Security issues in the future of social networking

ENISA Position Paper for **W3C Workshop on the Future of Social Networking**

Author: Giles Hogben, ENISA

Introduction

This paper is based on work done by ENISA in compiling its position paper on Security Issues and Recommendations for Online Social Networks (1) and subsequent dissemination work (e.g. (2)) built on the recommendations of this paper. This work was conducted using an expert group of academic and industry experts and used input from a workshop (3). This paper emphasises two key issues for discussion at the workshop:

Access control and authorisation in portable social network formats.

Social Networks are at a crossroads between being monolithic proprietary applications and open applications in the federated identity management space. What does it take to qualify as an identity management system? The following are the main defining characteristics of identity management systems – all of which Social Networks now satisfy:

- Storage of personal data: identity management is about the management of data defining a person's identities. Social Networks certainly satisfy this requirement – like no other IT system on earth. The biggest repository of personal images on the internet is not Flickr but Facebook (already with a staggering 30 billion images, while 14 million new images are uploaded every day). The largest number of personal profiles on the planet is held not in a government identity registry (at least not one we know about...) or one of the much heralded Federated Identity Providers but in the data warehouses of the Social Networking providers.

- Tools for managing personal data and how it is viewed: identity management systems do not just store personal data, they manage it – allowing query, transfer and display of the data in the system. This is one of the main functions of Social Networks. They provide userfriendly tools which allow users to define in considerable detail how their personal profiles are displayed, both in terms of visual layout and the data fields which are displayed. They also provide sophisticated tools for searching (by users) and mining (by advertisers) profile data.

- Access control to personal data based on credentials: this criterion is probably the most important. Any identity management system must give its users control over who accesses which parts of their personal data. Usually this is based on knowing whether the person accessing the data fulfils certain criteria (and has credentials to prove this). For example, a database of medical records might allow access only to users who can prove somehow that they are doctors. Social Networks are increasingly offering this functionality. In social networks, the main boundary protecting a user's data is whether a person attempting to access it has been defined as a friend or is a member of a shared group. Recently, however, Social Networks have added features which allow users to restrict access down to the level of individual friends (or business associates) for each field of their personal profile. In other words, they are now offering very granular access control.

- Tools for finding out who has accessed personal data: most identity management systems provide datatracking tools so users can see who has accessed personal data. This functionality is often not fully implemented in Social Networks because users browsing other people's profiles generally prefer to remain anonymous. It is possible to install profile trackers on some Social Networks however, and many Social Networks provide quite detailed anonymous statistics on accesses to user profiles.

So Social Networks fulfil all the main criteria to qualify as mainstream Identity Management applications but a big difference between Social Networks and state of the art IDM systems until recently has been the openness of their architecture. Federated Identity Management evolved from the experience that keeping personal data in one central location under the control of one large corporate provider is not only a bad idea from a security and scalability point of view but also tends to alienate users who, understandably, perceive such systems as a 'Big Brother'. System architects and users prefer to store their personal data more flexibly and securely.

Until recently, Social Network providers had not faced this issue – which was eclipsed by their huge success in attracting users for other reasons. Social Networking's business model is based primarily on the ability to leverage large warehouses of personal information under their exclusive control. ENISA's position paper (1) already pointed out that the tendency towards a lock-in effect inherent in Social Networking revenue models was detrimental to user privacy and security. Business models which depend on amassing increasing amounts of personal data do not favour any measures which inhibit the viral spread of the Social Network – something which privacy and security measures often tend to do.

ENISA recommended that open formats and standards should be developed to break the data lock-in effect and counterbalance this economic and social pressure. At the time, this recommendation was made as a 'blue sky' ideal, because there appeared to be no economic incentive to provide such open standards – in fact, quite the opposite. Somewhat surprisingly, however, we are now seeing it become a reality. A series of developments in the last year will accelerate this evolution: three of the biggest providers, Facebook, Myspace and Google, have all issued data-portability application programme interfaces (APIs). That is, they allow third parties to integrate a user's social network profile data into external web applications. For example Google's Friend Connect system is based on a triad of open specifications – OpenID, OpenSocial and oAuth, which allow users to display social profile information from members of their network on any web page.

It remains to be seen how much providers will actually allow the export and open transfer of their data stores rather than 'framing' them into pages (where it is still drawn from a central repository) or exposing interfaces only to selected corporate partners, however it seems that this evolution to management tools for personal data will continue apace because:

- Social networking is becoming the preferred (by end-users) way to manage personal data. It is an area where people take an active interest in how their personal information is managed and displayed rather than being passive account-holders as in most identity management systems. Social engagement provides a much-needed incentive for end-users to engage in processes such as setting privacy rules and providing feedback on spammers.
- As previously mentioned, social networks represent the world's largest body of personal data.

Another related trend is that users give away social network account passwords to social aggregators such as (4) in order to simplify management of their various profiles. In the absence of a more fine-grained mechanism for delegating authorisation, they are left with little choice, but this is actually a very dangerous thing to do from a security point of view. We need to see tools for more fine-grained delegation of authorisation to help solve this problem.

In conclusion to this section, three key take-away points arising from this discussion are emphasised:

1. A move to open architectures and data formats for Social Networks is crucial to improving security and privacy since business models based on increasing the user base through viral techniques generally discourage privacy and security whereas open formats create a market for secure and privacy-respecting data storage.
2. In opening up these personal data stores, it is crucial that the confidentiality and privacy of data continue to be respected; i.e., portable access control and privacy rules must be provided along with portable data. Open standards allow users to “leave the Hotel California” but they also need a secure suitcase to take their data with them.
3. Fine-grained authorisation schemes which can delegate access are very important in such open architectures.

Architectures for scalable trust and anonymity using social networks

Identity theft and authentication are fundamental problems in social networking and lie at the root of many of its security problems. There have been proposals to pilot the use of identity cards in Social Networks, but none of them have got off the ground. This could be because people have an instinctive aversion to using ID cards in an area which is supposed to be fun. It could also be because the technology infrastructure simply isn't there yet: ID cards cannot yet be used across border for example and few people have a smart-card reader attached to their computer. Furthermore, such technology does not always protect the people who are most vulnerable: adults often lend payment cards complete with PIN to children and there's currently no way to stop this kind of delegation with ID cards.

A more promising idea is the use of web-of-trust techniques for establishing identity. There are huge amounts of untapped trust data in social networks. Extracting it in a reliable way is a complex problem to solve, but the social network itself (the network of contacts) could be used to for example to establish identity.

End-user metaphors have to be chosen carefully but social networks might actually be a good tool to build up trust in keys which could then be used to identify the user. In such a model, users vouch for the identity of their own network of contacts using a PGP-like model for trust. Most people can tell quite easily if a friend's profile is faked and a large proportion of users also meet in person allowing them to perform a “face-to-face” identity verification. This social identification mechanism is already used for example in the Polish social network, nasza-klasa.pl (5). Users are permitted to publish fake profiles and data but are encouraged to do so transparently by the presence of a mechanism for “reporting” fake profiles. Reporting is not necessarily taken as a negative action - the mechanism allows legitimate uses of fake profiles (e.g. for educational purposes), while exposing malicious fake profiles. As an extension of this idea, we might see social networks being used to build up key trust, which could then be used to export this identity assurance information from the social network and used as an alternative to PKI - for example. Also reputation built up on social networks is an important, and largely unused source of trust information. A typical scenario where this idea is implemented might be as follows:

- Each user is issued a token (eg. public-private keypair) - ideally on joining the social network. They may not necessarily be aware that this is happening as it may be managed entirely by the social network provider until the user wants to export his profile (and trust data). The token is like a social network identity card - it assures the person's name and potentially certain attributes like age,sex and location (ASL).
- Every time user A is accepted as a friend by another user, the token is given a positive or negative trust rating (only once per other user). No user intervention is required to do this or in fact at any point so far. Trust ratings could also be allocated according to a more sophisticated "second order" scheme whereby trust ratings allocated depend on the trust rating of the vouching party.
- If user A suspects that another user B is not who they say they are (in terms of Name + ASL) then you can explicitly state this by signing a revocation certificate and posting it in a directory (the user-experience is similar to that described for Nasza-klasa.pl).
- If user A knows user B personally, user A can go through an explicit "ceremony" as in (6) where user A verifies user B's token and profile together in person and vouches that it is definitely user B's profile and token (this may be understood by analogy with a PGP key signing party). This adds user B's key trust.
- Positive and negative scores (certificates when exported) of the user's token are aggregated to give an identity reputation.
- Anyone can examine the score on a user's token to evaluate whether to believe that they are who they say they are.
- If a user wants to leave a specific social network and go to another one, they can take their token with them as a public-private key-pair and a public key certificate from the provider over the key and personal data and the trust score as electronic signatures of other people over that certificate.
- This could be extended from key identity reputation to other attributes than name, age, sex, location - to e.g. work experience, reliability - i.e. anything one might get a reputation for. This is an extension of the testimonial system seen in existing social networks.
- Voting need not happen by default on agreeing to take someone as a friend but through systems like Compare People (7).
- Attribute reputation could be exported through public key certificates as above.

Using social key-trust to encrypt social data

Such a scheme could also be used as a basis for a smart way of encrypting data in social networks to strengthen privacy so that network members with an adequate trust level in their keys can see the data, but others, including possibly even the service provider cannot. A typical use-case is

- Data from social networks is encrypted using the public key from the basic use-case above. This is used to export the data in a secure way and transport it between social networks. The private key corresponding to the public key is used to decrypt the data.
- Data could even be encrypted when inserted into the Social Network provider's database to provide extra privacy.
- Data in profiles could be encrypted in such a way that only private keys whose public component is signed by the data owner would be able to decrypt the profile data. This provides a what is in effect a portable access control system for social networks.

References

1. **ENISA.** Security Issues and Recommendations for Online Social Networks. [Online] 2007. http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf.

2. Social Networking - Security at The Digital Cocktail Party. [Online] 2008. http://tnc2008.terena.org/core/getfile.php?file_id=307.

3. Next Generation Electronic Identity - eID beyond PKI. [Online] http://www.enisa.europa.eu/pages/eID/eID_ws2007.htm.

4. 20 Ways To Aggregate Your Social Networking Profiles. [Online] http://mashable.com/2007/07/17/social-network-aggregators/.

5. Nasza Klasa (our class) - Polish social networking site. [Online] http://nasza-klasa.pl/.

6. **John Brainard, Ari Juels, Ronald L. Rivest, Michael Szydlo, Moti Yung.** Fourth Factor Authentication: Somebody You Know. [Online] http://www.rsa.com/rsalabs/staff/bios/ajuels/publications/fourth-factor/ccs084-juels.pdf.

7. Compare people (Facebook application). [Online] http://apps.facebook.com/comparepeople/.