Design of an Anonymous Instant Messaging Service

Gábor György Gulyás
Dept. of Telecommunications
Budapest University of Technology and Economics
H-1117 Budapest, XI. Magyar tudósok körútja 2. Room: I.B.113.
gulyasg@hit.bme.hu

Abstract

Instant messaging is in its renaissance; there are hundreds of millions of users worldwide. However, as we are using these services at home and work, and even on the way between, several privacy issues arise. In this paper I formalize requirements for privacy friendly messaging services and propose a novel anonymous instant messaging service that fulfils these requirements and allows anonymity as well. The suggested solution applies the technique called Role-Based Privacy by organizing profiles in a tree hierarchy. I also provide the analysis of total anonymity and unlinkable pseudonymity in the service and highlight interesting research objectives for extending the model presented in the paper.

1 Introduction

Today, in the digital age the Internet is getting more integrated with everyday life and so do social services including Instant Messaging (IM). Age-groups ranging from teenagers to adults use these kinds of services in their everyday life at multiple locations including work, home or even use mobile messaging software while being on the move.

The authors in [SP04] interviewed several subjects and mention several privacy related issues regarding IM services: privacy from non-contacts, privacy regarding availability, and privacy of the communication. However, these problems are generic and concerning communication committed in chat services as well (previous work in [GG06]).

In this paper I propose a messaging service model that allows anonymity. The model has both the characteristics of instant messaging and the chat services: should have a contact list and allow conferences (instant messaging) and rooms that may be explored separately (difference between conferences and rooms are conferred later). For achieving anonymity and enhanced privacy settings on visibility I propose Role-Based Privacy (RBP) [RL08].

2 Requirements

The motivation of this work is to propose a privacy enhancing messaging service. The goals that such a service should accomplish are enlisted below and based on the proposal of [SP04] but refined and derived from previous work in [GG06]:

- user privacy should be protected from non-contacts by flexible protection options
- privacy should be strengthened regarding availability
- anonymity should be achievable in some contexts
- in other contexts unlinkable pseudonymity should be available for managing multiple personae
- the privacy of communication should be protected on the network
- flexible and coherent privacy settings should help users

The threat model assumed by this paper is simple: service and service level operator users are trusted (in future work this assumption may be revised), and regular users are not. Hence, user privacy should be primarily protected against other users.

3 Anonymous Messaging Service

There are different aspects and architectures for messaging services. However, due to the nature of instant messaging and chat services I propose the use of a centralized service (harmonizing with the concept of a trusted service), but different architecture types may also be applicable. For the other requirements enlisted in the previous section I propose the use of identity management based on the technique of Role-Based Privacy (see Section 3.2).

3.1 Network Architecture

For achieving anonymity user privacy should be strengthened separately on the network and application level as well. Besides protecting the confidentiality, integrity of network level communication application level protocols, such as identity management should be designed with privacy in mind (this concept is presented in previous work for the web in [GG08]).

For achieving network level anonymity an anonymizing service should be used, however, as the architecture is centralized, a MIX type service should be used to access the central servers [DC81], such as TOR, JAP or I2P[1]. Peer-to-peer connections (for file transfers, private conversations, etc.) may be anonymized or protected by other means, such as traffic analysis protected Transport Layer Security (TLS) channels.

3.2 Identity Management with Role-Based Privacy

Role-based profile management is the core concern of the service. In everyday life we share information with others according to the transactions we commit (e.g. shopping in the grocery), the role we play (e.g. co-worker, a chess club or a family member), or we conform to other criteria. If necessary these roles could be represented with unlinkability, meaning other participants are unable to link profiles realizing different roles. This concept should be implemented in messaging services to offer enhanced features on availability and anonymity as well.

Accordingly, I suggest that in services model the user should be able to manage her identities by setting up different profiles for different places, such as rooms, conferences. Profiles are structured data sets including many kinds of descriptive information on the identity such as screen name, contact information, status (visible, unavailable, busy, etc.), and in some cases a globally unique identifier that was selected during the registration process.

The most prominent difference between conferences and rooms is how users identify themselves: with their globally unique pseudonym in conferences, and with locally unique identifiers within rooms for allowing anonymity. In the latter case anonymity is possible (unlinkable pseudonymity) as profiles may be changed any time without the presence of any trivially linkable information (such as identifiers). However, identity changes should be carried out carefully (e.g. no messages or timings should also indicate the link between profiles). In rooms total anonymity (no identifiers) should also be an option.

There should be other ways for contacting other users, like dialogues and contact lists (also called buddy lists in some IM services). A dialogue should be represented as a conference; however, global identifiers may not be revealed as it may not be known. Contact lists would be useless without global identifiers; therefore contacts (ordered in contact groups) should be identified under any circumstances.

For providing flexible and easily perspicuous identity management a profile hierarchy should be used: profiles should be ordered within a tree-like hierarchy for providing inheritance of profiles. Unset profiles should inherit their settings from the nearest ancestor that is set. The concept of using a profile hierarchy is similar to the concept introduced by the authors in [MH08] on how pseudonyms should be used

[1] http://www.torproject.org, http://www.i2p2.de, http://anon.inf.tu-dresden.de/index_en.html

for managing linkability. The lower profiles are set with the more distinct values the higher unlinkability is achieved against other users.

However, total unlinkability of profiles is only achievable in rooms where no global identifiers are attached. In other contexts only separable visibility may be achieved, which is also an important privacy protecting feature [SP04]. The profile hierarchy is illustrated on Figure 1.

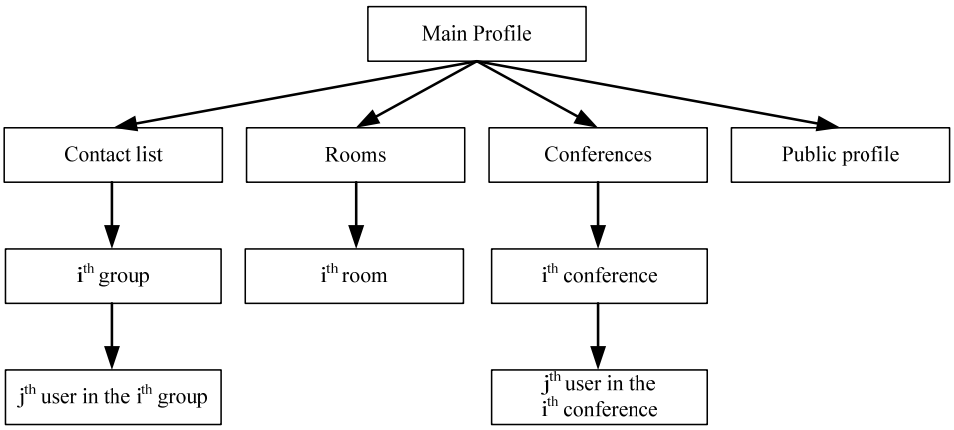

Figure 1. Profile hierarchy.

I elaborate the usage of profile hierarchy with a simple example. For instance a user is known as 'John Doe' within all rooms. However, he joins the room called 'Flea Market' with an alias 'Bob'. Since other users only see these information these identities may not be linked, although the user may remove the profile set for the flea market any time to reveal a higher level profile know as 'John Doe'. In conferences the pseudonym acquired would also be visible in the profile providing linkability.

In messaging services today similar operations are used as below for managing privacy; however, the proposed operations are sound with the RBP model presented and defined to manage profiles in the hierarchy by realizing privacy and status settings at the selected node of the profile hierarchy:

- *Ignore* (⇔ *enable*): an ignored user (identity) will see the ignorer user's profile, however, will not be able to send messages to her.
- *Ban* (⇔ *enable*): similar to the ignore operation, but the banned user sees the banner's offline profile (or which is for unknown users). Banning would allow hidden surveillance in rooms, thus it should not be allowed (allowing anonymous reading would realize the same effect).
- *Identity change* ⇔ *reveal identity*: in rooms this operation means an identity change (introducing unlinkable identities), in other places it is a simple profile changing operation.

The need for privacy protection against non contact users should be handled by introducing anonymous credentials [JC01]. For instance malicious actions need to be

stored in a special passport which is only accessible for the service, but users may declare restriction towards it.

For instance if the service detects that a user sent a SPAM message, it increases the SPAM counter in the passport, or a service operator should be able to add tags to it (e.g. "virus" indicating that the user's computer was infected with some kind of a virus). These entries can not be accessed by other users, but should be able to define constraints for specific actions regarding these settings, such as limiting the access to their public profile for user without spamming activities.

3.3 Further Privacy-Related Enhancements

Profile management settings need to be harmonized with privacy protection to provide a better protection against distraction caused by alerts. For instance at work contacts in the friends group should not be able to distract the user, however, events originated by contacts in the co-workers group should alert the user. This feature provides a better and more flexible privacy protection.

Further properties may be introduced for the rooms and conferences to strengthen privacy (and for other contact places also), such as limitations (file transfer, file size, message per sec, etc.), password or key requirements, proper credentials required for join, anonymous comments. In rooms anonymous observation should also be an option.

Another possible extension would be enabling modular event sources, such as a user defined time-table for modifying profile settings, or adding location based modules (based on WiFi Access Point information or GPS location). By using these modules the user may disable co-workers after 17h, or only allow access to her office profile while she is in the company's building.

4 Analysis of the Anonymous Messaging Service Model

The anonymity criteria presented in [GG08] can be adapted to the conferred messaging scenario, in which anonymity is still a core concern, but additionally the unlinkability of identities is another one, and should be treated equally to anonymity: introducing unlinkable profiles allows a different level of anonymity (unlinkability is regarded against other users).

As the presented service model relies on a network level anonymizer (which eliminates threats regarding the privacy of the communication) only users within the service should be considered as potential attackers. Requirements regarding availability issues, anonymity and unlinkable pseudonymity are achieved by RBP within rooms, conferences and contact lists.

In conferences and on the contact list anonymity is not an option, although the proposed technique provides flexible and easily manageable privacy protection by allowing proper profile management. These parts of the service provide pseudonymous identification instead of anonymity (this may be recognized as a certain level of anonymity). Anonymity achieved in rooms by introducing unlinkable identities is always possible and total anonymity may also be enabled.

In some contexts the presence of too few individuals may reduce the chance of unlinkability. Hence, allowing the presence of some bots in the room may also help, especially if it is possible for the user to take over the control on one of them. The bot should be exiting when the user does, for avoiding confusing situations (e.g. two different users take over the same bot within an uninterrupted session).

5 Conclusion and Future Work

The proposed technique, Role-Based Privacy, is a possible solution for offering better privacy management and anonymity if implemented properly. In my opinion the suggestions presented in this paper should be generalized furthermore and extended for services based on social networks (some privacy vulnerabilities addressed in [MC08]), which are getting more and more widespread. Related work to this topic has already been submitted and accepted [GG09]. Further analysis of anonymity is also a research objective in the future within the generalized RBP model for social networking services; for instance examining analytically the unlinkability of separated identities is an interesting problem.

6 Acknowledgements

I wish to thank my supervisors, Dr. Sándor Imre and Róbert Schulcz, for supervising and supporting my research, and for funding my travel expenses.

This paper was made in the frame of Mobile Innovation Centre's integrated project Nr. 2.3 supported by the National Office for Research and Technology (Mobile 01/2004 contract).

7 References

[DC81] D. Chaum, “Untraceable electronic mail, return addresses, and digital pseudonyms”, The Communications of the ACM 24, February, 1981, pp. 84-88.

[GG06] G. Gulyás, “Analysis of anonymity and privacy in instant messaging and chat services”, In: Dr. Ferenc Kiss (ed.), Tanulmányok az információ- és tudásfolya-

matokról 11. (Alma Mater Series), pp. 137-157., BME GTK ITM, October 2006. ISSN: 1587-2386, ISBN: 963-421-429-0. (in Hungarian)
Online: http://pet-portal.eu/files/articles/2006/10/im_privacy.pdf

[GG08] G. Gulyás, R. Schulcz, and S. Imre, “Comprehensive Analysis of Web Privacy and Anonymous Web Browsers: Are Next Generation Services Based on Collaborative Filtering?”, Joint SPACE and TIME International Workshops 2008, Trondheim, Norway, 17/06/2008.

[GG09] G. Gulyás, R. Schulcz, and S. Imre, “Modeling Role-Based Privacy in Social Networking Services”, SECURWARE 2009, Athens, Greece, 18-23/06/2009. (accepted)

[JC01] J. Camenisch, A. Lysyanskaya, “An Efficient System for Non-transferable Anonymous credentials with Optional Anonymity Revocation”, In the Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques (EUROCRYPT '01), London, UK, 2001, pages 93-118.

[MC08] M. Chew, D. Balfanz, and B. Laurie, “(Under)mining Privacy in Social Networks”, W2SP 2008, Oakland, California, USA, 22/05/2008.

[MH08] M. Hansen, A. Schwartz, and A. Cooper, "Privacy and Identity Management", IEEE Security and Privacy, vol. 6, no. 2, Mar/Apr, 2008, pp. 38-45.

[RL08] R. Leenes, J. Schallaböck, and M. Hansen, “PRIME white paper (V3)”, 15/05/2008.

[SP04] S. Patil, A. Kobsa, “Instant Messaging and Privacy”, In Proceedings of HCI 2004, Leeds, U.K., pp. 85-88.