

Ensuring Privacy in Presence Awareness Systems: Next Generation Networks

Michael Nyarko, Neco Ventura

*Centre of Excellence,
Department of Electrical Engineering,
University of Cape Town
Cape Town, South Africa
{michaeln, neco}@crg.ee.uct.ac.za*

Abstract— Presence technology has played a significant role in the way that people interact, allowing a more efficient means of communication by mitigating unsuccessful attempts to reach persons who were unavailable over various means of communication such as cellular phone, personal computer or even a landline. Presence technology has completely revolutionized the way people interact with one another over the internet. Since its introduction into the communication arena, existing internet applications such as Instant Messaging, email and online games, have enjoyed an increase in number of users. Presence technology's success since its introduction has placed it as a possible candidate for Next Generation Network's services integration tool. However, with such an increase in number of users, certain challenges arose. Among these is the issue of privacy. Who may and may not view a user's presence information? How is this information kept private from third parties? Privacy concerns of users using the presence technology, greatly affect their willingness to use the particular application, and if not well addressed, users may lose confidence and stop using the particular application. This project addresses this concern of privacy by providing a mechanism to ensure privacy. An architecture is proposed to implement the securing of users presence information. As a practical facet of the project at hand, the author developed and implemented a subset of the proposed architecture over an Internet Protocol Multimedia Subsystem network. The implementation demonstrated the privacy ensuring mechanism desired in this project.

Keywords— Presence, privacy, entity, server

I. INTRODUCTION

The advancement of technology over the years has seen a wide deployment of network applications into existing internet infrastructure with a common aim to integrate existing services. Presence has over the years been envisioned as the basic service of many if not all web based applications in the near future. This is a technology that gives users the opportunity to be informed on matters such as the reachability, availability and the willingness to communicate of their companions, spouses and any other interested party.

The authors would like to thank Telkom SA, the National Research Foundation (NRF), Technology and Human Resources for Industry Programme (THRIP), the Department of Trade and Industry (DTI), Nokia Siemens Networks and TeleSciences, for supporting this research project.

This technology allows users to communicate their communication means and capabilities which include whether or not their communication media supports audio, video or Instant Messaging (IM). Initially this was a service built on top of the Session Initiation Protocol (SIP) event notification framework, to allow Presence User Agents (PUA's) to subscribe to or fetch a presence entity's (presentity) presence information. However, presence functionality has far advanced beyond that and is now being used in all spheres of life, from commercial to social circles. Presence maximises efficiency of communication by preventing users from trying to reach unavailable users. With this kind of technology, users need not try keep track of where their persons of concern are at any given point in time, as this can readily be done for them. The issue of privacy however, has long plagued the wide deployment of presence services ever since its introduction into the communication arena. Privacy affects the degree of social presence [1] and the level to which humans interact with media-based communication devices is affected by this same factor of privacy. The level of privacy is largely influenced by the users' perceptions together with the actual security features of that system. For instance a public system, such as internet café, would be perceived as offering lower level of privacy as compared to private systems like a personal laptop.

In today's modern world, information drives everything. The well informed are making better decisions than those less informed. Companies and individuals are constantly looking for ways to gain more information about matters that concern them and mostly to capitalize on that information. The kind of information that the presence service can divulge could have unpleasant results if it falls in the wrong hands. Marketers are able to compile a users location history thereby being able to determine their shopping habits and when best to advertise. People have the tendency to take risks when they feel they have nothing or very little to lose if their activities were discovered by unintended third parties [1]. This leaves them vulnerable to predators looking to capitalize on any given opportunity. With the high and ever growing crime statistics of many countries today, presence service is required to be very secure and privacy policies well implemented. Thieves could benefit greatly from knowing the location of a

presentity at a given time, for an example if they are home or not.

Privacy, however, is seen as a non functional requirement [2] and is commonly left out of the design process such that end products do not meet privacy requirements. This however needs to change if presence services are to be widely deployed. Efforts are currently being put into incorporating privacy requirements into the design process to better ensure users' willingness to use the presence service on presence capable devices. The user has to have a very high degree of confidence that the implementation of privacy policies are correct else they often very quickly abandon the application [3]. Take for an example the current implementation of the presence service on Google Talk, when a presentity sets their status to busy, they would expect buddies not to disturb them and if they persistently send IM's, the user is forced to take other measures such as blocking that particular user or logging off completely.

II. PRESENCE IN NEXT GENERATION NETWORKS

Presence is believed to be the service of the Next Generation Networks (NGN) [4] and is soon becoming a generic interface for user-application integration. This integration is prominently driven by the adoption of common signalling standards, SIP and SIMPLE [5]. Presence is seen as the ultimate real-time communications, messaging and routing infrastructure that not only supports collaborative applications for user-user interaction but also communication between users and applications [6]. Presence technology goes further to support application to application integration, where it is used to announce which applications are up, what their functions are and the type of protocols they accept. This promising technology shares the vision of NGN, promising users the ability to reach other users instantly regardless of location, over a variety of media, including chat, video and wireless or traditional voice. This technology has seen tremendous growth over the years stemming from the establishment of companies such as Groove Networks in 1998 by Ray Ozzie (Creator of Lotus Notes), to foster presence-based software. Figure 1 below presents a general overview of the envisioned NGN network, a network in which presence technology is used extensively to optimise service provisioning.

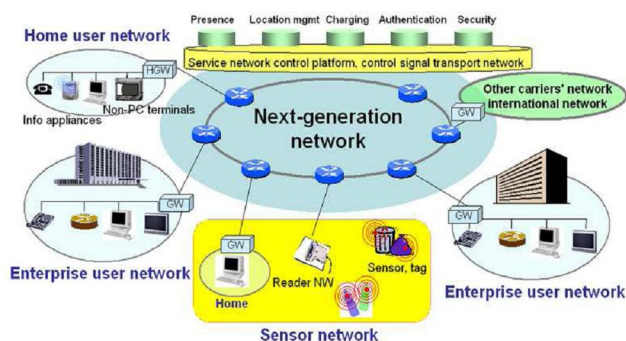


Fig. 1 Overview of envisioned NGN network

III. SIP PRESENCE ARCHITECTURE

Figure 2 presents the basic layout of the SIP presentity architecture in which a presentity may have several Presence User Agents (PUA's) communicating with a single Presence Agent/Server (PA/S). The PS receives information from all PUA's belonging to a particular presentity and then builds a complete picture of the presentity's current activity(s). Other presentities attached to the same PS then acts as watchers if subscribed to that particular presentity's presence.



Fig. 2 Sip Presence Architecture

A. Presence Server

The Presence Server acts as a repository for all presence information. When a presentity registers itself to the IMS network, a SIP PUBLISH request is sent to the PS on behalf of the presentity containing presence information about that presentity from the Serving Call Session Control Function (S-CSCF) after being authenticated. The PS then sends a SIP NOTIFY request to all subscribed watchers after storing the presence information. When changes in the status of the presentity occur at any point in time, further SIP PUBLISH and NOTIFY requests are generated to inform the PS and the registered watchers respectively. To avoid abrupt disconnection of devices from the network a default subscription duration is usually incorporated into the PS. Presentities are required to refresh their subscription with the PS before the expiration of this time else their status is automatically set to Offline.

B. Protocols

Previously, companies implemented their own protocols to provide IM services but are now moving towards protocols standardised by the Internet Engineering Task Force (IETF), such as SIP and Extensible Message and Presence Protocol (XMPP). Several other protocols are involved in the implementation of presence technology over the internet, which include XCAP, Hypertext Transfer Protocol (HTTP) and SIP for Instant Messaging and Presence Leveraging Extensions (SIMPLE). The two currently used protocols include SIMPLE and XMPP. These two protocols are IETF standards and are fast replacing proprietary protocols previously used by companies. Their incompatibility however means that a number of presence systems cannot work together. SIP is the only protocol used in the implementation of the proposed framework.

SIP is an application-layer control protocol used in the IMS network and serves the purpose of establishing, modifying and terminating of multimedia sessions between two terminals. This open and flexible protocol is used by the UCT IMS Client (UIC) [7] to communicate with the IMS core. The body of a SIP message is described using the Session Description Protocol (SDP) [8], which is a syntax for describing media flows (address, port, media type, encoding, etc), standardised in [9] and later in [10]. SIP allows service providers to freely choose among standards based components and quickly harness new technologies. Table 1 below presents a subset of SIP methods used in the IMS network for inter entity communication.

TABLE I SIP REQUESTS

Method Type	Usage
INVITE	Establishes a session
ACK	Confirms an INVITE request
BYE	Ends a session
CANCEL	Cancels establishing of a session
REGISTER	Communicates user location (hostname , IP)
OPTIONS	Communicates information about the capabilities of the calling and receiving phones

IV. PROPOSED ARCHITECTURE

The author implemented the incorporation of an access list into the Presence Server as specified in [11]. The layered structure depicted in figure 3 below, allows for easier extension of the IMS network to include other applications. New applications are added to the application layer and changes made in the Home Subscriber Server (HSS) to channel the desired messages to that particular application server. All communication from the access layer to the application layer still runs through the core, network layer, to further facilitate security enforcement.

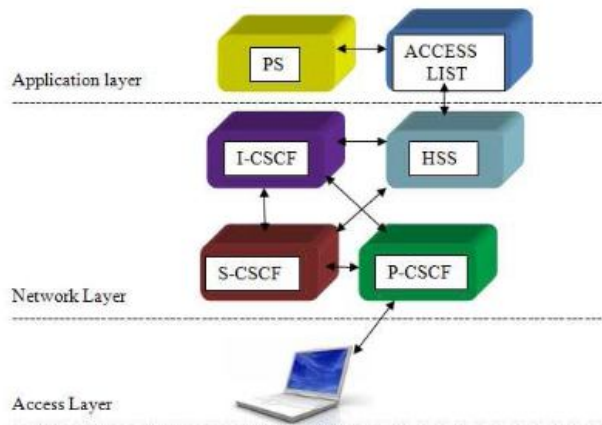


Fig. 3 Proposed Architecture-Layered view of the IMS network

A. The Access List

Figure 4 below depicts the basic structure of the access list specified in [7]. The structure involves the categorizing of watchers into groups such as family, friends, others, etc. Each group is then assigned a particular set of viewable information about the presentity, referred to as tuples.

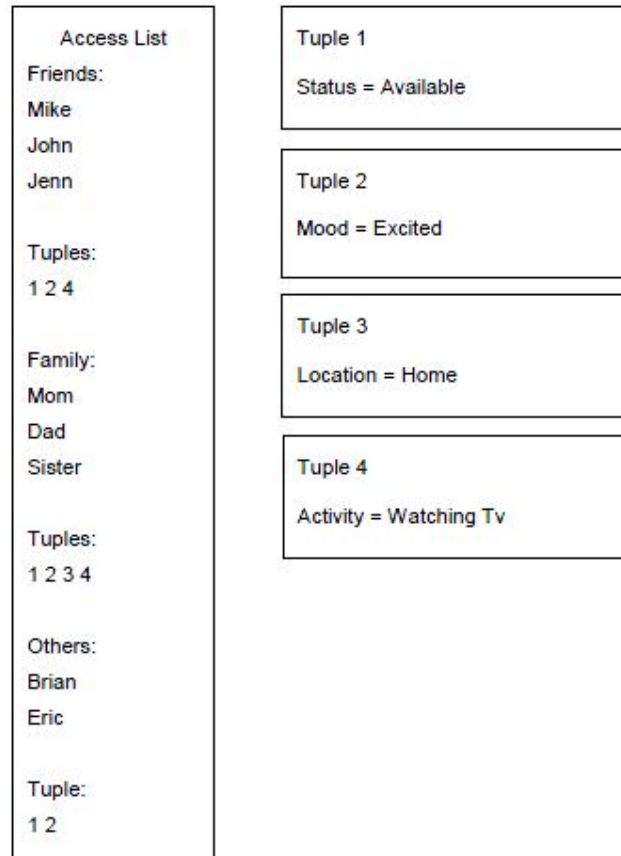


Fig. 4 Example of an access list

V. PERFORMANCE EVALUATION

For ease of evaluation and testing purposes, the access list was implemented on the client side. The author could then easily set different test values, using a simple graphical user interface, without having to make any major changes in the PS. With every publish message that was sent to the PS, new set of rules could be included and the results immediately seen on the UCT IMS client output terminal. For simplicity, only two tuples, location and note, were used together with two users, Bob and Alice. Location represented the current location of the user and the note represented his/her current status. A value of one (1) or zero (0) could then be assigned to either of these tuples to render them viewable or non viewable by third parties respectively.

Four usage scenarios are outlined in table 2, considering all possible combinations of the two tuple values.

**TABLE II
TEST VALUES**

Note	Location	
	0	1
0	00	01
1	10	11

**TABLE III
TEST RESULTS**

Case	Location	Note
00	Unknown	Guess
01	Unknown	Tired
10	My Room	Guess
11	BTF	Cloud 9

Figure 5 below, snapshot of the UCT IMS CLIENT, presents a graphical result of one of the cases tabulated above. Note that the respective values of the two tuples are highlighted in green circles.

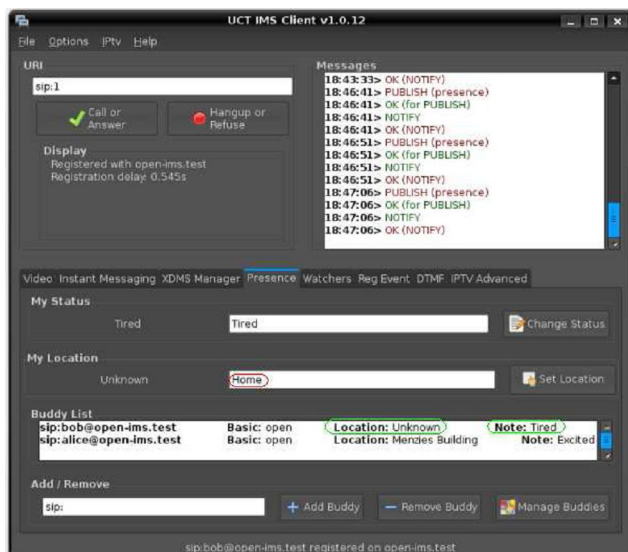


Fig. 5 Case 01 – Location not viewable, note viewable

VI. CONCLUSIONS

The objective of this project was to provide a mechanism for ensuring presence privacy over an IMS network. A test bed was created using the IMS core, a Presence Server(PS) and a client. A proposed architecture was designed, developed and implemented. The implementation introduced the use of an access list as a set of rules by which the PS leverages presence information concerning a presentity. The access list

was simplified and implemented on the client side for testing purposes. The presentity was given the ability to change these rules with every PUBLISH message sent to the PS thus giving the user more control over their presence information while inculcating a sense of privacy. The implementation was successful and was able to demonstrate that privacy can easily be incorporated into presence awareness systems. Watchers were only allowed to view information that the user has set to viewable. The PS stored the rules that accompanied each PUBLISH message sent to it and updated the existing rules each time a new message was received. It also acted as the sole publisher of all presence information to watchers such that in an event where a third party tries to PUBLISH presence information on behalf of the presentity, the PS still implemented the presentity's preset rules before publishing. This feature further tightens the security offered by the presence server and even if the IMS network was ever to be compromised, users can be rest assured that their privacy is still well maintained.

REFERENCES

- [1] C. Tu, *The relationship between social presence and online privacy*. The Internet and Higher Education Volume 5, Issue 4, 2002, Pages 293-318
- [2] E. Yu, L. M. Cysneiros *Designing for Privacy in the Presence of Other Requirements..* 4th Workshop on Deception, Fraud and Trust in Agent Societies. Bologna, Italy, July, 2002
- [3] P. Godefroid, J. D. Herbsled, L. J. Jagadeesan, and D. Li, *Ensuring Privacy in Presence Awareness Systems: An Automated Verification Approach*. ACM 2000 Conference on Computer Supported Cooperative Work, Philadelphia, December ,2000
- [4] J. Fontana. Presence Applications poised for take-off. [Online]. Available: www.networworld.com/news/2004/09064specialfocus.html. 2008
- [5] L. P. Cox, A..Dalton, and V. Marupadi, *Smoke Screen: Flexible Privacy Controls for Presence Sharing*. International Conference On Mobile Systems, Applications And Services, 10th workshop on Mobile Computing Systems and Applications, June , 2007
- [6] M. Pitman, N. Ventura, *Aggregate Efficacy of Resource List Servers in IMS Presence Services* [online]. Available: [http://home.intekom.com/satnac/proceedings/2008/papers/ip/Pitman No 55.pdf](http://home.intekom.com/satnac/proceedings/2008/papers/ip/Pitman%20No%2055.pdf)
- [7] UCT IMS CLIENT [online]. Available: <http://uctimsclient.berlios.de/>
- [8] G. Bertrand. *The IP Multimedia Subsystem in Next Generation Networks*, White Paper. May 30, 2007 Available: http://www.rennes.telecom-bretagne.eu/~gbertran/pages/ip_multimedia_subsystem.html
- [9] RFC 2327 [online] Available: <http://www.ietf.org/rfc/rfc2327.txt>
- [10] RFC 3264 [online] Available: <http://www.ietf.org/rfc/rfc3264.txt>
- [11] 3GPP TS 23.141 v8.1.0, *Presence service; Architecture and functional description*. June, 2008

Michael Nyarko obtained his BSc (Eng) Electrical and Computer degree from the University of Cape Town and is currently doing his MSc degree in Electrical Engineering. His research interests are IP Multimedia Subsystems and Electronic Learning Application Servers.