

To be or not to be in control that is the question

J. de Heer, A.J.H. Peddemors & W.B. Teeuw¹

Telematica Instituut
P.O. Box 589 7500 AN Enschede, The Netherlands +31 (53) 4850485
{Johan.deHeer, Arjan.Peddemors, Wouter.Teeuw}@telin.nl

Abstract

The challenge of managing secure access to information and applications scattered across a wide range of internal and external-computing systems is no sinecure. In this paper we describe an example of a B2E context-aware mobile application framework to introduce the concept of location (where am I, where are my colleagues) as an integral part of a traditional presence and instant messaging system. The question we raise is who may see where I am, and who determines this? Or stated more broadly, how do we handle identity management in a context-aware mobile application framework? The model for location handling we opt for is such that the user is always in control of who receives his position information. The paradox is that although the user is in control of whom receives his position information, the network or server provider may always circumvent the subscription mechanism. This security leak imposes implications on privacy and trust issues.

Introduction

The immediate future for mobile applications lies in connecting employees and their employers, in particular in developing and enhancing business-to-employee (B2E) applications. There is now a growing consensus that it is in the B2E arena where early adoption of mobile solutions will have the most beneficial impact on the enterprise. The benefits of providing (mobile) employees with the information they need in an effective and efficient manner means mobile B2E communications and content provision to your employees regardless of where they are or what type of device they are using.

We believe that personalised and device-optimised B2E info communications with automatic localisation will become a decisive topic in the near future. We envision an integrated mobile enterprise solution that will ensure that your business communications and data services can be communicated to any end device at anytime, anywhere, individual, convenient and above all secure.

A business-to-employee (B2E) example is a calendar/scheduling service that automatically changes the user presence into "in a meeting" at the moment that he enters the meeting room associated with a scheduled meeting. Another example is the notification service that informs the user when a friend or colleague is in the same area, if his current presence indicates that he is interested in receiving these notifications ("online and ready for vicinity events").

However, the challenge of managing secure access to information and applications scattered across a wide range of internal and external-computing systems is no sinecure. For example, think of providing access to visiting colleagues from a related organisation without diminishing security or exposing sensitive information. The management of multiple versions of user identities across multiple applications makes the task even more overwhelming.

Future mobile application framework are context-aware

It is very likely that future mobile application domains adept new paradigms that specifically target the mobile environment. We believe that an important paradigm is *context-awareness*. Context is relevant to the mobile user, because in a mobile environment the context is often very dynamic and the user interacts differently with the applications on his mobile device when the context is different. While a desktop machine usually is in a fixed context, a mobile device goes from work, to on the road, to work in-a-meeting, to home, etc. Context is not limited to the physical world around the user, but also incorporates the user's behaviour, and terminal and network characteristics.

Also, based on and broader than context-awareness are concepts like personalization, ambient intelligence, pervasive, and ubiquitous computing. They can be found as basic principles in long-term strategic research for mobile and wireless systems such as formulated in [1] and [2].

¹ Authors listed in alphabetic order

Note that – as a first weak signal for the 2010 scenarios on ambient intelligence [2] - the majority of context-aware computing to date has been restricted to location-aware computing for mobile applications (location-based services).

Presence, Location and Instant Messaging (PLIM) Platform

We have developed an experimental framework that joins the concepts of Presence, Location and Instant Messaging (PLIM) in an extended existing instant messaging system [3, 4]. The additional location functionality lets a mobile device determine its location in an indoor environment at a fine-grained level (room-level in an office building). The experimental framework prototype uses a Bluetooth network infrastructure to let a mobile device determine its indoor position as well as to deliver IP connectivity. Thus, we consider the *presence* information as used in existing presence and instant messaging services as an important form of context. Presence provides information about the current state and activity of the user. Presence information is adequately handled by existing software on traditional computing platforms and increasingly also on mobile platforms. Additionally, we consider *location* a prime form of context information. This provides information about the current location of the user. Both indicators of context are part of this context-aware mobile application framework. The PLIM framework is an example of how context information is relevant in a networked mobile environment.

User requirements for PLIM

- The user must be able to indicate who is allowed to see at which location he is;
- The user must be able to indicate who is allowed to see his presence information;
- The user can indicate that urgent messages that arrive from certain users are always directly received, even when his present status is 'away' or 'do not disturb';
- The linking of the user's current position with the position of the persons on his list (if he is allowed to get position information from these persons). This feature can support, for instance, the generation of a notification event when a listed person is within a certain distance of the user;
- The permission to see one's location is independent from the permission to see one's presence information;
- The user can link location status with presence status, i.e. he can indicate that if he resides at a certain location, his presence status is set appropriate for that location. For instance, if the user never wants to be disturbed in meeting room X, he can indicate that whenever he is at this location, the presence information is set to "do not disturb". [5]

Security handling²

As the user moves, the mobile device (e.g., PDA) is in range of often changing Bluetooth cells. When a PLIM client enters a new cell, it asks the location server available at the access point for its current location (an access point is aware of its location). Then, the client – on behalf of the user - sends a location status update to the messaging server. The location handler in the messaging server makes sure that the users who watch the location status of the updating user get, for instance, a notification. Security on location information is handled on two levels. First, the user may indicate to the client software not to provide location to anyone. Secondly, a subscription mechanism let the user again determine who may see its presence and location information. The model for location handling we opt for here is such that the user is always in control.

Privacy & Trust: The network or server may know where you are [6]

The paradox of location is that location-independence requires a smart network that knows where we are. For both mobile applications like cell phones, and less-mobile applications like Internet access, the network needs to know where you are, and where your colleagues are within the business environment. In other words, a person's identity is becoming more mobile. Though it is easy to think of services that are possible when a network is automatically aware of where you are. For example, real time location-specific usage on road travel accompanied by a pay-when-you-use principle. On the other hand, there are other implications for the network 'knowing where you are' depending on a company's perspective and ability to act. For example the wireless 911, an emergency phone system in the US that will allow police to track mobile phone users with a greater precision.

These implications may either pose as opportunities or threats. The desire for privacy, for instance, could be threatened. Not only does the network know where you are at all times, but it stores also details about your identity and possible other information about you. As a consequence, users may have

² We limit ourselves to location handling, though the same level of argumentation holds for presence handling

to lessen their anonymity in order to realise these enhanced services, while business will have to ensure that they respect their promises of whom they share their information with. Also the (perceived) level of trust can be considered a business enabler or disabler [7]. In the case of PLIM for example, in which the network not automatically knows where you are, the server provider, on the other hand, may circumvent the subscription mechanism and providing location information to third parties, which may violate the trust relation between the user and the server provider.

Conclusion

Handling identity management in a context-aware mobile application framework either pose opportunities or threats? The model for location handling we opt for is such that the user is always in control of who receives his position information. The paradox is that although the user is in control of who receives his position- and presence-information, the network/server provider may circumvent the subscription mechanism. This security leak imposes implications on privacy and trust issues and on user-, business-, and network requirements.

References

1. Wireless World Research Forum, "Book of Visions 2001", Version 1.0, <http://www.wireless-world-research.org/>
2. K. Ducatel, M. Bogdanowicz, F. Scapalo, J. Leijten, J-C. Burgelman, "ISTAG Scenarios for Ambient Intelligence", <ftp://ftp.cordis.lu/pub/ist/docs/istagscenarios2010.pdf>, Feb 2001.
3. A.J.H. Peddemors, M.M. Lankhorst, J. de Heer (2002). Combining presence, location and instant messaging in a context-aware mobile application framework. *GigaMobile/D2.8 (TI/RS/2002/068)* Telematica Instituut Enschede. https://doc.telin.nl/dscgi/ds.py/Get/File-21982/PLIM_d28.pdf
4. GigaMobile project. <http://www.telin.nl/Middleware/GIGAMOBILE/demos/GigaMobile.html>
5. M. Markslag, A.J.H. Peddemors, J. Reitsma (2002). The Location Visualization demonstrator. https://doc.telin.nl/dscgi/ds.py/Get/File-22017/Location_Visualization_Demonstrator.ppt
6. Kathryn Kai-ling Ho (2002). The network knows where you are. [http://www.cbi.cgey.com/pub/bi-news/pdf/phpTMZlpn\\$.pdf](http://www.cbi.cgey.com/pub/bi-news/pdf/phpTMZlpn$.pdf)
7. Van Kranenburg, H. (2000) *Privacy aspects in Internet and mobile services*, Enschede: Telematica Instituut, GigaMobile/D1.1.6, Enschede: Telematica Instituut. https://doc.telin.nl/dscgi/ds.py/Get/File-13064/D1.1.6_privacy_SOTA.doc