. We assume multiple types of communication (e.g., phone calls, emails, OSN comments), and $c_k(U_i, U_j, \tau)$ returns the number of interactions for communication type k. w_k is the weight of type k, which depends on the importance/intimacy of the communication (e.g., phone calls are considered as more intimate than OSN comments with public visibility), and which converts different units of communication (minutes spent on a phone call vs. length of an email) to a unit of time (e.g., by estimating the amount of time spent on online communications).

$$F(U_i, U_j, \tau) = \frac{\sum_k w_k \times c_k(U_i, U_j, \tau)}{\tau} \quad (1)$$

Hence, the frequency of communication between users U_i and U_j at τ is $F(U_i, U_j, \tau) + F(U_j, U_i, \tau)$.

Note that we depict a normalized average line $A(U_i)$ of the communication frequency, representing the normalized average frequency of communication between Bob and all his other friends. The same line also represents the average frequency of communication between Carol and all her other friends. Based on this average frequency, Alice can distinguish how frequently her own friends (Bob and Carol) interact with David compared to their other friends such that Alice can evaluate their tie strengths in a fair and unbiased manner. The average frequency A of user U_i is defined as Eq. 2. Let T be a set containing every time window τ, and $R(U_i)$ be a set of U_i's friends. When $F(U_i, U_j, \tau)$ is defined as Eq. 1, the average frequency of communication, $A(U_i)$, for U_i's friends U_x (where $U_x \in R(U_i)$ and $x \neq i$) in one

time window can be calculated as follows:

$$A(U_i) = \frac{\sum_{\tau \in T} \sum_{U_x \in R(U_i)} F(U_i, U_x, \tau) + F(U_x, U_i, \tau)}{|T| \cdot |R(U_i)|} \quad (2)$$

The reciprocity of communication from user U_i to another user U_j at a time window τ can be calculated as shown in Eq. 3, where i $\rightarrow$ j, i $\leftarrow$ j, i $\leftrightarrow$ j, and i $\nleftrightarrow$ j mean one-way communication from i, one-way communication from j, reciprocal communication, and no communication, respectively. By calculating in both directions (i.e., from U_i to U_j and from U_j to U_i), we identify one-way communication during that time window. Note that we define the threshold Th of one-wayness based on some observed amount of data (where $0 < Th < 0.5$).

$$O(U_i, U_j, \tau) = \begin{cases} \text{i} \nleftrightarrow \text{j} & \text{if} \quad F(U_i, U_j, \tau) + F(U_j, U_i, \tau) = 0 \\ \text{i} \rightarrow \text{j} & \text{if} \quad \frac{F(U_i, U_j, \tau)}{F(U_i, U_j, \tau) + F(U_j, U_i, \tau)} \geq 1 - Th \\ \text{i} \leftarrow \text{j} & \text{if} \quad \frac{F(U_i, U_j, \tau)}{F(U_i, U_j, \tau) + F(U_j, U_i, \tau)} \leq Th \\ \text{i} \leftrightarrow \text{j} & \text{otherwise} \end{cases} \quad (3)$$

The RelationGram labels the relationship status (e.g., classmates, family, etc.) between the inviter and the mutual friends, and this relationship label is assigned by the common friend. As a result, the inviter has no control over the relationship label.

The RelationGram also labels the composition of *online* and *offline* communication frequencies, where online communication may include email exchange, OSN conversation, etc., and offline communication may include phone conversation, physical interaction, etc. With these labels, a user can infer tie strength. For example, from Figure 4, Alice can infer that Bob, who is a classmate, has known David for the past four years and their frequency of communication has been decreasing such that Bob no longer interacts frequently with David compared to his other friends. On the other hand, Alice can see that Carol, who is currently in a relationship with David, has known him for about two years and she has been communicating on average more frequently with him than with her other friends. Furthermore, the "100% on-line" labels will help indicate individuals who have only established a relationship over purely online means, such as Bob and David's recent interactions in Figure 4. As a result, Alice may be able to infer, with higher confidence, that Carol's graph indicates a strong tie with David with both online and offline interactions.

This RelationGram also captures the recency of communication as follows: the x-axis to the right represents a recent time span compared to the left side. For example, Figure 4 confirms that David has communicated with Carol more recently (last month) than with Bob (2 months ago).

The reciprocity of communication is visualized with variations of coloring schemes for each dot. A fully colored dot would represent that two people communicate reciprocally. For example, both Carol and David have initiated and responded to each other last year, 7 months ago, 4 months ago, and last month. If the dot is only colored in half, only one side has tried to interact without any response from the other party. For example, 2 years ago, David initiated the communication with Carol (in which case she did not respond), but 2 months ago, it was the other way around.

The existence of more than one mutual friend is depicted by the number of graphs in the same plot. In this case, Alice can infer that two of her friends are also friends with David. A concern is that a large number of mutual friends would clutter the image such that Alice may not be able to clearly see anyone's graph. We suggest that the system picks a few of Alice's best friends (i.e., socially accountable friends whom Alice has authenticated), displays their graphs first, and leave it as an option to view other friends' graphs if necessary.

3.3 Security & Privacy Discussion

Inflation attack. Unfortunately, each parameter by itself may be insufficient to indicate the social tie strength. Indeed, some parameters may be subject to "inflation": one party can increase the value of the parameter arbitrarily without the other party's agreement. For example, frequency of communication by itself is inflatable, simply by sending SMS messages or posting notes on OSNs. The same holds for the recency of communication by sending SMS messages recently. Hence, the visual representation of a single parameter may not be a sufficiently robust indicator for determining tie strength. On the other hand, the combination of five parameters makes tie-strength manipulation more challenging and apparent. Finally, such inflation attacks are only powerful if they occur over a long time period, further compounding the attack complexity.

Collusion attack. The RelationGram purposely displays the graphs of socially-accountable people to Alice to mitigate colluding attacks; David can collude with his best friends (with whom Alice may not be close) and generate graphs portraying strong ties. However, such graphs are meaningless to Alice since she may not trust David's close friends.

Privacy and security trade-offs. Alice's friends may feel uncomfortable to reveal the graphs depicting their tie strength with David for privacy reasons. Thus, we entrust full disclosure control to users such that users themselves can decide to either reveal or protect their own graphs depicting their interactions with a particular set of friends. Those friends of Alice who decide to reveal their RelationGrams, however, may be able to mutually strengthen their friend relations with David since their decision helps David initiate a new social relationship with Alice. Similarly, we can let users decide whether to reveal or protect their relationship status (e.g., classmate, significant other, etc.). Hence, if Bob does not want to disclose to Alice that he is a classmate of David, Bob can simply select a benign label, such as "acquaintance."

Note that disclosing the graphs mutually benefits each other as it can strengthen their friendship (i.e., a user has an incentive to help the other party since the other party's graph also helps the user build new relationships). Our approach is thus incentive-compatible as everyone benefits from participation. However, concealing the graph does not necessarily imply weak tie strength as a relationship may be privacy-sensitive.

We do not recommend users to apply only a minimal set of communication channels (e.g., email only for online interactions) for generating graphs since RelationGrams may provide misleading tie-strength information. For example, Bob and David may have long phone conversations but few email exchanges, in which case only showing online interactions may mislead Alice to deduce that Bob and David may not be close friends. However, when users decide to share their RelationGrams with their friends, *the privacy leakage from RelationGrams is minimal as the data is aggregated and normalized* (i.e., RelationGrams do not reveal exact values); hence, users benefit by strengthening friendship at the price of minimal, controlled privacy leakage. In case users are worried about showing the increase and de-

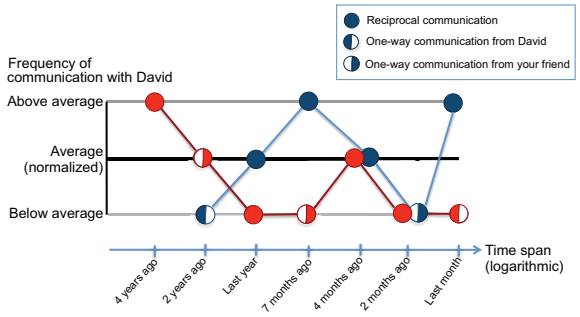

Figure 5: A variation of Figure 4 for enhanced privacy protection. This RelationGram only shows whether the frequency of interaction is above, on, or below average.

crease of the communication frequency values, such details can be simplified to show only 3 frequency values: above-, on-, or below-average, as shown in Figure 5.

As mentioned in Section 3.2, the RelationGram displays Alice's best friends first, and privacy can be further preserved by removing the name labels on the RelationGram, as shown in Figure 5. As a result, Alice may not easily determine which of the two graphs is Carol's. A trade-off, however, would be when the displayed graphs are not consistent; two graphs on Figure 5 present conflicting information, where the red graph shows diminishing communication frequency values while the blue graph shows above-average communication frequency values. As a result, lack of the mutual friends' names in such a case prevents Alice from making informed decision in case Alice generally favors Bob more than Carol for accepting invitations.

Another approach would be to apply differential privacy with appropriately chosen random noise to communication frequency values [11], and techniques such as constrained inference can be applied to significantly improve the accuracy of the differential privacy outputs [20]. We leave a more detailed privacy analysis as future work.

4. Authentication Scenarios

In this section, we present a high-level overview of our approach to help users authenticate online identities with the proposed visualization of tie strength. In the context of online friend requests, there are three possible scenarios:

1. The user has directly met the requester (physical encounter),
2. The user has not directly met the requester, but there is at least one mutual friend between the user and the requester (friend of a friend),
3. The user neither has met nor has any mutual friends with the requester (no mutual friends).

Scenario 1: physical encounter. We assume that given two users who have directly met in person, they have exchanged each others' public keys such that it is trivial to authenticate another party given their public key. Many mechanisms already exist to exchange public keys among people who meet in person: Resurrecting Duckling [38], Seeing-is-Believing [30], or physically exchanging the hash of the key on a business card. After physically meeting and actively exchanging public keys, each party can leverage trust in the received key of the other party to authenticate subsequent messages.

This approach can be applied to OSNs to authenticate friend invitations. We conducted a formative study to understand what evidence OSN users consider important for accepting friend invitations. (We put details of the study setting and results in Appendix A). Among 122 participants, 92% indicated prior encounter as an important criterion before accepting friend requests. Consequently, people can easily authenticate the inviters whom they met previously and exchanged public keys with.

Scenario 2: friend of a friend. Existence of mutual friends is a well-known factor for determining tie strength as studied in social science [35]. Our formative study supports this fact as 76% of 122 participants indicated common friends as an important feature when they accept an online friend invitation (see details in Appendix A). In case there are no previously exchanged or authenticated public keys, we leverage identity authentication based on mutual friends. The challenge with this approach is to prevent online impersonation attacks. Considering the model we discuss in Section 2.1, we briefly revisit the steps required for Alice to validate David's friendship invitation, considering the RelationGram in Figure 3. Since Alice has no prior knowledge of David's public key, Alice can evaluate it based on the information she gathers from Carol who is a friend of both Alice and David and who already shares her public key with them. To help Alice make the right decision, Carol can endorse the information by digitally signing the parameters representing her tie strength with David, and grant him the right to present the visual graph of their tie strength to Alice. Alice can authenticate such evidence by validating Carol's digital signature. Based on how much Carol is socially accountable to Alice and the tie strength as shown on the RelationGram, Alice can make sound judgment on authenticating David's online identity.

Scenario 3: no mutual friends. There may be situations when Alice has not exchanged or authenticated David's public key or there are no mutual friends between Alice and David. For example, David meets a new group of people but forgets to exchange authenticating information, or he just joined Facebook, having no friends yet. Authenticating David in this case requires a different type of approach; for example, exchanged emails, phone conversations, along with physical proximity measurements from smartphones may be combined to help Alice authenticate David. This problem, however, is outside the scope of this paper because our solution relies on the accountability arising from physical encounters, which does not exist in this scenario.

Discussion. We have designed a protocol to securely authenticate users who meet in person, and implemented it on the Android platform. Since several protocols for local authenticated exchange already exist to handle Scenario 1 (e.g., [30, 38]), we focus in this paper on Scenario 2, and leave Scenario 3 for future work.

5. Authenticating Online Friend Inviters

We illustrate how online friend invitations can be verified such that OSN users can authenticate online identities of others. We introduce Indirect Friend Authentication (`IFA`) for Scenario 2 where the inviter is a friend of a friend.

For this application context, we assume that people use smartphones for communication, as a greater number of smartphones are being sold.[3] Using smartphones, we further assume that every user can generate a public-private key pair, measure the parameters to represent tie strength, and

[3]As of March 2012, 50.4% of all mobile consumers in the U.S. own smartphones (`http://blog.nielsen.com/nielsenwire/?p=31688`).

automatically communicate with cloud application providers. Cloud application providers may be similar to Google which provides a backup service for contact information on phones, and we trust them for the availability of user information.

5.1 Indirect Friend Authentication

Our cautious OSN member Alice receives an invitation from someone named David, and this invitation indicates that they have two mutual friends: Bob and Carol.

Our Indirect Friend Authentication (IFA) protocol helps Alice authenticate David by leveraging two mutual friends. In a nutshell, the IFA protocol presents evidence that reflects the interpersonal tie strength between Alice's friend(s) and David in a RelationGram as explained in Section 3. Based on the visual evidence and the strength of social ties with her friends, Alice can make sound judgment on accepting or rejecting David's invitation.

Evidence Generation. Bob and David mutually agree to disclose the information that reflects their social proximity (i.e., reciprocity, recency, frequency of communication, and length of the relationship), and so do Carol and David.[4] Different ways exist to gather information to represent these parameters. For example, David's and Bob's phones can automatically detect and record the duration of a meeting, the call history between them, exchanged SMS text messages, Facebook posts, etc. Furthermore, the OSNs can analyze the information about their online message exchanging behavior, the photos in which both are tagged together, etc. Note that these are the optional features that users opt-in for usage and those with privacy concerns may decline to use our protocols. When all the information representing tie strength is properly gathered on Bob's phone, it would sign (using K_B^{-1}) the visual graph of their tie strength from Bob's perspective, sign David's public key, and hand it over to David. (Under Bob's permission, this process is transparent to Bob.) Carol does the same for David. Thanks to Bob's and Carol's release of the visual graphs, David has the evidence implying his social relations with Alice's friends and he inserts the graphs into the invitation.

Evidence Verification. When Alice receives the invitation from David, she has an option to see the RelationGram to determine how strong the social ties between David and her friends are. If the number of mutual friends is big (e.g., over 5), the IFA protocol determines Alice's best friends among all mutual friends and displays the visual graphs of the best few friends initially, but Alice can also check her other friends' graphs if she believes that their graphs would help her make a better decision. In this example, Alice has only two mutual friends so she can see both graphs in a single plot. Alice first verifies Bob's signed graph and David's public key using Bob's public key that she can retrieve from her own phone or from the cloud application provider. She also verifies Carol's graph in the same manner. When Alice successfully authenticates that the graphs are generated by her real, trustworthy friends (e.g., by verifying their digital signatures), she may decide to accept or reject David's invitation based on his strength of social ties with her friends. However, it is possible that the authentication fails or the graphs do not convey strong ties, possibly due to some abnormal interaction conditions (e.g., Bob could have recently relocated, reducing his interaction frequency with David and limiting the communication medium to Facebook only). We

[4]As explained in Section 3.3, disclosing the graphs mutually benefit each other, but undisclosing does not necessarily imply weak tie strength as a user can be privacy-sensitive.

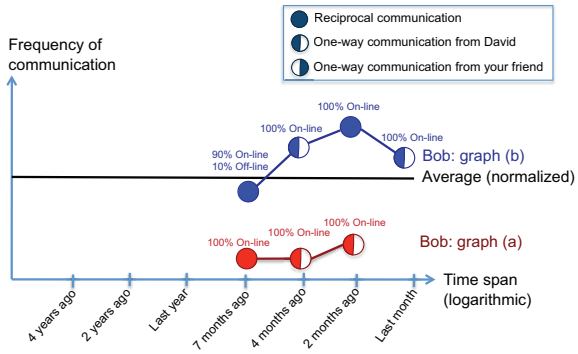

Figure 6: A RelationGram indicating unauthenticated relationships. Graph (a) shows minimal online-only communication between Bob and David. Graph (b) has high traffic with David but only in online communications.

emphasize that the visualization is one type of available evidence for users to make better tie strength evaluation, and the IFA protocol recommends Alice to gather other evidence before accepting David's invitation.

5.2 Security Analysis of IFA

We analyze how the IFA protocol mitigates the adversary models as described in Section 2.4. Recall from our example in Figure 3 that Alice and Bob met in person and exchanged public keys, and Bob and Carol are Alice's and David's common friends. We now show how the IFA protocol prevents Alice from accidentally accepting David's invitation crafted by Mallory launching impersonation, collusion, and Sybil attacks.

Impersonation Attack. Mallory can impersonate David by creating a bogus account using his information. Since the IFA protocol recommends Alice to leverage her trustworthy friends for tie strength evaluation, Mallory needs to have them as her friends. In essence, Mallory would need to convince some of Alice's real friends to accept her invitation. Some of Alice's friends (e.g., Bob) may be easygoing in terms of accepting friend invitations. Note that even if Bob is already a friend of David, Mallory can claim that David is creating an alias account. If Bob and David are close friends, Bob would verify David's invitation in other ways (e.g., in person or by phone), in which case Bob can easily recognize that Mallory's invitation is bogus and rejects such an invitation. On the other hand, if they are not close, Bob may end up accepting Mallory's invitation. However, Bob is unlikely to endorse a visualization or public key with his own signature because of his social accountability as discussed in Section 2. In the unlikely event that Bob endorses the relationship, the weak evidence of Mallory would deter Alice, as Bob would rarely communicate with Mallory and his graph may be similar to graph (a) in Figure 6. In the worst case, Bob could have communicated frequently with Mallory recently and reciprocally showing a graph similar to graph (b) in Figure 6. On the other hand, unless Bob meets David in person or communicates on the phone to authenticate David, Bob's graph would indicate that all the communication is purely based on online messages, and Alice can infer that she should thus not anchor strong trust in Bob's graph. As a result, cautious Alice is unlikely to accept David's invitation. Furthermore, even if many of Alice's friends accept Mallory's invitation, their graphs would not imply strong evidence to bind Mallory's identity to David.

In order to successfully attack Alice, Mallory needs the

evidence of tie strength and endorsement by Alice's trusted friend(s). Hence, tie-strength inflation among attackers is meaningless.

Collusion Attack. In order to convince a legitimate user to accept invitations from fake online identities, two or more attackers may collaborate to inflate each other's tie strength. For instance, Mallory can collude with another attacker Oscar and artificially generate a visual graph indicating strong trust relations. Unless Oscar is Alice's trusted friend whose graph she would rely on, their collusion to elevate tie strength is meaningless since Alice would ignore the graph.

Sybil Attack. Unlike the above two attacks, a Sybil attacker may create multiple *virtual* online identities that do not represent real people [8]. A victim may establish a friend relation with an attacker who has multiple strongly-tied Sybil identities as his friends.

Mallory can create multiple Sybil identities, generate strong tie relations with them, and attempt to deceive Alice. Unless Mallory's Sybil identities are friends with Alice (e.g., using impersonation attack which fails), the `IFA` protocol will not reveal any RelationGrams and Mallory's Sybil attack has no effect on Alice.

6. Implementation & Evaluation

We have implemented the `IFA` protocol in the context of Facebook friend invitations.Figure 7 shows the architecture and the flow of our protocol to validate Facebook friend invitations. Next, we delineate the Facebook application that we have implemented based on the `IFA` protocol called *"Do I Really Know You?"* and the online user study result.

Our Facebook web application called *"Do I Really Know You?"* is an integrated web application such that 1) users can access their friend's invitations and present visualizations in a seamless manner, and 2) the visualizations can be displayed on any smart phone with a web browser.

Do I Really Know You? We have implemented our application using three types of APIs that Facebook provides: GraphAPI, OldREST API, and Facebook Query Language (FQL). This application requests users to grant access to

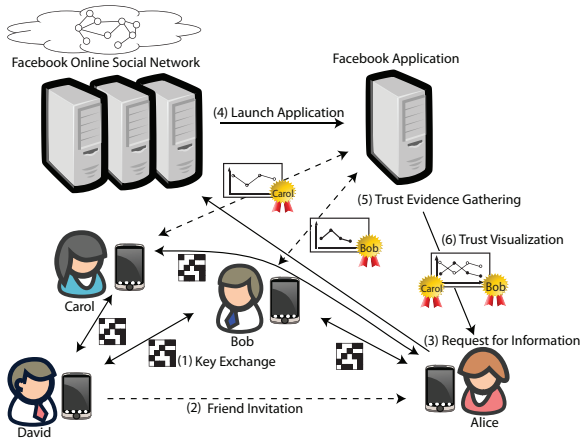

Figure 7: Architecture of **`IFA`** protocol on Facebook. This diagram illustrates the process of **`IFA`** on Facebook as follows: (1) Alice exchanges keys with her friends Bob and Carol. (2) David wants to be Alice's friend. (3) Alice requests a RelationGram. (4) Facebook launches our application. (5) Our application obtains RelationGrams from Alice's friends after endorsement. (6) The application returns the endorsed RelationGram to Alice. (7) Alice verifies the tie strength between David and her friends (Bob and Carol) using the endorsed RelationGram.

Figure 8: A snapshot of a RelationGram on Facebook. This application allows users to visually verify the tie strength between their best friends and inviters.

retrieve posts and comments on their walls.

When a user invokes *"Do I Really Know You?"*, it gets a token which enables this application to access the Facebook database on behalf of the user. The application then queries the database according to the user's policy. First, the application retrieves a list of pending friend invitations (via Facebook's *notifications.get* API). With at least one invitation, the application queries information about the inviter and the mutual friends (via *friends.getMutualFriends*). Then, the application retrieves a stream of wall information (via *stream.get* query with *limit=0* as a parameter).

As mentioned in Section 3.2, we do not explore how to automatically infer close friends of a user. Instead, when there are more than three mutual friends, this application requests the user to select the "best" friends with whom he wants to infer the inviter's tie strengths. Based on the comments from the selected mutual friend's Facebook wall, this application calculates the number of comments between each mutual friend and the inviter.[5]

Finally, the application plots the interaction frequency in a RelationGram on the web browser. Figure 8 is a snapshot of the tie strength visualization using this Facebook application.

Evaluation. We conducted an online user study to verify how much OSN users understand tie strengths between their own friends and the invitation senders and whether our visual approach provided more convincing evidence to accept/reject invitations compared to the current OSN approaches. We used Amazon Mechanical Turk (MTurk) where each participant was rewarded with $1.00 for completing the survey. Instead of inviting local people around the university for a lab-based study, we observe that MTurk workers provide a more diverse pool of participants [5, 25]. As a result, well-designed MTurk tasks provide high-quality user-study data [5, 9, 25, 39]. We followed common HCI methodologies for running MTurk studies as Kittur et al. [25] and Downs et al. [9] suggest. Based on the MTurk demographics [32], we set the location restriction flag on MTurk to invite only users located within the U.S. and reduce issues of internationalization.

Among 100 total participants, 93 were eligible for our analysis since 7 participants did not meet our requirements as they either 1) provided contradicting answers to rephrased questions, 2) ignored our instructions, or 3) did not agree to

[5]We only focus on the Facebook communication in this implementation. It is our future work to extend and include various communication methods as mentioned in Section 3.2.

run the *"Do I Really Know You?"* application on their Facebook pages.

Demographics. For the qualifying 93 participants, 47.3% identified themselves as males and 52.7% identified themselves as females. In terms of the age, 12.9% were in the age range of 18–20, 52.7% were in the range of 21–30, 20.4% were in the range of 31–40, and 14% were at least 41 years old. The majority of people (80.6%) indicated to spend at most 10 hours on Facebook per week, and 12.9% would spend 11–20 hours per week. There were 6.5% participants who spend at least 21 hours per week. Among those 93 participants, 80.6% had at least one pending friend request when they participated.

We asked the participants to download our *"Do I Really Know You?"* application on their Facebook pages and try it for at least 3 times with either currently pending friend requesters or those who are already their friends but whom they would like to visualize the tie strengths. After the third usage, we provided a code that they can enter on the MTurk page such that we can validate who ran the application as instructed. We then asked them questions to evaluate our application.

Sample questions. Sample questions that we asked are:

- How understandable is this application?
- Would you accept a friend request if this application shows that the requester has below-average/above-average/no interaction with your friends?
- How easy was it to understand how close two people were based on the graph?
- Do you think that this application provides a good indication for the strength of friendships between your friends and a requester?
- How likely is it that you will use this application before you confirm/reject a friend request?
- With this application, will you feel secure to add only an intended person to your friend list?

Results. Participants provided promising feedback satisfying our desired properties as follows:

- **Relevance:** 84.9% of the participants indicated that they were able to understand tie strength of people as shown on the graphs. 84.9% expressed that our application with a visualization illustrating five social parameters provided a good indication of tie strength, and 82% indicated that the graphs seemed to indicate correct tie strength information. We also asked them to evaluate the usefulness of each parameter: 77.4% indicated that frequency of communication helps them make better decisions, 72% indicated recency of communication to be helpful, 80.7% indicated the existence of mutual friends to be helpful, 73.3% indicated reciprocity to be helpful, and 75.3% indicated length of the relationship to be helpful.
- **Robustness:** When we asked them if they would accept an invitation if the visual graph of the inviter is placed below average or at zero communication frequency with their friends, 90.3% responded that they would not accept the invitation; 6.5% indicated that they would accept as long as there are some mutual friends, and 3.2% would accept regardless of the RelationGram. Hence, *RelationGrams can successfully protect users from accepting invitations from potentially malicious strangers.*
- **Privacy:** The participants liked that they were able to discern which information they felt comfortable sharing with others. For example, 81.5% indicated that they would be willing to share the diagram with their close friends and/or family members.
- **Usability:** 82.8% indicated that our application was manageable or easy to use. 88.2% found our visual evidence to be useful and 83.8% expressed the likeliness to use our application before confirming an invitation.

Participants provided positive feedback in acceptability: given RelationGrams, 72.7% indicated that they would feel secure to confirm only an intended person as their friend.

7. Discussion and Future Work

While we have demonstrated that our system provides useful real-world evidence to users for validation of online properties, the system raises several issues that warrant further discussion.

A first question is how usable such a system would really be, whether it would represent too much of a burden on the user that negates its utility. Although further research is needed, several points indicate that the burden would be minimal. Existing systems could automatically collect interaction information without burdening users, aggregating email, SMS, Google+, etc. exchanges. Smart phones could also collect information about people we physically meet, through the use of voice recognition or by detecting the proximity of the other party's smart phone. Generation of evidence, endorsement (i.e., digital signature), and distribution to friends could also be automated. A minor burden would be the configuration, where a user can decide which tie strength visualizations to share with others. This could occur through an opt-in process, where a user could add friends whose tie-strength information can be shared.

Another important question is on incentives: would users really have incentives to share their tie strength visualizations? In our user studies, it was clear that users seemed eager to obtain such information to validate online invitations with confidence. Although further studies are needed, we believe that people's inherent altruism that explains Internet phenomenons such as Wikipedia would also encourage users to share their tie strength visualizations, because little burden is required on their part, and they can help their friends to befriend each other with more safety.

8. Related Work

Social tie strength. Friend recommendation systems and tie strength analyzers have been a popular research topic for improving social media design elements. Gilbert and Karahalios design a predictive model mapping social media data to tie strength using multiple parameters, and their model distinguishes strong and weak ties with over 85% accuracy [16]. However, their approach does not guarantee to provide non-subjective assessment of tie strengths since users can easily figure out their tie strength based on the accessibility of private information. Based on their findings of factors affecting tie strength, we develop visualizations and test how they influence online identity authentication.

Researchers have analyzed if the existence of friendship links are valid indicators of user interactions in OSNs. Based on the study using the Facebook [41] and Twitter [22] data, the authors show that user interactions in OSNs significantly deviate from the social link patterns. Wilson et al. also propose an interaction graph that can better represent the actual user interactions based on the reciprocity of OSN communications [41]. Unlike their graph which solely considers OSN interactions, we propose that tie strength is derived

based on both online and physical interactions.

Security for social network sites. Researchers have investigated the feasibility of launching identity theft attacks on OSNs. Experiments demonstrate the ease of crawling personal information of real OSN users by creating a phony profile and exploiting how users would confirm the friend request [1], even despite some purposely left clues of the inviter's fictitious identity [33]. Hamiel and Moyer exploit an identity theft attack by impersonating a high-profile security expert with publicly available personal information and demonstrate that the forged profile received many friend requests, even from the immediate family member of the target [19]. Bilge et al. extend this work by automating the impersonation of the existing user profiles and sending requests to the victims' contacts, successfully crawling personal information of the contacts [2]. All these works emphasize the importance of authenticating the online identities to minimize the exposure of personal information to attackers.

Net Trust is a trust evaluation system that enables a user to make educated decisions about websites based on the implicit and explicit ratings from the social networks and providers [7]. We doubt the robustness of social network topology information, as various recent attacks confirm [1, 2, 19, 33]. Thus, we propose tie strength indicators that are more robust than social network topology.

Secure associations of user identities and public keys. PGP [42] proposes a "web of trust" to associate public keys with individuals. Unfortunately, long trust chains and the distrust revelation problem hampers its usefulness, because users overclaim trust relations as the information is publicly visible. Moreover, PGP only considers *endorsement* without *evidence*, hampering its power and usefulness.

User authentication based on the social network information has been an emerging research area. Brainard et al. develop a vouching system using human-mediated authentication for access control in situations where primary authenticators become unavailable [4]. From the backup authentication mechanism that allows previously-appointed trustees to provide account recovery code, Schecher et al. reveal two problems: people forget whom they choose as trustees and many trustees would reveal authentication codes to a close friend [34].

Evaluating the credibility of online identities using social networks has also been studied by Sirivianos et al. [37]. Their approach relies on two aspects: trust metric computation based on the tag values that friends assign to a user's identity, and the credentials on the trust metric by an OSN. Garris et al. also apply web of trust for spam filters with zero false positives [15]. Their whitelisting system exploits friend-of-friend relationships among email correspondents and populates whitelists automatically with cryptographic private matching techniques to preserve the privacy of email contacts. However, these systems rely on the robustness of the social network topology, which is questionable unless approaches that we suggest are adopted.

9. Conclusion

Online user behavior is faced with an uncomfortable trade-off: should we really accept unauthenticated friends' invitations that might represent impersonation attempts to deceive; or should we deny them at the cost of losing potentially valuable relationships and become socially isolated? Currently, there is no secure and usable mechanism that would enable us to resolve this dilemma.

Our online identity authentication model helps to resolve this dilemma. Friendship invitations become authenticated, thereby thwarting impersonation and deception. We expect that user actions would become substantially safer in online social networks if deterrence against deception based on social accountability would be supported.

Our online identity authentication system implements a simple identity authentication logic in a visually compelling manner that is consistent with mental models derived from real-life experience. That is, it enables a casual user to authenticate online identities in a safe and easy-to-use manner.

10. References

[1] Sophos Facebook ID Probe. `http://www.sophos.com/pressoffice/news/articles/2007/08/facebook.html`.

[2] L. Bilge, T. Strufe, D. Balzarotti, and E. Kirda. All Your Contacts Are Belong to Us: Automated Identity Theft Attacks on Social Networks. In *Proceedings of WWW*, 2009.

[3] Y. Boshmaf, I. Muslukhov, K. Beznosov, and M. Ripeanu. The socialbot network: When bots socialize for fame and money. In *Annual Computer Security Applications Conference (ACSAC)*, Dec. 2011.

[4] J. Brainard, A. Juels, R. L. Rivest, M. Szydlo, and M. Yung. Fourth-Factor Authentication: Somebody You Know. In *Proceedings of CCS*, 2006.

[5] M. Buhrmester, T. Kwang, and S. D. Gosling. Amazon's Mechanical Turk: A New Source of Inexpensive, Yet High-Quality, Data? *Perspectives on Psychological Science*, 6(1):3–5, 2011.

[6] R. S. Burt. Structural Holes and Good Ideas. *American Journal of Sociology*, 110(2):349–399.

[7] J. Camp. The Reliable, Usable Signaling to Defeat Masquerade Attacks. In *Workshop on the Economics of Information Security*, 2006.

[8] J. R. Douceur. The Sybil Attack. In *IPTPS*, 2002.

[9] J. S. Downs, M. B. Holbrook, S. Sheng, and L. F. Cranor. Are Your Participants Gaming the System?: Screening Mechanical Turk Workers. In *Proceedings of CHI*, 2010.

[10] P. Doyle and S. Hanna. Analysis of June 2003 Survey on Obstacles to PKI Deployment and Usage. 1.0, 2003.

[11] C. Dwork. Differential Privacy: A Survey of Results. *Theory and Applications of Models of Computation*, 4978:1–19, 2008.

[12] Economist. Duly notarised. `http://www.economist.com/blogs/babbage/2011/09/internet-security`, Sept. 2011.

[13] C. Ellison and B. Schneier. Ten Risks of PKI: What You're not Being Told about Public Key Infrastructure. *Computer Security Journal*, XVI, 2000.

[14] N. E. Friedkin. A Test of Structural Features of Granovetter's Strength of Weak Ties Theory. *Social Networks*, 2:411–422, 1980.

[15] S. Garriss, M. Kaminsky, M. J. Freeman, B. Karp, D. Mazieres, and H. Yu. RE: Reliable Email. In *Proceedings of NSDI*, 2006.

[16] E. Gilbert and K. Karahalios. Predicting Tie Strength With Social Media. In *Proceedings of CHI*, 2009.

[17] E. Gilbert, K. Karahalios, and C. Sandvig. The Network in the Garden: An Empirical Analysis of Social Media in Rural Life. In *Proceedings of CHI*, 2008.

[18] M. S. Granovetter. The Strength of Weak Ties. *The American Journal of Sociology*, 78(6):1360–1380, 1973.

[19] N. Hamiel and S. Moyer. Satan Is On My Friends List: Attacking Social Networks. In *Black Hat Conference*, 2008.

[20] M. Hay, V. Rastogi, G. Miklau, and D. Suciu. Boosting the accuracy of differentially private histograms through consistency. In *Proceedings of the VLDB Endowment*, volume 3, pages 1021–1032, 2010.

[21] Q. Hu, Z. Xu, T. Dinev, and H. Ling. Does Deterrence Work in Reducing Information Security Policy Abuse by Employees? *Communications of The ACM*, 84(6):54–60, 2011.

[22] B. A. Huberman, D. M. Romero, and F. Wu. Social Networks That Matter: Twitter Under the Microscope. *First Monday*, 14(1), 2009.

[23] D. Irani, M. Balduzzi, D. Balzarotti, E. Kirda, and C. Pu. Reverse social engineering attacks in online social networks. In *Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA)*, July 2011.

[24] T. H.-J. Kim, L. Bauer, J. Newsome, A. Perrig, and J. Walker. Challenges in Access Right Assignment for Secure Home

Table 1: Survey results of importance of different features for accepting/rejecting a friend invitation.

	Not important at all	Not important	Indifferent	Somewhat important	Very important	Total
You met the inviter before.	0.8%	0.8%	6.6%	20.5%	71.3%	100%
There are 10 common friends.	9.8%	5.7%	8.2%	44.3%	32.0%	100%
You and the inviter attend(ed) the same school.	5.7%	10.7%	14.8%	48.4%	20.5%	100%
You see the photo of the inviter.	6.6%	4.1%	9.0%	32.0%	48.4%	100%
Your good friend has known the inviter for at least 2 years.	8.2%	9.0%	23.8%	34.4%	24.6%	100%

Networks. In *Proceedings of USENIX Workshop on Hot Topics in Security (HotSec)*, Aug. 2010.

[25] A. Kittur, E. H. Chi, and B. Suh. Crowdsourcing User Studies with Mechanical Turk. In *Proceedings of CHI*, 2008.

[26] D. Krackhardt. The Strength of Strong Ties: The Importance of *Philos* in Organizations. *N. Nohria and R. Eccles (eds.), Networks and Organizations: Structure, Form,and Action*, pages 216–239, 1992.

[27] D. Z. Levin and R. Cross. The Strength of Weak Ties You Can Trust: The Mediating Role of Trust in Effective Knowledge Transfer. *Management Science*, 50(11):1477–1490, 2004.

[28] N. Lin, P. W. Dayton, and P. Greenwald. Analyizing the Instrumental Use of Relations in the Context of Social Structure. *Sociological Methods Research*, 7(2):149–166.

[29] N. Lin, W. M. Ensel, and J. C. Vaughn. Social Resources and Strength of Ties: Structural Factors in Occupational Status Attainment. *American Sociological Review*, 46(4):393–405, 1981.

[30] J. M. McCune, A. Perrig, and M. K. Reiter. Seeing-Is-Believing: Using Camera Phones for Human-Verifiable Authentication. In *Proceedings of the IEEE Symposium on Security and Privacy*, 2005.

[31] R. Reagans and B. McEvily. Network Structure and Knowledge Transfer: The Effects of Cohesion and Range. *Administrative Science Quarterly*, 48(2):240–267, 2003.

[32] J. Ross, L. Irani, M. S. Silberman, A. Zaldivar, and B. Tomlinson. Who Are the Crowdworkers?: Shifting Demographics in Mechanical Turk. In *Proceedings of CHI*, 2010.

[33] T. Ryan. Getting in Bed with Robin Sage. In *Black Hat Conference*, 2010.

[34] S. Schechter, S. Egelman, and R. W. Reeder. It's Not What You Know, But Who You Know. In *Proceedings of CHI*, 2009.

[35] X. Shi, L. A. Adamic, and M. J. Strauss. Networks of Strong Ties. *Physica A: Statistical Mechanics and its Applications*, 378(1):33–47.

[36] B. Shneiderman. Designing Trust into Online Experiences. *Communications of the ACM*, 43(12):57–59, 2000.

[37] M. Sirivianos, K. Kim, and X. Yang. FaceTrust: Assessing the Credibility of Online Personas via Social Networks. In *Usenix HotSec*, 2009.

[38] F. Stajano and R. J. Anderson. The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks. In *Security Protocols Workshop*, 1999.

[39] M. Toomim, T. Kriplean, C. Portner, and J. A. Landay. Utility of Human-Computer Interactions: Toward a Science of Preference Measurement. In *Proceedings of CHI*, 2011.

[40] B. Wellman and S. Wortley. Different Strokes from Different Folks: Community Ties and Social Support. *The American Journal of Sociology*, 96(3):5538–588.

[41] C. Wilson, B. Boe, A. Sala, K. P. N. Puttaswamy, and B. Y. Zhao. User interactions in social networks and their implications. In *ACM EuroSys*, Apr. 2009.

[42] P. R. Zimmermann. *The Official PGP User's Guide (second printing)*. Cambridge, MA: MIT Press, 1995.

APPENDIX

A. Formative Study

Our goal for this formative study was to understand the criteria that OSN users consider important for accepting online friend invitations. We recruited 130 active Facebook users using Amazon Mechanical Turk (MTurk), where each participant was rewarded $1.00 for completing the survey. We were able to analyze results from 122 participants after eliminating careless participants as follows: 1) we were able to filter out those who would not qualify for the study (e.g., a participant who spends 0 hours on Facebook, etc.), 2) we were able to detect careless participants who provided contradicting answers to some questions that we purposefully asked multiple times with different wordings, 3) we were able to detect those who would add accept an invitation from a stranger, and 4) we measured the duration of their participation to eliminate those who finished the study too quickly. For demographics, 61% were females and 40% were males, all from the U.S. with the average age of 25 years old (standard deviation = 7.32).

Here are some questions that we asked and the corresponding responses:

- Do you currently have any pending invitations that you have neither accepted nor rejected for over a week? (47% currently had pending invitations.)
- How much do you mind if a stranger can see the details of your account? (67.5% answered to care a lot, 28.5% answered to mind somewhat, and 4.1% answered not to mind.)
- Have you ever rejected or ignored a friend invitation on Facebook? (92.7% have rejected/ignored invitations and 3.3% answered that they were not sure.)
- When you receive friend invitations, how often do you check their Facebook pages before accepting/rejecting/ignoring the invitation? (56.1% answered to check very often, 20.3% answered to check somewhat often, 15.4% answered to check sometimes, and 8.2% answered to check rarely.)
- What feature(s) do you check before you accept/reject a Facebook friend invitation? (The main features that the participants check the most were the inviter's name (86.2%), common friends (85.4%), and the picture of the inviter (65%).)
- Do you care how many friends you have on Facebook? (82.1% answered not to care, 8.9% answered to care, and 8.9% answered that they may care.)
- Do you currently have a stranger in your Facebook friends list? (100% answered no.)
- How important is each feature when you make a decision on accepting/rejecting a friend invitation? (Answer is in Table 9.)

Based on this user study, we were able to confirm that users consider 1) physical prior encounter, and 2) common friends as important features before they accept friend invitations, and our approach leverages these two features to help OSN users establish trust relations with confidence.