UTILIZING SOCIAL NETWORKING PLATFORMS TO SUPPORT PUBLIC KEY INFRASTRUCTURES

Volker Gruhn, Malte Hülder and Vincent Wolff-Marting
Chair of Applied Telematics, University of Leipzig, Leipzig, Germany

Keywords: Social Networking Platform, Public Key Infrastructure, Web-of-Trust.

Abstract: Although public key infrastructures (PKI) exist for quite a while already, neither hierarchical PKI based on Certification Authorities (CA) nor decentralized webs-of-trust have come to great popularity, particularly not in the private sector. In this paper we want to analyze some reasons for this development and propose possible solutions. The utilization of social networking platforms which have become popular by the so-called ”web 2.0”, may bridge the gap between webs-of-trust and social networks. Thus, the web-of-trust structure may also become more popular and more widely spread due to the better usability this combination provides. For example, key exchange and authentication of the key owners' identities can be supported by extended means of social networking platforms.

1 INTRODUCTION

There are mainly two ways of organizing public key infrastructures (PKI) (Ferguson and Schneier, 2003): In hierarchical organizations (Housley et al., 2002), (Caronni, 2000) the keys are managed centrally and their authenticity is proven by a Certification Authority (CA). As a decentralized management alternative, web-of-trust structures (Zimmermann, 1995), (Eckert, 2004) have been developed, in which users confirm their authenticity to one another. The web-of-trust is based on the function of ”trust” being transitive in some way, i.e. if for example user A trusts in user B, and user B trusts in user C, then user A may also have some trust into user C. Because A does not know C directly, the trust into such an indirect connection decreases with the length of the connection (Maurer, 1996a).

During the last years we have seen, that PKI develop only in a rather hesitant way. We see different reasons for this inert development: Hierarchical PKI are quite expensive. Due to the amount of data that has to be managed by CAs, investments and costs for extremely reliable technology and the protection of data privacy are quite high. Decentralized web-of-trust structures are based on some kind of peer to peer principle, and thus are cheaper to realize, but availability and protection of data privacy is left to the users. Moreover, both approaches suffer from intricateness and bad usability that is brought about by their consequent use. For example, for both of the two most popular e-mail clients Microsoft Outlook and Mozilla Thunderbird, separate programs need to be installed to be able to use the OpenPGP web-of-trust (Callas et al., 1998).

Although the high costs are a good argument for hierarchical PKI not being accepted in the private sector, this argument does not hold for decentralized structures. In the following section we will look into the shortcomings that prevent private users from applying web-of-trust infrastructures and how they can be overcome. In particular we will examine the chances that arise from social networks and the so-called ”Web 2.0”.

2 SHORTCOMINGS OF CURRENT APPROACHES

If the function of ”trust” is transitive as assumed above, a rather close meshed web-of-trust should

Gruhn V., Hülder M. and Wolff-Marting V. (2007).
UTILIZING SOCIAL NETWORKING PLATFORMS TO SUPPORT PUBLIC KEY INFRASTRUCTURES.
In *Proceedings of the Second International Conference on Security and Cryptography*, pages 245-250
DOI: 10.5220/0002125902450250

emerge quite soon, because almost everyone has a number of people they trust in and each of them should have a partly disjunct group of trusted people. Already in 1967 Milgram (Milgram, 1967) reckoned, that any man knows any other by at most 6 links. In 2003 this hypothesis was confirmed – at least for the users of electronic media like e-mail (Watts, 2003). Hence the path of trust from one person to another should also have an average of only six nodes. But why are the existing webs-of-trust more like islands rather than a worldwide network (Guardiola et al., 2002)?

One reason for this phenomenon may be that the meaning of ”trust” is not clear to many users. On one hand this means to verify the authenticity of an acquaintance, but on the other hand it also means to trust that person to confirm the authenticity of its own contacts accordingly. As soon as the trust into the contact's diligence is unclear, the transitivity of the function of trust does not hold anymore.

Other reasons lay in the cumbersome handling of current PKI implementations. Although in the meantime extensions for most of the established e-mail programs exist, a lot of them are not equipped with these extensions at delivery. Because of this, users of PKI have to explain, why they append their e-mails by some cryptical mass of data. Therefore, users often do not send signed e-mails to users of whom they do not know whether they use PKI themselves. The not-knowing about the existence of PKI applications even between direct contacts, is one reason for our procedure.

Key exchange is also complicated: When two users have verified their identity and the identity of their keys, they can sign the inspected key with their own key in order to show the mutual trust. Such a signed key should be published again, in order for a third person being able to judge the trustworthiness of an unknown key by checking its signatures and evaluating their trustworthiness. Here once more, bad usability tests user acceptance: For the verification, the keys and their fingerprints have to be available, the keys have to be signed and republished afterwards.

3 UTILIZING SOCIAL NETWORKS TO SUPPORT A RELIABLE DISTRIBUTION OF PUBLIC KEYS

In the recent years social network platforms in the world wide web grew rapidly. Based on Milgrams small world theory (Milgram, 1967) some of them connect people with similar interests or taste (e.g. Yahoo! Inc., 2007; Last.fm Ltd., 2007) while others mainly reproduce real world circles of acquaintances (e.g. MySpace.com, 2007; Zuckerberg, 2007; OPEN Business Club AG, 2007).

Especially the latter ones trace a form of interpersonal relationships that implies a certain level of knowledge and trust between the network's members like it is assumed to exist within a web-of-trust. Social network platforms that connect members on the base of interest will probably not provide this property. Therefore in the rest of this paper ”social network” denotes only networks with a real world representation. They can be utilized for a public key management in different ways that can build upon each other:

1. Social network platforms can act as key servers and provide services similar to existing web-of-trust servers (e.g. Kuethe and Laager, 2007).
2. They can actively support mutual key signing.
3. They can offer additional support supplementary to public key management.

The benefit of these options will be discussed in the following subsections.

3.1 Key Management

The most elementary way of supporting key management is to include public keys like other contact details – platform users can upload their own keys and download other people's keys. Compared to existing key servers (e.g. Kuethe and Laager, 2007) this provides mainly additional comfort. Searching and identifying keys and key holders is more convenient as network platforms generally contain more personal information than traditional key servers do. Further more, easy usage and the current general popularity of social network platforms might help to arouse public interest in electronic signatures as a collateral benefit.

As the author of a key will not be authenticated soundly by the platform when uploading a key, no assertion on the originality of the key can be made to begin with. Unlike traditional key servers, social networks are actively used for communication and thereby do provide an additional way of multilateral authentication. While it is simple to create a bogus account, it might be a serious obstacle to build up and maintain a network with this account, which is compatible to the real world network of the impersonated victim. Regular interaction via the platform, especially in the context with real world activities – e.g. appointments – can provide basic trustability in an account. Some of that trust might be transferred

to public keys escrowed with the account – especially if the keys have not been changed for a longer time. But this does only apply for first-grade contacts: such an indirect trust can not be regarded transitive. Moreover, no protection against sophisticated attacks like man-in-the-middle or account hijacking (Ferguson and Schneier, 2003) is provided. Subsuming, placing trust in a key that has not been verified by any other means has to be discouraged.

3.2 Supporting Authentication and Key Signing

To improve the web-of-trust-character of a virtual social network explicitly, the implementation of a user-authentication- and key-signing-protocol is required. Two competing key-signing-concepts exist: the web-of-trust (Caronni, 2000) and the hierarchic approach (Housley et al., 2002) often also referred to as public-key-infrastructure (PKI). In a web-of-trust, users sign their keys mutually, while in a PKI all signing is done by few centralized entities. Traditionally, key signing in a web-of-trust is a process that requires several user interactions. The user has to obtain the key, verify the key using a secure channel of communication, sign the key and afterwards publish the new signature. The signature covering a key and possibly additional attributes is also called ”certificate”.

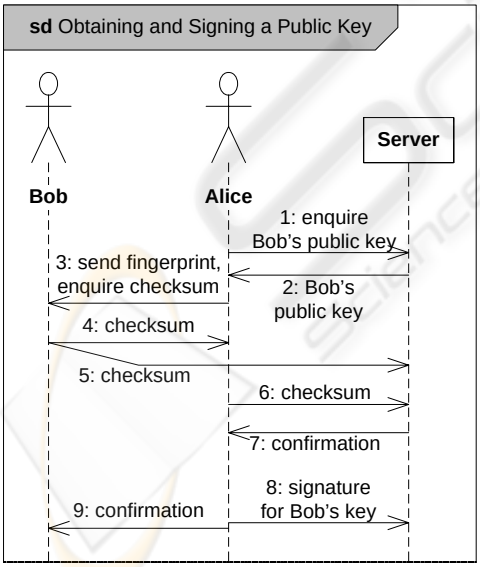

Figure 1: UML Sequence-Diagram: Obtaining and Signing a Public Key.

Figure 1 outlines a possible sequence of key-verification and -signing. The sequence requires direct communication between the users (steps 3, 4 and 9). This communication should never be conducted via the facilities of the social network but via an independent communication channel. A phone call would be advisable as the sound of the voice and accompanying idle conversation can provide a quite reliable authentication between acquaintances. A meeting in person probably provides the highest protection against fraudulent impersonation (”identity theft”) while e-mail, instant communication and other digital channels will not. Depending on targeted dependability, a platform's policy might prescribe or forbid certain communication channels for that purpose – the platform might as well register the channel with the signatures in step 8 and use that piece of information to weight the signatures in trust calculations. The OpenPGP message format defines different ”signature types” to reflect different diligence in the owner verification (Callas et al., 1998, Section 5.2.1.).

The checksum used in the steps 4-6 should be uniquely calculated for each recipient, it should not be confused with the fingerprint traditionally used for key verification. A unique checksum enforces the direct communication and thereby the implicit authentication of the key-owner: a random value might be sufficient. With a traditional fingerprint that can easily be calculated by anyone, the direct communication might be bypassed. The server should not accept signatures (step 8) unless it received the corresponding checksums (steps 5,6). This narrows the danger of providing a fake context for a previously injected fake key. An exception has to be made for the key holder. He will probably not accept to re-negotiate signatures made using other platforms or ways. It might be useful to distinguish between signatures made using this social network platform and other signatures. The latter might be excluded from trust calculations for example. A generic fingerprint however should be send with the inquiry in step 3 to ensure that the key transmitted in the previous step is sound.

Generally, in this environment all communication with the server should be encrypted and authenticated. As current platforms depend on the Hypertext Transfer Protocol, Transport Layer Security (TLS) (Rescorla, 2000; Dierks and Rescorla, 2006) will be a solid choice. The message of step 5 should be signed with the key in question to prevent man-in-the-middle attacks; if step 4 is conducted electronically, it should be signed as well. To increase user acceptance, the protocol should be conducted as automated as possible.

If a hierarchic approach is preferred, instead of accepting signatures in step 8, a certificate for the key can be generated and signed by the server as soon as

a certain number of verifications have been reported to the server (similar to (CAcert Inc., 2007; Thawte Inc., 2007)).

In certain situations a key signature, respectively certificate, might have to be invalidated. OpenPGP and X.509 provide mechanisms to revoke certificates and key signatures (Callas et al., 1998; Housley et al., 2002). The revocation of a certificate is a permanent measure that prohibits any further use of the certificate. It is primarily provided for cases of accidentally disclosure of the private key and for wrongly issued certificates. In a web-of-trust, a public key can be revoked with the matching private key and with previously authorized revocation keys. Certificates respectively can be revoked by the key they have been issued with or any revocation key previously authorized for that key. In a hierarchy, revocation is done by the certification authority. A social network platform needs to provide key signers and holders with the ability to upload revocation signatures in a web-of-trust environment, and a protocol to revoke certificates in response to complaints in a hierarchic environment. Besides that, users might want to explicitly distrust some other users for personal reasons that however do not legitimate a revocation – for example because they suspect those users to be unable or unwilling to execute the authentication protocol correctly and instead issue untested certificates. Various authors have analyzed this topic and provide trust calculation frameworks that do incorporate the concept of distrust (Marsh, 1994; Golbeck et al., 2003; Richardson et al., 2003; Guha et al., 2004). A social network platform providing trust calculations should regard this aspect as well.

3.3 Advanced Support for Key Management

An important feature of webs-of-trust is the ability to place trust in unfamiliar signatures based on a trust path (Caronni, 2000). But at the time of this publication, there seems to be no user-friendly way to discover such a path, only experimental approaches exist (McDowell, 2005; ”Darxus”, 2002). Virtual social network platforms, however, provide features to find links to other network members. Finding a trust path within the network and calculation of trust can be offered as well, if public key information is integrated into the platform.

Furthermore the platform can identify gaps in the web-of-trust and encourage users to close them. Figure 2 illustrates a simple social network containing a web-of-trust. The connecting lines denote acquaintanceship, the arrows point from a key signer to a key

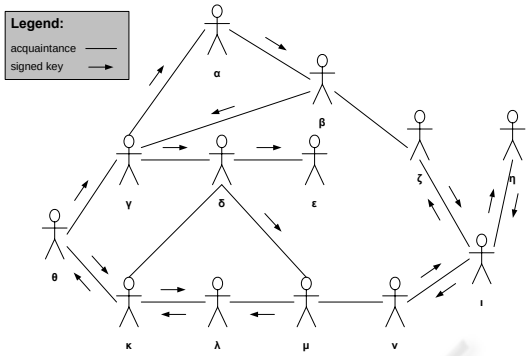

Figure 2: A Web-of-Trust in a Social Network.

holder. While the network is strongly connected, the web-of-trust is not. To connect both components the platform can suggest β and ζ or μ and ν to mutually sign keys. Moreover there exist some bridges which are edges that disconnect the web-of-trust if removed. δ and κ should be invited to sign their keys as well as most of the unilateral connections. For practical reasons, the users should be encouraged to always sign their keys mutually. Graph theory will help to identify critical edges in a realistic (i.e. far more complex) environment.

Users might consider to bind their keys to their virtual social network account and vis-a-vis. This might be meaningful to clarify that the specific key is supposed to be used in the context of the social network. Without such a link, an impersonator might simply ad his victim's real public key to a bogus account. That will neither allow him to sign messages nor to decrypt messages with the key pair in question notwithstanding it might lure others to place trust in the bogus account. An OpenPGP key can be linked to a social network account by adding and self-signing a ”User ID Package”. The convention suggests to format the user ID as an RFC 822 mail name (Callas et al., 1998), any other UTF-8 string is allowed as well. To find a suitable naming convention for any social network should not be a difficult problem.

A X.509 certificate should be linked to the account via the ”SubjectAltName” entry. Various formats are allowed here including e-mail addresses and uniform resource identifiers (Housley et al., 2002). Alternatively the ”Subject”-field can be used, but that would require the usage of an ”X.500 distinguished name” (see ITU-T, 2005), which might not conveniently fit to the social network's existing naming conventions. Since the X.509 certificates described in this paper would be exclusively issued by the social network platform, a link to the account seems to be mandatory.

4 RELATED WORK

In (Khan and Shaikh, 2006) a relationship algebra is proposed, that allows a general mapping of social relationship networks into the generic relationship algebra. It also allows defining a set of constraints, which may be utilized to answer certain questions that can be processed by algebraic operations. (Khan and Shaikh, 2006) provide two examples: one of them is the reviewer selection for a scientific conference or journal, another one a vaccination and immunization example. However, this approach may be extended to trust in social relationship networks as well.

(Ries et al., 2006) provide a survey of trust systems. As each of the proposed approaches provide their own trust model, it is difficult to compare them. However, (Ries et al., 2006) name a set of criteria that allows analysing different systems dealing with trust, and come to the conclusion that a certain degree of uncertainty or confidence has to be modelled, in order for such a system to be useful in virtual social networks.

Marsh (Marsh, 1994) provides a comprehensive discussion of the notion of trust. He also shows that trust is not transitive over arbitrary long chains, as this would end in conflicts regarding distrust. However, as we expect the chains in social relationship networks to be rather short, the transitivity of trust can be assumed to a certain degree.

(Golbeck et al., 2003) provide an algorithm for trust calculations in social networks as a proof-of-concept. They propose to use it to classify creditability of resources in a semantic web such as documents and messages. They specially emphasis on the difference between knowing the origin of a resource and trusting its content. The algorithms also consider distrust explicitly. (Richardson et al., 2003) follow a rather similar approach. They specially accentuate that trust calculations will lead to different results depending on the start node, i.e. the user whom the trust is calculated for. Both papers do not mention virtual social network platforms explicitly that were just emerging at the time of their publication, but the algorithms are suitable in this environment as well. Further research on the concept of distrust has been done by (Guha et al., 2004).

Maurer (Maurer, 1996a) also states that confidence values have to be measured on a scale rather than being 0 or 1. He proposes the scale between 0 and 1, so that the values may be interpreted as probabilities. He then describes how the confidence over a path of recommendations may be calculated. Concluding that trust fades rather quickly over a path of recommendations, he suggest that a reasonable system should only work with rather short paths. In (Maurer, 1996b) Maurer provides comprehensive calculations to cheating probabilities for a one-way message authentication. It might be interesting to extend these calculations to a web-of-trust environment to compare the probabilities.

(Guardiola et al., 2002) did some research with the PGP web-of-trust. They showed that it is rather a set of strongly-connected clusters than a connected graph and found it robust against intentional attacks.

(Datta et al., 2003) introduce a "quorum based decentralized PKI" as an alternative to the web-of-trust. It bases on a massive redundant key storage in a peer-to-peer network. That approach is rather focused on the authentication of accounts. It provides no link between persons and accounts. Existing acquaintance and trust relations between persons are not taken into consideration.

5 CONCLUSION

In the previous chapters it has been shown, how virtual social network platforms can help to overcome shortcomings of existing public key distribution infrastructures. A simple protocol for mutual authentication and key signing for members of such a network has been introduced. Instead of inventing new technological solutions, improvements in usability and automated support are proposed. The solution is fully compatible and can coexist with existing key distribution and authentication structures. A web-of-trust can even span multiple independent, even competing network platforms.

This paper mainly focuses on key exchange and trust between individuals. Within large organizations and companies, a hierarchic approach seems to be more appropriate than a web-of-trust, as the web-of-trust would react rather slowly on entries to and exits from the organization. A virtual social network platform will not add any features to existing authentication schemes within organizations. Small and medium-sized companies might however utilize the means described in this paper and provided by network platforms as this might be easier and less expensive than implementing an own public key infrastructure.

Communication between members of different organizations can be secured via social network platform regardless of each organization's size as a short cut, whenever no simpler means of authentication of the communicating people exists, such as mutual signing of root certificates.

ACKNOWLEDGEMENTS

The Chair of Applied Telematics/e-Business is endowed by Deutsche Telekom AG.

REFERENCES

CAcert Inc. (2007). CAcert. http://www.cacert.org/.

Callas, J., Donnerhacke, L., Finney, H., and Thayer, R. (1998). *OpenPGP Message Format. RFC 2440.*

Caronni, G. (2000). Walking the web of trust. volume 00, page 153, Los Alamitos, CA, USA. IEEE Computer Society.

"Darxus" (2002). GPG/PGP signature path tracing. http://www.chaosreigns.com/code/sigtrace/.

Datta, A., Hauswirth, M., and Aberer, K. (2003). Beyond "web of trust": Enabling p2p e-commerce. *Proceedings of the IEEE International Conference on E-Commerce*, pages 303–313.

Dierks, T. and Rescorla, E., editors (2006). *The Transport Layer Security (TLS) Protocol Version 1.1. RFC 4346.*

Eckert, C. (2004). *IT-Sicherheit*. Oldenbourg Verlag, 3. edition.

Ferguson, N. and Schneier, B. (2003). *Practical Cryptography*. Wiley.

Golbeck, J., Parsia, B., and Hendler, J. (2003). *Cooperative Information Agents VII*, volume 2782 of *Lecture Notes in Computer Science*, chapter Trust Networks on the Semantic Web, pages 238–249. Springer, Berlin, Heidelberg.

Guardiola, X., Guimera, R., Arenas, A., Diaz-Guilera, A., Streib, D., and Amaral, L. A. N. (2002). Macro- and micro-structure of trust networks. *ArXiv Condensed Matter e-prints*.

Guha, R., Kumar, R., Raghavan, P., and Tomkins, A. (2004). Propagation of trust and distrust. In *WWW '04: Proceedings of the 13th international conference on World Wide Web*, pages 403–412, New York, NY, USA. ACM Press.

Housley, R., Polk, W., Ford, W., and Solo, D. (2002). *Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile. RFC 3280.*

ITU-T (2005). Recommendation X.500, "The Directory: Overview of Concepts, Models and Service".

Khan, J. I. and Shaikh, S. (2006). Relationship algebra for computing in social networks and social network based applications. *Proceedings of the 2006 IEEE/WIC/ACM International Conference on Web Intelligence (WI'06)*.

Kuethe, C. and Laager, R. (2007). OpenPGP public key server. http://pks.sourceforge.net.

Last.fm Ltd. (2007). Last.fm. http://last.fm.

Marsh, S. P. (1994). *Formalising Trust as a Computational Concept*. PhD-Thesis, Department of Computing Science and Mathematics. University of Stirling.

Maurer, U. (1996a). Modelling a public-key infrastructure. In *ESORICS'96*.

Maurer, U. (1996b). A unified and generalized treatment of authentication theory. In *STACS: Annual Symposium on Theoretical Aspects of Computer Science*, volume 1046 of *LNCS*, pages 387–398.

McDowell, J. (2005). Experimental PGP key path finder. http://the.earth.li/~noodles/pathfind.html.

Milgram, S. (1967). The small world problem. *Psychology Today*, 2:60–67.

MySpace.com (2007). Myspace. http://www.myspace.com.

OPEN Business Club AG (2007). Xing. http://www.xing.com.

Rescorla, E. (2000). *HTTP Over TLS. RFC 2818.*

Richardson, M., Agrawal, R., and Domingos, P. (2003). *The SemanticWeb - ISWC 2003*, volume 2870 of *Lecture Notes in Computer Science*, chapter Trust Management for the Semantic Web, pages 351–368. Springer, Berlin / Heidelberg.

Ries, S., Kangasharju, J., and Mhlhuser, M. (2006). A classification of trust systems. In Meersman, R., Tari, Z., Herrero, P., et al., editors, *OTM Workshops 2006*, LNCS 4277, pages 894–903. Springer-Verlag Berlin Heidelberg.

Thawte Inc. (2007). Thawte. http://www.thawte.com/secure-email/web-of-trust-wot/index.html.

Watts, D. J. (2003). *Six degrees: The Science of a Connected Age*. Norton.

Yahoo! Inc. (2007). Flickr. http://www.flickr.com.

Zimmermann, P. R. (1995). *The Official PGP Users Guide*. MIT Press, Boston, Massachusetts, U.S.A.

Zuckerberg, M. (2007). Facebook. http://www.facebook.com.