A privacy-aware model for communications management in the IP multimedia subsystem

J. Ophoff
R. A. Botha

A Privacy-Aware Model for Communications Management in the IP Multimedia Subsystem

J.Ophoff[1] and R.A.Botha[2]

[1]Centre for Information Technology and National Development in Africa (CITANDA), Dept. of Information Systems, University of Cape Town, South Africa
[2]School of ICT, Nelson Mandela Metropolitan University, South Africa
e-mail: jacques.ophoff@uct.ac.za; ReinhardtA.Botha@nmmu.ac.za

Abstract

Never before have people been so connected to one another. Today we have the ability to communicate with almost anyone, anytime, anywhere. Our increased connectivity and reachability also leads to new issues and challenges that we need to deal with. When we phone someone we expect an instant connection, and when this does not occur it can be frustrating. On the other hand it is equally disruptive to receive a call when one is busy with an important task or in a situation where communication is inappropriate. Social protocol dictates that we try to minimize such situations for the benefit of others nearby and for ourselves.

This management of communications is a constant and difficult task. Using presence – which signals a person's availability and willingness to communicate – is a solution to this problem. Such information can benefit communication partners by increasing the likelihood of a successful connection and decreasing disruptions. This paper addresses the problem of staying connected while keeping control over mobile communications.

The paper presents a model for privacy-aware communications management, extended to the IP Multimedia Subsystem (IMS). The model stresses the privacy of potentially sensitive presence information. A unique perspective based on social relationship theories is adopted. The use of relationship groups not only makes logical sense but also assists in the management of presence information and extends existing standards. Thus the model presents a solid foundation for the development of future services. In these ways the proposed model contributes positively towards balancing efficient mobile communications with the need for privacy-awareness.

Keywords

IP Multimedia Subsystem, Communications management, Privacy

1. Introduction

Without control mobile communications risk becoming disruptive and disorganizing (Rennecker and Godwin, 2005). These consequences can be far-reaching. Ling (2004) states that many people find mobile phones disturbing, and there are numerous situations where the use of mobile phones are seen as inappropriate.

According to Ling (2004, pp. 125–142) there are three general domains in which mobile communications can cause disruption: public settings with extensive norms governing behaviour (such as restaurants), interpersonal interactions and on an

individual, internal level. It is clear that the disruption caused by an incoming communication affects the recipient, people in the immediate vicinity, and also changes the social status and behaviour patterns.

The problem of disruptions is extremely relevant when we frame it against the current state of information overload. Having to deal with a multitude of facts and tasks as efficiently as possible has meant that our attention has become scarce – put another way we are trading in the economics of attention (Davenport and Beck, 2000). Operating in this environment requires us to manage our attention, and correspondingly our communications, as efficiently as possible if we want to lead a productive life.

In the face of these challenges people often reconsider their perception of acceptable use and adopt a more tolerant attitude (Palen et al., 2000; Love and Perry, 2004). Research suggests that a range of dynamic factors influence our communications: the communications medium, relationship between caller and receiver, status differences, affinity towards a contact, expectations of reciprocity and culture all play a role (Rennecker and Godwin, 2005). Perhaps this explains why an effective solution to this problem is yet to be found.

While the convergence of communication channels with the Internet is delivering richer communication experiences no standards exist to communicate context between the caller and receiver. 'Call manager' mobile applications allow a degree of rule-based control over communications and enable users to pull social networking data about a caller, but are not based on standards and are reliant on interfaces to third-party websites. Thus the Caller ID feature is still the only reliable context indication and is only available to the receiver. However, it is often unavailable because it can be switched off by the caller. Centralised analysis and management of a wide variety of context data is needed to overcome these problems (Baladrón et al., 2012).

In mobile communications a fundamental conflict exists between the desire for availability and the wish to maintain a high level of control over communication and personal privacy. Parties need a way to balance availability, interruptions leading to disruption as well as privacy requirements. This balance needs to be addressed on a technological and social level. The objective of this paper is the development of a prescriptive model for controlling disruptions in mobile communications using established presence standards in the IMS.

The paper proceeds with an overview of privacy concerns related to mobile communications, focusing on the sharing of context information. Thereafter, in Section 3, social relationships are examined as a contributing factor to our perception of privacy. Following this Section 4 presents and discusses a model for communications management in the IMS taking the previous points into consideration. A key aspect of the model is the use of presence as a service. Finally, Section 5 concludes the paper.

2. Privacy Concerns

As context information is of a highly personal nature it is natural to assume that users will be concerned about who has access to such information. It may be said that social networking and media is changing this attitude and that users are more willing to share personal information. However, further research is needed to confirm this – users may just be limited in their knowledge of the risks or lack good alternative applications which respect privacy. Three salient points are given by Schmidt et al. (2000) which summarize many of the privacy concerns people perceive:

1. People want to be in control of what about them is visible to others.
2. People want to know what others know about them.
3. People like to share information selectively.

In general, research indicates that privacy is less important than is currently thought and that users are willing to share personal information in exchange for useful services (Khalil and Connelly, 2006; Raento and Oulasvirta, 2008; Ophoff and Botha, 2008). However, this does not mean that the privacy of information is not valued (Danezis et al., 2005). Rather, the social relationship as well as the type of information influences privacy.

Research has shown that privacy concerns depend significantly on the relationship between caller and receiver (Consolvo et al., 2005; Khalil and Connelly, 2006; Raento and Oulasvirta, 2008). Users are more likely to share availability information with social relations such as significant other, family and friends (Khalil and Connelly, 2006). Similar findings have been shown for the sharing of location information (Consolvo et al., 2005).

It has also been shown that different kinds of context are perceived with varying levels of privacy. Information such as location and activity are perceived as more sensitive than company and conversation (Khalil and Connelly, 2006). However, it has been found that users often share such information in as much detail as possible, or not at all (Consolvo et al., 2005). This is in contrast to other projects which have found allowing granular information to be important (De Guzman et al., 2007; Raento and Oulasvirta, 2008). Controlling the granularity of information displayed to different groups and having the ability to fake some or all context information is an important aspect in giving users full control over their information (Raento and Oulasvirta, 2008).

3. Social Relationship Groups

The users in a contact list often express a social relationship with the user in charge of it. Relationships affect our knowledge of another user as well as our availability for communication with a user. Relationships also influence our perception of privacy and will determine how much information we are willing to share.

It is generally accepted that relationships are not innate, but are formed and develop gradually over time as exchanges between people take place (Roloff, 1981, pp. 61–

62). These social relationships are greatly influenced by the time or the need we have to develop a relationship (Trenholm and Jensen, 1996, p. 352). Consequently, many unique relationships develop between people.

Hartley (1993, p. 177) observes that in everyday life we often recognize complex, individual relationships arranged into groups. He proposes, for example, three such groups: family, friends, and co-workers. Such groups are easily expressible classifications of the type of relationship we have with a specific person. For example, instead of saying that one has a confiding, respectful relationship with someone, we would abstract it and simply call each other friends.

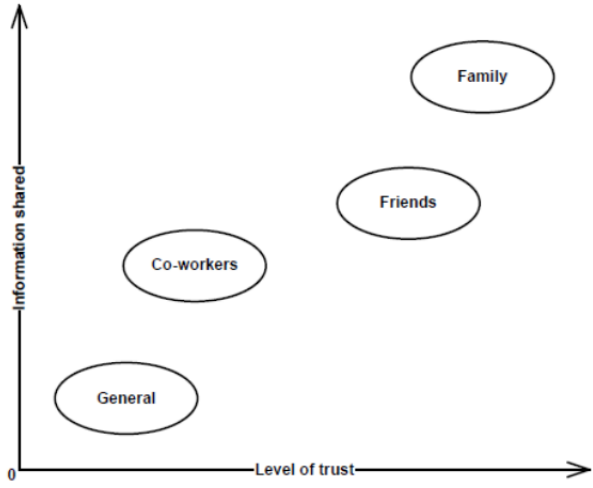

Figure 1: Social Relationship Groups

It is acknowledged that many types of relationships exist in the real world and it is left up to users to define the relationships which apply to them. However, it is common to identify general groups of relationships which apply to almost all users. As example four groups are suggested in Figure 1: general, co-workers, friends and family. The figure presents an illustrative example of how a user may classify relationships.

Social relationships move through various stages characterized by changing levels of communication and self-disclosure. DeVito (1992, p. 428) explains that these stages range from initial contact and involvement to intimacy, possibly followed by deterioration and, finally, dissolution. While trust increases when a relationship is growing, it is an almost universal truth that a deterioration of a relationship leads to a marked decrease in trust (DeVito, 1992, p. 426). The amount of information being shared is dependent on the state of the relationship as well as the sensitivity of the information (DeVito, 1992, p. 368).

Thus social relationships play an important role in our perception of privacy. It is likely that we would share more context information with someone we are familiar with or who reciprocates the act. Thus, in the long term, it may be possible to

automatically adapt the level of information sharing, based on the amount of reciprocated information and the sensitivity thereof.

4. A Model for Communications Management in the IMS

The IMS is a service enabling platform, offering features which services can build upon (Cuevas et al., 2012). On top of the core network various application servers reside which host and execute services. The main protocol linking all these components and responsible for establishing and managing sessions (referred to as calls in traditional telephony) is the Session Initiation Protocol (SIP) (Rosenberg et al., 2002). In addition the Session Description Protocol (SDP) plays an important role in describing multimedia sessions (Handley and Jaconson, 1998).

The ability to create advanced services is one of the most important features of the IMS. One of the most significant services that the network will provide is presence.

4.1. Presence as a Service

At a fundamental level presence conveys a user's availability and willingness to communicate. In the context of this research presence refers to whether a user can be contacted right now. Knowing about presence is useful because it saves communication time.

IMS presence can provide a much more detailed description of the current user state than currently available in applications, where presence information is limited to user availability. This description can include communication address information, such as email or mobile phone, the terminal capabilities, for example video support, and location information, all distributed in real time to authorized users. Information is transmitted in real time meaning enriched communications and a better end user experience.

In the network presence information is not only available to end-users, but also to other services which can benefit from the information. Figure 2 illustrates how, in addition to the data and sensors on the mobile phone, services used by the receiver can publish context information. These services can share context with each other and also publish presence information to the presence service. Another feature which increases the available context in the IMS is the session protocol, which is examined next.

4.2. Session Description Protocol

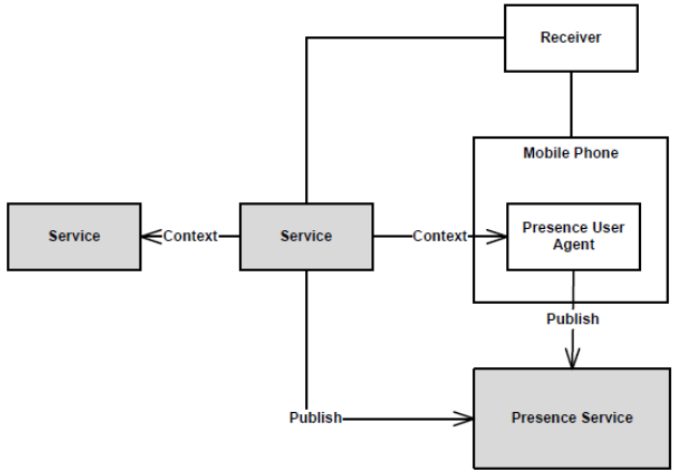

Figure 2: Service Context

In the network SDP provides a complete description of the session to be established. This description can be further classified into session- and media-level information. SDP makes session information, such as the subject of the session and the time at which the session is to take place, available. In addition, information about the media requirements for the session, such as port numbers and codecs, can also be retrieved.

The PUA or user can use this additional information for further decision making regarding the session. When combined with presence and a SIP message, which contains information such as the user address, routing and security requirements, this creates a comprehensive set of data which can be used as the basis for a decision model in a communications management service. In addition, a lot of information can be obtained from the network automatically.

4.3. Presence for Communications Management in the IMS

The model prescribes that callers be assigned into one or more groups, based on social relationship. Groups are implemented through authorization policies and rules. The existing standards which define authorization policies do not allow for user defined groups as part of the conditions of an authorization rule. Thus the model uniquely extends these rules by adding the group condition. This provides a mechanism by which a receiver can define a privacy list by groups of contacts and apply presence authorization accordingly.

A user would create and maintain a group document which is stored alongside presence information and authorization rules. When examining a rule set the presence server would identify whether a group (list element) exists as an identity condition. If a group does exist the presence server imports all the corresponding callers as specified in the document, before applying the necessary actions and transformations to the presence information. This is illustrated in Figure 3.

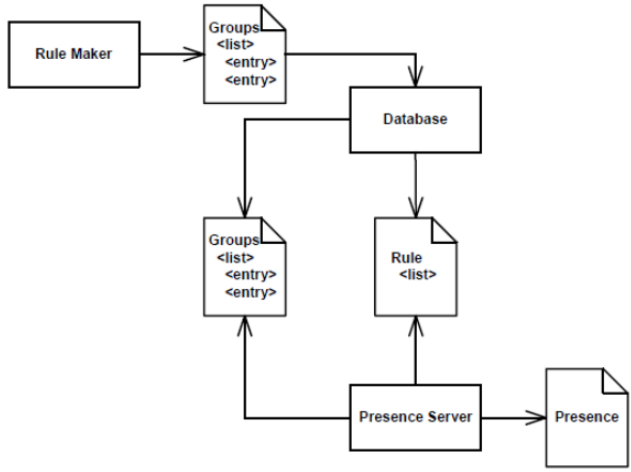

Figure 3: Groups Extension to the Presence Authorization Framework

Several entities in the IMS provide additional privacy to the user. This extends the functionality available through presence standards. The information contained by the SDP can be used as conditions for authorization rules. For example, the type of session can be used to filter requests for presence information when connected to anything other than a voice call. The filter criteria in the Home Subscriber Server can also be used as part of a presence authorization policy. The filter criteria is similar to the conditions part of authorization rules. However, in addition to specifying when a permission applies, the filter criteria can specify specific services to be invoked.

Figure 4 illustrates the proposed model. Standard IMS components are not elaborated, but numeric labels indicate the points of extension for communications management. Below each extension point is discussed:

1. IMS services used by a user can provide additional context information to a PUA or other services. A service can also publish information directly to a presence service.
2. Session information exposed by SDP further extends the information available to entities in the IMS. Together with service context this extends the information available to make communications management decisions.
3. The user profile information located on the Home Subscriber Server can be used for decision making by services in the IMS. The Serving Call/Session Control Function is the main entity that makes use of this information. The user profile can be updated via a SIP Application Server.
4. User profile information can also be used as an availability indicator to callers. However, in this case the omission of authorization rules must be taken into consideration as a potential loss of privacy can occur.
5. Services can assist users in managing communications. A SIP Proxy Server can be used to manage incoming communications and provide forwarding to a new endpoint. Thus the receiver can remain connected for communication using a single identity on the network.

6. The model call profile construct can be extended by using a SIP Terminating User Agent. This allows communications to be screened and routed in a preferred manner, including blocking calls. The caller may also be informed of any action and given additional options to proceed.
7. The IMS extends privacy features by allowing user profile information to be used as part of presence authorization rules.
8. Services can provide additional filtering of presence or session information before sending it to a caller. An example is a SIP Back-to-Back User Agent.

The model requires context, captured as presence information. This allows a receiver to present an availability state to potential callers. The model prescribes three approaches in using presence to manage communications. These approaches allow the receiver to indicate availability for communication, the caller to present call cues and the automatic handling of calls for the receiver. These mechanisms allow the caller to make an informed decision about whether to proceed with an intended call. Such knowledge can not only minimize receiver disruptions, but also save the caller from fruitless attempts to contact an unreachable target.

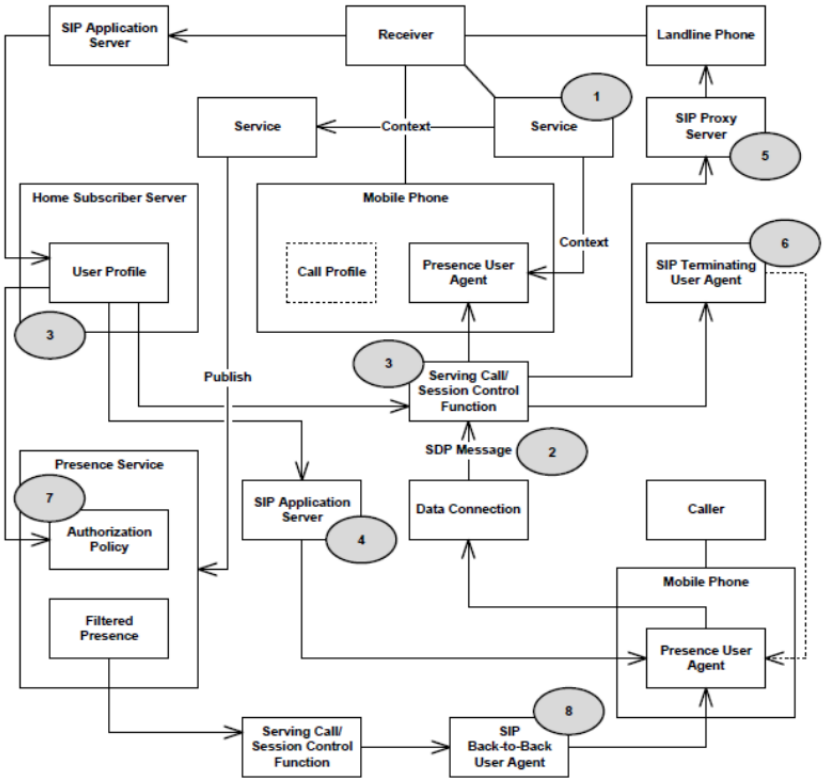

Figure 4: A Model for Communications Management in the IMS

The model also addresses how the receiver can maintain privacy of presence information. Requests for information can come from multiple sources, not all of them trusted. Thus the use of groups based on social relationships is prescribed. This

allows for authorization rules which closely relate to trust relationships in the real world. Authorization rules allow requests to be evaluated according to several conditions and can filter the final presence document before it is returned to a caller.

From the above it can be concluded that the model fits well into the IMS network and can be extended to meet the needs of communications management. Thus the model looks promising for providing value in next generation networks.

5. Conclusion

This paper presented an abstract IMS model based on presence standards, while incorporating privacy and social relationship theories. To facilitate a concise model a discussion of privacy based on context and relationships was given. This allowed the model's core functionality to be defined in a clear and consistent way. While the IMS creates the opportunity for implementing innovative features specifically relating to communications management, it is important to remember that such services are only available to users in the IMS.

Unfortunately relationships are not always the only consideration when deciding if personal information should be shared. Certain situations may force users to share information irrespective of their personal feelings. An example may be a company forcing employees to remain logged on to a communications system and displaying their availability status. These situations are acknowledged by the model and require further research.

6. References

Baladrón, C., Aguiar, J. M., Carro, B., Calavia, L., Cadenas, A. and Sánchez-Esguevillas, A. (2012). Framework for Intelligent Service Adaptation to User's Context in Next Generation Networks, *IEEE Communications Magazine* 50(3), pp. 18–25.

Consolvo, S., Smith, I. E., Matthews, T., LaMarca, A., Tabert, J. and Powledge, P. (2005). Location Disclosure to Social Relations: Why, When, & What People Want to Share, CHI '05: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM Press, pp. 81–90.

Cuevas, A., Nicoll, W. and Schroder, K. (2012). The challenges of IMS deployment at Telefonica Germany, *IEEE Communications Magazine* 50(8), pp. 120–127.

Danezis, G., Lewis, S. and Anderson, R. (2005). How Much is Location Privacy Worth?, *Proceedings of the Fourth Workshop on the Economics of Information Security*.

Davenport, T. H. and Beck, J. C. (2000). Getting the Attention You Need, *Harvard Business Review* 78(5), pp. 118–126.

De Guzman, E. S., Sharmin, M. and Bailey, B. P. (2007). Should I Call Now? Understanding What Context is Considered When Deciding Whether to Initiate Remote Communication via Mobile Devices, *GI '07: Proceedings of Graphics Interface 2007*, ACM Press, pp. 143–150.

DeVito, J. A. (1992). *The Interpersonal Communication Book*, 6th edn, HarperCollins Publishers.

Handley, M. and Jaconson, V. (1998). *SDP: Session Description Protocol*, RFC 2327, Internet Engineering Task Force.

Hartley, P. (1993). *Interpersonal Communication*, Routledge.

Khalil, A. and Connelly, K. (2006). Context-aware Telephony: Privacy Preferences and Sharing Patterns, *CSCW '06: Proceedings of the 2006 20th Anniversary Conference on Computer Supported Cooperative Work*, ACM Press, pp. 469–478.

Ling, R. (2004). *The Mobile Connection: The Cell Phone's Impact on Society*, Morgan Kaufmann.

Love, S. and Perry, M. (2004). Dealing with Mobile Conversations in Public Places: some implications for the design of socially intrusive technologies, *CHI '04: CHI '04 Extended Abstracts on Human Factors in Computing Systems*, pp. 1195–1198.

Ophoff, J. and Botha, R. (2008). Mobile Communications: User Perception and Practice, *South African Computer Journal* 40, pp. 63–73.

Palen, L., Salzman, M. and Youngs, E. (2000). Going Wireless: Behavior & Practice of New Mobile Phone Users, *CSCW '00: Proceedings of the 2000 ACM Conference on Computer Supported Cooperative Work*, pp. 201–210.

Raento, M. and Oulasvirta, A. (2008). Designing for privacy and self-presentation in social awareness, *Personal and Ubiquitous Computing* 12(7), pp. 527–542.

Rennecker, J. and Godwin, L. (2005). Delays and interruptions: A self-perpetuating paradox of communication technology use, *Information and Organization* 15(3), pp. 247–266.

Roloff, M. E. (1981). *Interpersonal Communication: The Social Exchange Approach*, Sage Publications.

Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M. and Schooler, E. (2002). *SIP: Session Initiation Protocol*, RFC 3261, Internet Engineering Task Force.

Schmidt, A., Takaluoma, A. and Mäntyjärvi, J. (2000). Context-Aware Telephony Over WAP, *Personal and Ubiquitous Computing* 4(4), pp. 225–229.

Trenholm, S. and Jensen, A. (1996). *Interpersonal Communication*, 3rd edn, Wadsworth Publishing Company.