SocialKeys: Transparent Cryptography via Key Distribution over Social Networks

Arvind Narayanan

November 5, 2010

This position paper outlines the philosophy, goals, current status and future challenges of SocialKeys, an ongoing project at Stanford. The participants are Narendran Thiagarajan and Dan Boneh in addition to myself.

Most e-mails, instant messages, and other peer-to-peer communications today are not encrypted or authenticated end-to-end. Given that these communications are typically stored in the cloud, they are greatly vulnerable to snooping or interception. Recent events have demonstrated the threat from service providers themselves as well as the governments of various countries.

The failure of PKI. The barriers to deployment of cryptography are not technological; rather, human factors such as identity, trust and usability have been the impediments. A public key infrastructure based on hierarchical certificates has worked well for commerce, but has been rejected by consumers for use in everyday communcations for many reasons.

In a famous experiment, Whitten and Tygar performed a usability analysis of PGP and concluded that it is nearly unusable for the majority.[1] The software has improved in the intervening decade, but the underlying design and architectural issues remain. Fundamentally, a PKI-based system forces users to manually make associations between the identity and the public key *of each user with whom they wish to communicate*.

How SocialKeys works. SocialKeys, by contrast, embraces the idea that public keys must be treated as attributes of the digital identities that people already own and use, i.e., their social network accounts, rather than requiring the creation of new identities for cryptographic purposes.

While this is not a new idea, we go one step further by enabling such an association for existing social networks, even though none of them support such a capability. We achieve this not by relying on a third-party service, but rather by repurposing social network features in unintended ways, in a manner reminiscent of key distribution over DNS.

[1] Alma Whitten and J. D. Tygar. *Why Johnny cant Encrypt: A Usability Evaluation of PGP.* In Proceedings of the 8th USENIX Security Symposium, 1999.

Specifically, we encode the public key as a URL, and use the "websites" attribute of social networking profiles to distribute the key. Since URL-encoded keys start with the prefix `https://socialkeys.org/pubkey`, client software can automatically detect them (the actual functionality of the URL is meaningless). The scheme does not interfere with the user's other activities because an unlimited number of URL fields are typically allowed.

Pros and Cons. SocialKeys offloads the establishment of user identities and trust between users to the social network instead of relying on a key manager. As a consequence, SocialKeys is almost completely transparent to the user the only required user interaction (apart from software installation) is a one-time set-up of a hardened passphrase that is used to generate the key pair; this passphrase needs to be reproduced if the user wishes to enable SocialKeys on a new personal device.

Philosophically, SocialKeys aims for best-effort security and "perfect" usability (in the sense of complete transparency) as opposed to best-effort usability and "perfect" security. The main chink in the SocialKeys armor is the issue of trust in the identities represented by social networking profiles.

In general, social network users gain confidence in their friends' identities by observing their status updates and other activity, through 1-1 communication, and through the transitivity of trust in identities. Nevertheless, this trust can be subverted by social engineering, as the "Robin Sage" experiment shows.[2]

Status and plans. Currently we have implemented key distribution over Facebook as well as an Android "service" that exposes an API that any SocialKeys-aware applications can use. The specification of SocialKeys is general and extensible and it is interoperable with OpenID or another social network.

Work in these areas is ongoing or planned:

- Finalizing the specification and key format
- Support for other social networks
- Extensions for client software such Firefox (to enable secure web mail, including Facebook messages) and Pidgin (to enable secure instant messaging).

Will a radically new approach to adoption of encryption in peer-to-peer communications that emphasizes usability make headway where over 3 decades of the traditional approach has had little success? And if so, will it have sufficiently robust security to be useful? These are the questions we are seeking to answer with SocialKeys.

[2]Thomas Ryan. *Getting in bed with Robin Sage.* Black Hat 2010.