Security and Privacy Preservation in Human-Involved Networks

Craig Asher[1], Jean-Philippe Aumasson[2,*], and Raphael C.-W. Phan[1]

[1] Electronic & Electrical Engineering, Loughborough University, LE11 3TU, UK
[2] FHNW, 5210 Windisch, Switzerland

Abstract. This paper discusses security within human-involved networks, with a focus on social networking services (SNS). We argue that more secure networks could be designed using semi-formal security models inspired from cryptography, as well as notions like that of ceremony, which exploits human-specific abilities and psychology to assist creating more secure protocols. We illustrate some of our ideas with the example of the SNS Facebook.

1 Background

Social networking services (SNS) is arguably one of the hottest internet applications to have hit the recent internet scene. People from all walks of life share personal information with their friends, sometimes friends of friends, and often with anyone having an internet connection. These people include professionals who link to friends they have met in their professions. For instance, there are over fifty mainstream cryptographers actively interacting with and updating each other on their recent activities or locations in the Facebook friends' list of one of this paper's authors. Facebook profiles also exist of celebrities, and of world leaders such as Barack Obama or Gordon Brown. However, Facebook and other SNS (Friendster, LinkedIn, MySpace, Orkut, to name a few) are victims of their success and face a multitude of security problems.

Privacy in SNS. In one's profile lie personal information such as birth date, local area, education background, significant other's name, religious and political views, etc. Due to security and privacy issues with Facebook being highlighted at different times, the default privacy setting is such that supposedly only friends can access profile info, while any member of the public can only see one's "public search listing", if one hasn't disabled this feature. Yet, it has been highlighted the amount of access to user profiles that is awarded to Facebook application developers.

Anyone can use the Facebook API to design a gadget application that can be integrated into users' profile, signalling the contradicting privacy policy enforced by Facebook; while seemingly attempting to safeguard a user's profile by limiting

*Supported by the Swiss National Science Foundation, project no. 113329.

access only to his friends, yet any motivated non-friend could build on publicly available code to develop a simple application. This action then allows this non-friend into the inner circle of developers who have more access privileges to user profiles. Almost all third-party applications during installation pop up a disclaimer box to which a typical user during any installation process would simply click Yes. This allows the developer of the installed application to access to the user profile.

What is perhaps unknown to a typical user is that even if she does not explicitly add any application nor check on the disclaimer box, a developer has access to developer library functions including `Users.getInfo` that allows to search on a Facebook ID for the user's profile including birth date and local area of residence[3]. A study lead by Felt and Evans in 2008 showed that [9] among the 150 then top applications, more than 90% didn't need the private information available to them, but only public information or no information at all.

Tied to this issue of easy access to personal information, often due to the user himself unknowingly sharing his information with friends on SNS, is the issue of adversaries circumventing authentication systems that are based on personal information verification, e.g., the widely used birth date in UK based authentication systems, mother's maiden names elsewhere, favourite pet names, etc.

An unavoidable threat. *"The social network is your strongest weapon... If you try to find a technical solution to identity spoofing, you'll step on the social feedback mechanism."* (Konstantin Guerick, cofounder of LinkedIn, in 2003 [21]). Indeed, a major problem of all SNS impersonation (or identity spoofing), that is, the fraud of pretending being someone else in order to get various benefits. For example, anyone can register an account under one's neighbour name, take a picture of her to put on the newly created profile, forge an authentic-looking email address `firstname.surname@somewebmailprovider`, send friend request to her friends and relatives, etc. Note that PGP's "web of trust" concept may be used to prevent from impersonation, however it cannot be directly integrated to SNS. Impersonation on SNS may be a key component of a more general identity theft fraud.

To counter the practical impossibility of authenticating each new user, some networking sites have used countermeasures to mitigate the risk of impersonation on those platforms, for example:

- In its early days, Facebook was limited to users from universities, and required an email address with the extension `.edu`.
- LinkedIn uses a sort of identity escrow [13]: to contact another site member, LinkedIn requires you to contact someone you both know for an introduction.

However, for the sake of accessibility, most networks have no such practices, and only rely on complaints by users, who then have to justify themselves by, for example, showing a picture of them holding an ID. Perhaps the strongest form

[3] See `http://wiki.developers.facebook.com/index.php/Users.getInfo`.

of authentication is via interactions on those platforms (discussions, exchange of photos, etc.). It may thus be desirable to encourage interactions between alleged friends, or, more generally, to design protocols that rely on human behaviour.

A holistic approach. In order to follow a holistic approach to security, including the human factor into the consideration is a wise move. Some work in this direction has been initiated, the so-called idea of ceremony design [12], inspired by cryptographic protocols. Instead of brushing off the fact that humans are often the weakest link with a statement that this treatment is out of the scope of network security, the idea behind the ceremony approach is to deal with this factor explicitly in a security system's design; where humans are treated as separate entities from their machines, and assumed to be subject to social and psychological influences or tendencies. For example, the process by which one authenticates to its e-banking service, using a personal device physically protected by the account's owner, is a typical case of ceremony, which captures out-of-band channels; for comparison, the process that secures Amazon transactions is transparent to the user, and requires no non-trivial human interaction to succeed.

More generally, where once upon a time machines (non-humans) were introduced into conventionally human-performed tasks for the sake of human convenience, these days we increasingly see the re-inclusion of human entities into network security tasks, e.g., pairing in Bluetooth [5] and wireless USB standards [25], CAPTCHA [3].

In this work, we highlight the increasing emphasis on *human-involved network* tasks; exemplified by the above discussed example of ceremonies, and the involvement of humans as intermediaries during authentication processes. More precisely, we believe that the notion of ceremony, along with the definition of a formal security model, constitutes an adequate framework to protect privacy in SNS, and limit the risk of impersonation. We advocate the use of semi-formal adversarial model in the design of SNS, inspired by models used in the analysis of cryptographic protocols.

2 Open problems and first steps

Within the context of human-involved networks, we list these two main open problems below:

1. How do we best model security within human-involved networks, taking the holistic approach of including social and psychological issues of humans and inspired by the ceremony design paradigm.
2. Can we design mechanisms or protocols that achieve security or privacy tasks within human-involved networks where we have the additional human party being able to perform machine-intractable tasks, e.g., to achieve authentication, secrecy (sharing of information, profiles, etc), even possibly multi-party computation.

To motivate the need for careful consideration of security in social networks design, we first look at how example SNS can be circumvented. We observe that the use out-of-band channels seems unavoidable to achieve reasonable level of authentication, and argue in favor of the use of semi-formal security model inspired from cryptography.

2.1 Example issues to address

To approach the above discussed problems, take Facebook again as an example for discussion. Its authentication factor (employed by the Facebook system to authenticate new users) is based on emails, i.e., what ties to a human user is an email account that the user supplies upon registration, and which becomes the Facebook username.

Registration and authentication. The authentication security of many SNS reduces to that of the underlying email registration system. This is where the problem lies: with almost all webmails, any human can register for a new email account without any verification of the human's identity; bots are prevented from registering by CAPTCHA's, although these can be relatively easily attacked with human solvers, or via CAPTCHA farms that charge a few dollars for solving a thousand CAPTCHA's.

Even in the event that the adversary is trying to forge the email address of a user for whom his friends know for sure to have a specific email account, the adversary could still try to create an email address that is a small difference from actual user's email address; this makes it probable that one overlooks the difference and deems the email address to be the authentic one. Indeed, such email accounts by convention do not have built in identification mechanisms that tie to the human user's actual identity, since it would be assumed that the human user would use some out-of-band channel, e.g., telling someone in person, to communicate to his correspondents what his email address is.

Recommendation. Rather than relying on the authentication security of email registration systems, it seems prudent that SNS be designed such that if it is required that a username needs to be tied a real human identity, that some out-of-band channel be used between the registering user and Facebook to authenticate the former. Nevertheless, this is impractical since it is not in Facebook's interest to identify users; rather, it is users of Facebook who have a stake in the need to identify other users. Thus, it is better that Facebook maintains the same view of authentication security as that of email registration systems: that authenticating users is out of scope of its design, but is more of the concern of a Facebook application as a service to application users.

Befriending strangers. Another issue with SNS is that of adding new friends to a user's friends list. Typically, a user could request to be added to another user's friends list, and the latter needs to confirm this before the addition is

made to the list. Therefore, exploiting this, another implicit way that Facebook users authenticate potential new friends is based on the "who you know" factor, or "who knows you", i.e., if I get a friend request from someone whose username contains the name of a researcher I have heard of, and when I see his friends list I see many researchers in the same field, I would generally have little suspicion that he is an impersonator. Indeed, since it is easy to register for an email account bearing a name (first and last name), an adversary could randomly search for a user, view his friends list (which is public) and try making friend requests to the user and all his friends and friends of friends etc by using an email address bearing the name of someone they know (obtainable from their friends list either also on Facebook or it can be a friends list of another SNS like MySpace). As long as one in the circle of friends accepts the request, the adversary would successfully become an insider to the friends circle, and via friendship links he can now portray a much more convincing profile to other friends in the circle since he is already a friend of a user in that friends circle.

Recommendation. It is therefore worthwhile to consider revising the `Confirm Friend` command in Facebook to include some form of out-of-band channel between the friend requester and the friend confirmer, e.g., including the phone number, or ensuring both parties are simultaneously online and logged on to Facebook to partake in a voice based challenge response protocol, so that the confirmer can verify the requester really is who s/he believes to be. Also, SNS may encourage the use of video meetings, which would prevent from impersonation as long as the victim's is physically known.

Alternatively, some would argue for LinkedIn's method of adding friends (contacts), i.e., the friend requester needs to explicitly input a description of how s/he knows the friend confirmer.

A radical approach was taken by the popular microblogging platform Twitter, whose *verified accounts* (mostly for celebrities) are manually authenticated via direct contact with the alleged owner of the account. Still, email account remains the weakest link.

Gaining entry into the friends circle via any point. In fact, due to the social network of friends, through connectivity degrees (as explicit on LinkedIn), the point to note is that an adversary may gain entry into a friends circle at any point (i.e., via any user adding him as a friend) no matter the degree of the connection from the actual target user that the adversary wishes to attack. And since SNS like Facebook are used by people of all ages, even if the target user is a security paranoid, chances are that s/he would be a friend (or relative) of a friend of someone naive and gullible who would not think twice about confirming friend requests from strangers. To prove this point, the first author randomly made friend requests to five stranger girls and two confirmed the requests without any checking. While it may not be interesting to attack the easily trusting users, it is through them that an adversary becomes an insider of the friends circle and by iterating the friend request process s/he can slowly work his/her way towards the target user, who may be several degrees away.

Similarly as with issue 2, even if the friend requester is consider an insider to the friends circle since s/he is already on the friends list of some user in the friends circle, the friend confirmer should still apply Recommendation 2 to authenticate the friend requester.

Recommendation. Besides recommendation of the second issue, a general recommendation is to only allow email accounts from email registration systems that authenticate the registering user. For example, Gmail used to have some form of this where they required new users to be invited by existing users. Another recommendation, e.g., for the design of a ceremony, would be to encourage users to look at the friend list of people who send friend requests, to spot more easily stranger insiders.

Accounts on multiple SNS. It is common for people to be registered on several SNS, because of the networks' complementarity (for example, one for professional contacts, and another for personal contacts and actual friends), or because of a trend shift, for instance. However, this opens the possibility of attacks combining several networks, as illustrated by a trick involving accounts on two SNS [7] (description is given with MySpace and Facebook as examples, but the attacks works for almost any SNS, and does not exploit any feature specifica to MySpace or Facebook). In short, this trick works by

1. befriending strangers that are both on network X and on network Y;
2. spot friends of those friends that are on network X but not on network Y;
3. use the information available from network X to forge profile of this second set of strangers on network Y;
4. send friend requests to the first set of strangers.

In [7], the author remarks that in fact on Facebook, the site may even automatically suggest the forged profiles as friends of people indirectly connected to you, which amplifies the power of the attack.

Although very simple, the above attack is potentially very powerful, and seems difficult to prevent by the networks themselves, even if they would collaborate and share information on their users.

Recommendation. To help preventing that kind of attack, SNS may include information on contacts that have no account on the network, and create a status of "ghost friends". For example, there exists automated tools (e.g. in Facebook) to import contacts from popular webmails, and also to send invitations to unregistered contacts, but there is no feature to save information on unregistered contacts. Also, it may be desirable to encourage interaction between SNS, or to design tools to check the similarity of authentication factors (typically, email addresses) from one network to another.

Moreover, to minimize the damage, SNS should be careful with friend suggestions, for example by only suggesting accounts that have been registered for a long time, and had enough interactions with other people to convince of their authenticity.

2.2 Designing more secure SNS

Within SNS like Facebook, the initial underlying trust assumption needs to be carefully thought through. A lot of these rely on the trust assumption that email addresses link to an individual person; yet typical email account registration mechanisms don't authenticate the user so the existence of an email address based on a name is insufficient. One interesting immediate work will be the design of social network authentication mechanisms based on email that explicitly treats the initial setup of trust assumptions among potential users. Some work in this direction appear in [15, 12].

For the rest of this paper, we will use the term 'friend' of user ID1 to denote another user ID2 who has been directly added by ID1 to its SNS (some SNS may use other terms, e.g., "contact", etc). We will use the term 'friends list' of ID1 to denote all users who are directly a friend of ID1. We use the term 'indirect friend of degree n' to denote a user IDi who is not directly a friend of ID1 (i.e., not in ID1's friends list) but who is connected indirectly to ID1 via some n intermediate friends; e.g. if ID1 is a friend of ID2 who is a friend of ID3 who is a friend of ID4, and this is the only path connecting ID1 and ID4, then they are said to be indirect friends of degree 2. While they are not directly friends, it is worth to capture this connection since human tendency often leads to the propagation of the trust that a user has in his direct friends down through the chain of each pair of direct friends consecutively connected in the social network path. We use the term 'friends circle' to denote the network of social paths connecting each consecutive pair of direct friends. For instance, ID4 is an insider within ID1's friends circle.

We feel that since SNS inherently serve the purpose of being a second (virtual) friends circle to actual physical human friendship circles in real life, it makes sense to leverage on the actual human interactions in real life as an out-of-band channel to strengthen the SNS. Out-of-band channel examples include telephone (voice), video conferencing, etc. Other settings that use out-of-band channels to strengthen security include SAS-based protocols [22], Bluetooth [5], wireless USB [25].

Modelling the adversary. We believe that to design secure and sound protocol, one would benefit from using security models similar to those used to evaluate the security of cryptographic protocols (see e.g. [6] for key-exchange, or [23] for protocols involving RFID tags). Such models formally define the actions available to the user, and thus exploitable by the adversary. In particular, notions of adversaries like *honest-but-curious*, or *active adversary* seem well suited to describe the different type of personalities within an SNS.

Although formal models are not panacea, for they don't by convention capture all the attack possibilities (and notably the arguably principal threat to security systems, social engineering), they could provide guidance for identifying potential weaknesses in SNS, and thus simplifying the establishment of countermeasures.

A first, simple, proposal of a model may consist of the following functionalities, where "NID" stands for the network ID:

- Register(NID, email): when the email provided is not already in use by a registered user of the SNS, this returns a new user ID.
- GetPublicInfo(NID, ID1, ID2): if the request is made by an entity not yet registered, ID1 is some generic symbol, otherwise it is this user's ID; if ID1 is allowed to, it receives the public information of the user ID2.
- GetPrivateInfo(NID, ID1, ID2): if ID1 is allowed to, it receives the private information of the user ID2.
- GetContacts(NID, ID1, ID2): if ID1 is allowed to, it receives the list of friends of ID2.
- ContactRequest(NID, ID1, ID2): ID1 asks ID2 to include it in its friend list, and thus gets the corresponding privileges of being an insider in ID2's friends circle.
- OutOfBandInteract(ID1, ID2): ID1 initiates an interaction with ID2 via an out-of-band channel, typically a human-involved physical communication medium e.g. voice or even face to face meeting.
- Corrupt(NID, ID1, ID2): ID1 obtains authentication credentials of ID2 and can thus impersonate her, to some extent (e.g., limited by interaction with other individuals).

More realistic models may include functions specific to a given SNS, as well as more refined functions for some of the examples above (e.g., ContactRequest may be decomposed into multiple steps). Depending on the particular SNS features, a model may contain formal functionalities for

1. classes of actions performed by users, like using a Facebook (third party) application, posting information (photo, comment) on one's profile, etc.;
2. actions by the interface that influence the users' choice, like display of friend suggestions, warning message, etc.

Such model would facilitate description and understanding of certain classes of attacks, for example the one described on multiple SNS. And this allows as a first step, to pinpoint sufficient conditions to foil an attack and thus designers of networks may introduce human-involved ceremonies to reduce the risk, or complicate such attacks.

3 Concluding remarks

It is commonplace in cryptography to quote Kerckhoffs' treaty [14] to motivate the case against achieving security by obscurity. What is perhaps lesser quote about this work and exactly matches our context of human-involvement in SNS is the following: "... [the system] must be easy to use and must neither require stress of mind nor the knowledge of a long series of rules to observe." Thus, the importance of taking the human involvement element into consideration during a security systems design stage; and equally the human induced issues such as

socio-economic and psychological factors that while not apparently technical do highly impact the security.

We have highlighted that SNS with registration processes based on email addresses are only as secure as the underlying email authentication mechanism since they assume an email address is uniquely identifying. We have argued the case for explicitly involving humans into the authentication process, in line with recent related work for email based machine authentication [12], ceremonies [8], SAS based protocols [22] and some others [3, 16].

References

1. A. Adams and M.A. Sasse, "Users are Not the Enemy," *Communications of the ACM*, Vol. 42, No. 12, 1999, pp. 40-46.
2. B. Adida, "BeamAuth: Two-Factor Web Authentication with a Bookmark," *Proc. ACM CCS '07*, 2007, pp. 48-57.
3. L. von Ahn, M. Blum, N.J. Hopper and J. Langford, "CAPTCHA: Using Hard AI Problems for Security," *Advances in Cryptology - EUROCRYPT '03*, Springer LNCS vol. 2656, 2003, pp. 294-311.
4. H. Berghel, "Faith-based Security: A Tongue-in-Cheek Look at Serious Security Issues," *Communications of the ACM*, vol. 51, No. 4, 2008, pp. 13-17.
5. Bluetooth SIG, "Bluetooth Core Specification v2.1 + EDR," 26 July 2007.
6. R. Canetti and H. Krawczyk, "Analysis of Key-Exchange Protocols and Their Use for Building Secure Channels," *Advances in Cryptology - EUROCRYPT '02*, Springer LNCS vol. 2045, 2001, pp. 453-474.
7. M. Elgan, "Why you can't trust 'friends' on Facebook," *IT World*, 26 November 2008.
8. C. Ellison, "Ceremony Design and Analysis," *IACR Cryptology ePrint Archive*, report 2007/399, last revised 17 October 2007.
9. A. Felt and D. Evans, "Privacy Protection for Social Networking Platforms," *Proc. W2SP '08*, 2008.
10. S.L. Garfinkel, "Email-based Identification and Authentication: an Alternative to PKI?," *IEEE S & P*, vol. 1, No. 6, 2003, pp. 20-26.
11. P. Gutmann, "Underappreciated Security Mechanisms" . Available at `http://www.cs.auckland.ac.nz/ pgut001/pubs/underappreciated.pdf`.
12. C. Karlof, J.D. Tygar and D. Wagner, "Conditioned-safe Ceremonies and a User Study of an Application to Web Authentication," *Proc. NDSS '09*, to appear.
13. J. Kilian and E. Petrank "Identity Escrow" *Advances in Cryptology - CRYPTO '98*, Springer LNCS vol. 1462, 1998, pp. 169-185.
14. A. Kerckhoffs, "La Cryptographie Militaire," *Journal des Sciences Militaires*, Vol. IX, 1883, pp. 5-38, 161-191.
15. S.-W. Lo, R.C.-W. Phan and B.-M. Goi, "On the Security of a Popular Web Submission and Review Software," *Proc. WISA '07*, Springer LNCS vol. 4867, 2007, pp. 245-265.
16. R.C.-W. Phan and J.-P. Aumasson, "Next Generation Networks (NGNs): Human-Aided and Privacy-Driven," *Proc. ITU-T Innovations in NGN Kaleidoscope Conference '09*, Geneva, Switzerland, 2008.
17. A. Rabkin, "Personal Knowledge Questions for Fallback Authentication: Security Questions in the Era of Facebook," *Proc. SOUPS '08*, 2008, pp. 13-23.

18. M.A. Sasse, S. Brostoff and D. Weirich, "Transforming the 'Weakest Link': a Human-Computer Interaction Approach to Usable and Effective Security," *BT Technology Journal*, vol. 19, No. 3, 2001, pp. 122-131.
19. S. Schechter, R. Dhamija, A. Ozment and I. Fischer, "Emperor's New Security Indicators: an Evaluation of Website Authentication and the Effect of Role Playing on Usability Studies," *Proc. IEEE S & P '07*, 2007, pp. 51-65.
20. B. Schneier, "Blaming the User is Easy - but it's Better to Bypass Them Altogether," *The Guardian*, 12 March 2009.
21. Securityfocus.com, "Defenses lacking at social network sites," 31 December 2003,
22. S. Vaudenay, "Secure Communications over Insecure Channels based on Short Authenticated Strings," *Advances in Cryptology - CRYPTO '05*, Springer LNCS vol. 3621, 2005, pp. 309-326.
23. S. Vaudenay, "On Privacy Models for RFID," *Advances in Cryptology - ASIACRYPT '08*, Springer LNCS vol. 5350, 2008, pp. 68-87,
24. R. West, "The Psychology of Security: Why do Good Users Make Bad Decisions?," *Communications of the ACM*, Vol. 51, No. 4, 2008, pp. 34-40.
25. Wireless USB Promoter Group, "Wireless USB Specification Revision 1.0," 12 May 2005.