PRIVACY FOR MHEALTH PRESENCE

Xin Huang[1, 2], Yang Jiang[2], Zuguang Liu[2], Theo Kanter[2] and Tingting Zhang[2]

[1]OUCL, University of Oxford, Oxford, United Kingdom
armoxilin@gmail.com
[2]ITM/IKS, Mid Sweden University, Sundsvall, Sweden
{yaji0800,zuli0900}@student.miun.se,
{theo.kantor,tingting.zhang}@miun.se

ABSTRACT

mHealth data provision focuses on providing health services to patients via mobile devices and presence technologies. It has great influence to the healthcare business today, especially in the developing countries. However, the mHealth presence might be sensitive; and it brings potential privacy issues. For controlling what presence information can be given to which watcher, and when in mHealth presence service, XML Configuration Access Protocol (XCAP) is introduced. Nevertheless, it is not enough if only XCAP is applied. It just controls the direct privacy leakage; indirect flow might still leak the privacy information. Thus, presence authorization policy and privacy filter, which are components of XCAP, are improved based on k-anonymity for stopping indirect privacy leakage.

KEYWORDS

Privacy, Wireless Network, Presence

1. INTRODUCTION

With the recent technological advances in mobile devices and technologies, the impact on mHealth becomes significant. The scope of mHealth is changing rapidly. Now it contains the use of computer, networking software and hardware technologies, such as mobile phones, personal digital assistants, tablets, patient monitoring devices, for providing health services to patients. Presence, as one of the important mobile service technologies, is a suitable foundation for mHealth applications. "In computer and telecommunications networks, presence information is a status indicator that conveys ability and willingness of a potential communication partner--for example a user--to communicate. A user's client provides presence information (presence state) via a network connection to a presence service, which is stored in what constitutes his personal availability record (called a presentity) and can be made available for distribution to other users (called watchers) to convey his availability for communication. Presence information has wide application in many communication services and is one of the innovations driving the popularity of instant messaging or recent implementations of voice over IP clients." [1]

In this paper, mHealth presence is introduced for mHealth data provision. It is based on the MediaSense framework, which focuses on the ability of making decisions about service delivery based on context (sensor) information. The distributed sharing of context information is based on the Distributed Context eXchange Protocol (DCXP). [2, 3] With this framework, mHealth sensor presence can be accessible to users that are on the DCXP network and with IP Multimedia Subsystem (IMS) capabilities.

However, the mHealth presence might be sensitive; and it brings potential privacy problems. For controlling "what presence information can be given to which watchers, and when" in

DOI : 10.5121/ijngn.2010.2403

mHealth presence service, XML Configuration Access Protocol (XCAP) is introduced. [4, 5, 6, 7] It is the foundation of presence privacy protection. XCAP provides a client with the means to add, modify, and delete XML configuration data of any kind stored in a server, such as users in a presence list, authorization policies (e.g., a list of authorized watchers), or a list of participants in a conference. However, it is not enough if only XCAP is applied. It just controls the direct flow; indirect flow might still leak the privacy information. Here is an example. The mHealth presence is monitored by the health center. Any authorized person in this health center can see the data in any authorized time at any place. Assume you do not want anyone to trace your activities, it is not working that you simply prevent somebody from watching your location in XCAP. If your mobile phone collects heartbeat rate information and submits to health center. The heartbeat rate when you are working, taking a rest, running, and sleeping are different. Thus, the health center can deduce your location and activities after learning for a few days.

Thus, XCAP needs to be improved for stopping indirect privacy leakage of the mHealth presence service. The risk management model are used to identify the privacy risks; and mitigation plans are proposed, which are used to prevent the privacy threaten. In this paper, presence authorization policy and privacy filter, which are components of XCAP, are improved as the mitigation plans. An authorization policy document contains the authorization rules and permissions specifying what parts of presence information can be sent to the watcher. The authorization policy is created and modified by the presentity using XCAP or other offline mechanisms. Privacy filters are applied to provide selective access of presence data. The presence authorization rules specify these filters for selective access to the mHealth presence. K-anonymity are utilized as the improvement model. K-anonymity focuses on non-interactive releases of relational data and requires that every record in the released dataset be syntactically indistinguishable from at least k−1 other records on the so-called quasi-identifying attributes (like ZIP code and date of birth). This is achieved by syntactic generalization and suppression of these attributes. Generalization means that individual attributes are replaced with a broader category. For example, age: 26 is replaced by age: [20, 30]. Suppression is that individual attributes are replaced with a star. However, K-anonymity is not enough for privacy protection from group privacy leakage and continuous query.

The main contributions of this paper are three-folds.

Firstly, XCAP based direct and indirect privacy protection for mHealth presence is proposed. XCAP is applied to the mHealth presence application for protecting direct privacy leakage. Improved presence authorization policy and privacy filters are used for preventing indirect privacy leakage.

Secondly, K-anonymity privacy theory is used as the mHealth privacy protection model and privacy degree measurement. The habit privacy protection is the main target instead of ID and location k-anonymity proposed before.

Finally, risks management model focusing on privacy is designed. The indirect flow privacy is highlighted in our risk management model.

Our paper is organized as follows. Section 2 discusses the related works; Section 3 explains the mhealth framwork and risks; Section 4 describes the enhanced presence authorization policy and enhanced privacy filters; Section 5 contains some results; finally, some important conclusions are made in Section 6.

2. RELATED WORKS

To the best of our knowledge, no prior work has been done to prevent the presence privacy using k-anonymity. Previous research on the presence privacy issues has either concentrated on the control of the presence information broadcast based on the specified policy or the encryption of the presence information using various methods.

Privacy Butler [8] is a personal privacy rights manager for online presence. It monitors and controls the online presence of its owner through providing notice of changes in online content, and facilitating modification of content that does not meet owner-specified policy.

Google Alerts [9] is a useful tool designed for companies to track their online presence. In order to use the tool, the companies have to register a callback email address as well as a set of search terms. Whenever new content is indexed by Google that matches the search terms, the Google Alerts automatically notifies company through sending an email on the callback email address. Similar technology could be used by users to provide notice of changes in their online presence, though it does not have access to online social networking sites (which typically require a login).

Patrice Godefroid et al. [10] propose a framework of verification approach to automatically detect violations of complex policies using VeriSoft, a tool for systematically testing concurrent systems [11], and through run-time monitoring. As with the other related work listed so far, the approach does not facilitate management of the online presence by attempting to modify content.

Literature discusses presence information encryption issues from multiple perspectives:

SmokeScreen [12] provides a flexible and power-efficient control for location privacy in presence-sharing networks. There require two complementary mechanisms: broadcasting clique signals enables sharing between social relations, since it can only be interpreted by other trusted users; broad-casting opaque identifiers enables sharing between strangers, since it can only be resolved to an identity by a trusted broker.

The wija project [13] is an instant messaging application based on the Jabber protocol. It allows users to encrypt and sign instant messages and to sign presence information. Albeit signing of presence information prevents from impersonating another user, it does not conceal presence at all.

In addition, Karsten Loesing and his colleagues [14] also design an instant messaging system to prevent the disclosures of a user's presence. They utilize an anonymous communication network to protect the users' physical addresses. Additionally, a distributed hash table (DHT) is used to store presence information, so that it is only detectable and applicable for intended users and even not comprehensible for the DHT nodes.

3. FRAMEWORK AND RISK ANALYSIS

In this section, the framework of mHealth presence is introduced firstly; the risk analysis primitives are introduced in part two; and in part three, the mHealth presence framework is evaluated based on the risk model; finally, the risk mitigation plan is proposed.

3.1 Presence Framework and XCAP

Sensor information can enrich the presence service. As described in Section 1, heartbeat rate sensors can be used to monitor the user's heartbeat rate. In addition, environment sensors are

also widely used; they detect parameters related to health, i.e., carbon dioxide, humidity, temperature. Besides, GPS services are also useful for today's mHealth services. The Fig.1 shows our presence framework: MediaSense framework. The distributed sharing of sensor information is based on the Distributed Context eXchange Protocol (DCXP), which is the fundamental protocol in our MediaSense framework [15]. The DCXP is an XML-based application level P2P protocol that offers reliable communication among nodes that have joined the P2P network. The DCXP naming scheme uses Universal Context Identifiers (UCIs) to refer to context information such as sensors in the DCXP network. It can provide sensor information in real-time between mobile applications and the sensor networks that are wirelessly attached to mobile devices via a Bluetooth Wireless Sensor Network Gateway (WSNG). 3G Gateway Support Node (GSN) and a Mobile DCXP Proxy (MDP) are added, so mobile clients can initial conversations with mHealth presence both on IMS networks and on the Internet via a 3G Session Border Gateway (SBG).

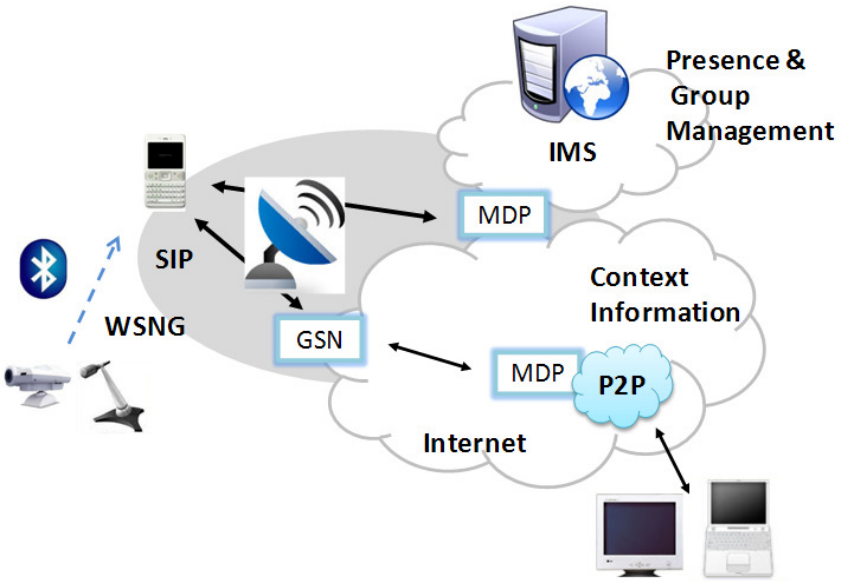

Fig. 1 Presence Framework

With this sensor information, mHealth presence service can be provided; Fig. 2 depicts the whole procedure. mHealth presence stands for the health situation and communication willingness. Presentity is the source of presence information; it could be users or programs. Presentity can publish the presence information via presence user agent. Presentity updates presence information by sending presence data in presence information data format (PIDF) [16]. Rich Presence Extensions to the Presence Information Data Format (RPID) [17] is an extension of PIDF, which includes detailed information about presentity like what is his current activity and what is his mood.

Presence agent receives the presence information from presence user agent; it merges all related information into a raw presence document under the control of composition policy. After the XCAP filtering, the raw document becomes potential presence document. Watcher is the presence information requester. The watcher can subscribe the presence information and receive the notification. The watcher's policy affects watcher's filter in order to change the potential presence document into filtered presence document. Then, the difference presence document will be generated by comparing with the previous presence document. The presence agent

creates and sends a notification to watcher; the watch use the previous presence document and the difference presence document to generate complete presence information.

The XML Configuration Access Protocol (XCAP) [4, 5, 6, 7] manages the presence access control. It can retrieve an item, delete an item, modify an item, and add an item on document, element, attribute. It uses authorization policies, also known as authorization rules, to specify what presence information can be given to which watchers, and when (Presence Rules application). It support resource lists application and resource list server service application which are the resource list access control applications in client and server side respectively. In addition, Pidf-manipulation application usage defines how XCAP is used to manipulate the contents of PIDF based presence documents. The XCAP protocol is based on the following IETF standards: RFC4825 [4], RFC4826 [5], RFC4827 [6], RFC5025 [7].

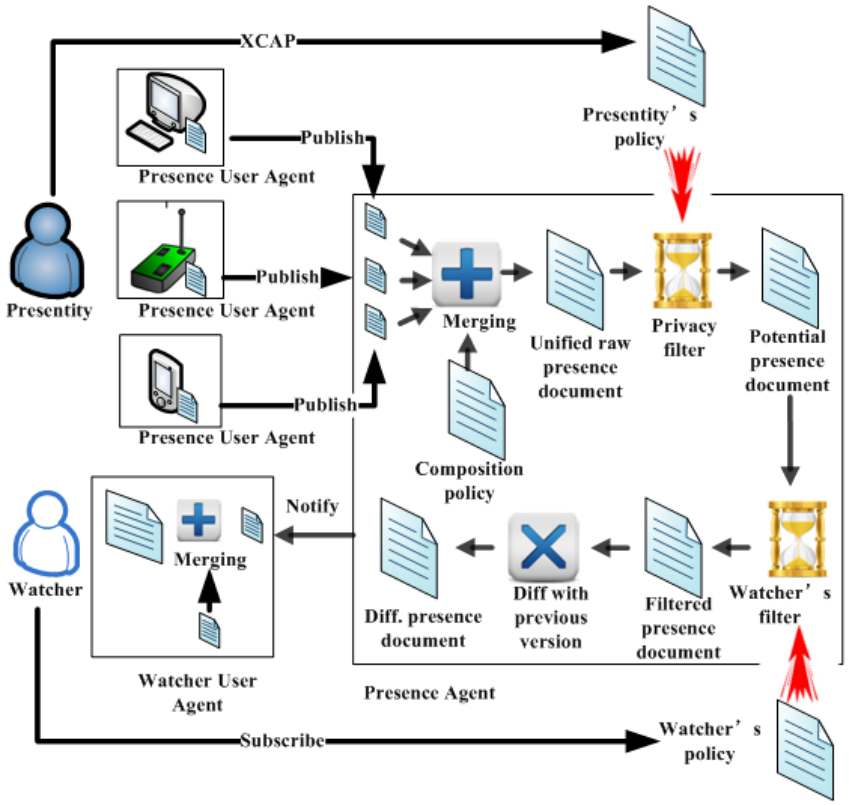

Fig. 2 XCAP for Presence

3.2 Risk Management

In order to analyze the security flaws in XCAP, risk profiles are built for risk management. And mitigation plans are proposed, too.

3.2.1 Risk Profile

In Fig. 3, the risk profile of presence information with network access is shown. Threats are represented visually in the profile using the following properties.

1) Asset is something valuable to the enterprise. Information publisher, watchers are user assets, which are involved in the system. The information assets are user profile, sensor data,

presentity, and presence. The IT assets are presence user agent, presence server (presence database). Among these assets, the critical asset is presence, and the corresponding system component is mHealth presence server.

2) Access is that how the actor will access the asset, e.g., network access, physical access.

3) Actor stands for the people, the application, or other things that may violate the privacy requirements of certain asset. There are mainly three categories: WSN, data proxy, context based applications/context (presence) service.

4) There are two main outcomes: Data Content Leakage (DnL) and Data Context Leakage (DxL) [18]

5) Impact is the severity of consequence. It has three levels: low means it could be happened but will have only a weak effect; medium impact threat should be figure out; otherwise it will cause a relatively severe impact; high level threat will cause destructive consequences and must be solved immediately.

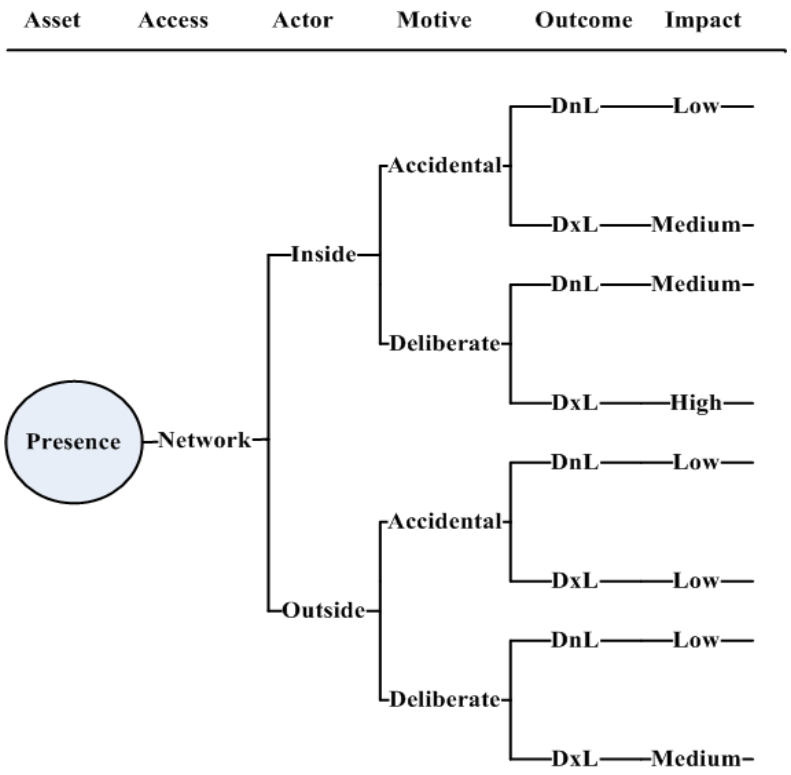

Fig. 3 Risk Profile

mHealth information needs to be protected against unauthorized access. Distribution of mHealth information must also use authentication, confidentiality, and integrity checks. The mechanisms to do so can be in transport protocol or in presence mHealth object itself. The issues concerning mHealth information are mainly related to (i) mHealth information collection (ii) mHealth information retention and (iii) mHealth information distribution and use.

From Fig.3, the risks of DnL are low, medium, low, and low, so watchers may not cause the DnL on purpose and by accident with the help of XCAP. However, the risks of DxL are medium, high, low and medium, so deliberate DxL is still a big problem in the framework.

3.2.2 Mitigation Plan

Based on the problem scenario, three privacy goals can be deduced. First, the watcher should be authorized before the presence information is given. Second, presentity must be able to specify what parts of presence information are given to watcher. The context of presence information, which is given to watcher, should not leak more information about the publisher; the rule of K-anonymity will be applied here.

4. DESIGN

An authorization policy document contains the authorization rules and permissions specifying what parts of presence information can be sent to the watcher. The common policy draft describes a framework for representing authorization policy, e.g., for geo-location and presence information. The authorization policy is created and modified by the presentity using XCAP or other offline mechanisms. Privacy filtering step is invoked in the presence data processing after the composition step. A candidate presence document is generated as a result of composition operation. Privacy filters are applied to provide selective access of presence data. The presence authorization rules specify these filters for selective access to the mHealth presence. In this section, we explain the presence enhanced authorization policy and enhanced privacy filters.

4.2 Enhanced Presence Authorization Policy:

An authorization policy document contains a set of rules, which contains conditions, actions, and transformations. Actions and transformations combinations are called permissions. The conditions specify request attributes; and the actions element tells the server if the system should block, polite-block or allow for the watcher identities. Before the presence goes to the watcher, the transformations modify the presence data as the requirements defined in privacy filtering operation.

Given a set of presence, attributes are characterized into two types: unique habit identifiers which identify certain habit directly; quasi-habit-identifier which is a minimal set of attributes (X1,…, Xd) that can be joined with external information to re-identify individual habit. The unique habit identifiers can be directly forbidden to access by XCAP. Nevertheless, the quasi-habit-identifiers, which is always needed by health center to monitoring your health situation, are always not able to apply direct access control. These sensitive attributes should be protected by K-anonymity [19, 20, 21]. It requires that a set of k presence records to be indistinguishable from each other based on a quasi-habit set. There are already some works that utilize k-anonymity to protect location information [22-25]. They design the rule that there must be k-1 other mobile clients in certain area when the user query some information from the server side. In this case, the server cannot distinguish the relationship from the query and the client; so, it protect the privacy of users. While in our paper, k-anonymity is applied to presence publication procedure, which is different form database based dataset publication and simple location k-anonymity. First, the scope is extended: ID and location privacy are not the only target anymore; life style or habit privacy protection is the main target. Second, procedure is different: our solution should fit to the presence privacy protection solution (XCAP) instead of simply data operation.

The K-anonymity rule requires the presence server (mHealth Server) predefine presence information to watchers with different level of precision. From lowest to highest level, the names of heartbeat rate levels are 'null', '{ill, healthy}', 'in or out of certain scale',

'[10*HRate%10, 10*(HRate%10+1)]', 'full'. And the name of time levels are: 'null', 'Month', 'Week', 'Date', ' {AM, PM}', '{Morning, Afternoon, Night}', 'Hour', 'Minute'.

One example of mHealth K-anonymity privacy rule is in Fig.4. The watcher can access the mHealth presence only when the current mHealth of the target matches all the values specified in the child elements of this element

```
<cp:rule id="AA56i09">
<cp:conditions>
<cp:validity>
<cp:from>2010-03-01T00:00:00+01:00</cp:from>
<cp:until>2010-03-10T00:00:00+01:00</cp:until>
</cp:validity>
<mp:mhealth-kanonymity-condition>
<mp:A1>K-HeatbeatRate=2</mp:A1>
<mp:A2>K-Time=2</mp:A2>
<mp:A3>K-HRate-Time=2</mp:A3>
</mp:mhealth-kanonymity-condition>
</cp:conditions>
<cp:actions/>
<cp:transformations>
<gp:provide-mHealth-data/>
</cp:transformations>
</cp:rule>
```

Fig.4 mHealth K-anonymity Privacy Rule

4.2 Enhanced Privacy Filters:

Privacy filters are in charge of providing selective access of presence data. It is specified in the presence authorization rules. They specify actions and transformations for different parts of presence data. The example might be <relationship>, which indicates the availability of final presence data depends on relationship between the presentity and the watchers. The normal actions include sub-handling (deny or allow subscription request based on matched conditions), block (reject the subscription), confirm (put the subscription in the "pending" state), polite-block (place the subscription into the "accepted" state, but produce a presence document that indicates that the presentity is unavailable), and allow (accept the subscription).

The Incognito [19] privacy filter is introduced in order to fulfil the K-anonymity rule. It is a bottom-up breadth-first search on the domain generalization hierarchy. The algorithm generates the entire possible minimal k-anonymous presence attributes table for a given presence attributes table. First (iteration 1), it checks k-anonymity for every single attribute in presence attributes table, discarding those generalizations that do not satisfy k-anonymity for the single attribute. Then, it combines the remaining generalizations in pairs performing the same control on pairs of attributes (iteration 2); then in triples (iteration 3), and so on, until the whole set of attributes in presence attributes table is considered (iteration |presence attributes table|).

5. EXPERIMENT RESULT

The original presence is in the second and third column of Table 1. Suppose that the quasi-habit-identifier is QI= {Heartbeat Rate, Time}, and assume k=2. At iteration 1, Incognito privacy filter checks 2-anonymity on each single attribute, and finds that HRate3, HRate5, and all the time do not satisfy 2-anonymity. Thus, HRate3=110 and HRate5=60 are generalized based on the scales defined in the heartbeat rate level of K-anonymity rule. After they reach the scale 'in or out of certain scale', 2-anonymity for HRate is hold. With the similar procedure, Time attributes are also generalized. At iteration 2, the filter checks 2-anonymity on the pairs of

attributes <Heartbeat Rate, Time>. We can tell that no attributes pairs are 2-anonymous by the fact that each <Heartbeat Rate, Time> pair is distinguishable from other pairs. Incognito therefore proceeds the generalizations by scale up all time attributes to {AM, PM} and all HRate attributes to 'in or out of certain scale'. After this, 2-anonymity is hold for the whole presence attributes table.

Table 1. Presence Filtering Procedure

Index	Original Data		First Iteration		Second Iteration	
	HRate	Time	HRate	Time	HRate	Time
0	70	8:00	70	Morning	[70, 80]	AM
1	75	10:00	75	Morning	[70, 80]	AM
2	75	15:00	75	Afternoon	[70, 80]	PM
3	110	17:00	Out of [70, 80]	Afternoon	Out of [70, 80]	PM
4	70	21:00	70	Night	[70, 80]	PM
5	60	22:00	Out of [70, 80]	Night	Out of [70, 80]	PM

6. CONCLUSION

The overall aim of this paper is privacy protection of mHealth presence framework. Firstly, presence technology is applied to mHealth application. mHealth presence is proposed. XCAP is applied to the mHealth presence application for protecting privacy. It controls the direct privacy leakage. Secondly, mHealth presence privacy risks are analyzed. Indirect privacy leakages are prevented by improved presence authorization policy and privacy filter. Finally, k-anonymity privacy theory is used as the privacy protection model and privacy degree measurement.

However, K-anonymity is not enough for privacy protection from group privacy leakage and continuous query. Intuitively, a computation on a set of inputs is private if, for any of its input elements, the computation produces roughly the same result no matter this element is included in the input dataset or not. This will be our future works.

ACKNOWLEDGEMENTS

The author would like to thank Sensible Thing that Communicate (STC) for their founding and the members of sensor reality group for their help.

REFERENCES

[1] http://en.wikipedia.org/wiki/Presence_information

[2] C. Angeles: Distribution of context information using the session initiation protocol (SIP). Master Thesis, Royal Institute of Technology, Stockholm, Sweden (2008)

[3] Sergio Quintanilla Vidal: Context-aware Networks Design, Implementation and Evaluation of an Architecture and a Protocol for the Ambient Networks Project. Master Thesis, Linköping University, Linköping, Sweden (2006)

[4] J. Rosenberg. RFC4825 The Extensible Markup Language (XML) Configuration Access Protocol (XCAP). 2007.

[5] J. Rosenberg. Extensible Markup Language (XML) Formats for Representing Resource Lists . IETF RFC5025, May, 2007.

[6] M. Isomaki and E. Leppanen. An Extensible Markup Language (XML) Configuration Access Protocol (XCAP) Usage for Manipulating Presence Document Contents. IETF RFC4827, May, 2007.

[7] J. Rosenberg. Presence Authorization Rules. IETF RFC5025, December, 2007.

[8] R. Wishart, D. Corapi, A. Madhavapeddy, and M. Sloman. Privacy Butler: A personal privacy rights manager for online presence. In IEEE Percom Workshop on Smart Environments 2010, September 2010.

[9] G. Inc. (2010) Googlealerts. Last accessed 14th October, 2010. [Online]. Available: http:/www.google.com/alerts

[10] Patrice Godefroid , James D. Herbsleb , Lalita Jategaonkar Jagadeesany , Du Li, Ensuring privacy in presence awareness: an automated verification approach, Proceedings of the 2000 ACM conference on Computer supported cooperative work, p.59-68, December 2000, Philadelphia, Pennsylvania, United States.

[11] P. Godefroid. Model Checking for Programming Languages using VeriSoft. In ACM Symposium on Principles of Programming Languages, pages 174–186, January 1997.

[12] Landon P. Cox , Angela Dalton , Varun Marupadi, SmokeScreen: flexible privacy controls for presence-sharing, Proceedings of the 5th international conference on Mobile systems, applications and services, June 11-13, 2007, San Juan, Puerto Rico.

[13] http://www.media-art-online.org/wija/

[14] Loesing, K.; Dorsch, M.; Grote, M.; Hildebrandt, K.; Roglinger, M.; Sehr, M.; Wilms, C.; Wirtz, G.; , "Privacy-aware presence management in instant messaging systems," Parallel and Distributed Processing Symposium, 2006. IPDPS 2006. 20th International , vol., no., pp.8 pp., 25-29 April 2006

[15] T. Kanter, P. Osterberg, J. Walters, V. Kardeby, S. Forsstrom, and S. Pettersson. The mediasense framework. In 2009 Fourth International Conference on Digital Telecommunications, pages 144-147. IEEE, 2009.

[16] G. K. A. B. W. C. J. P. H. Sugano, S. Fujimoto. Presence Information Data Format (PIDF). RFC3863, August, 2004.

[17] P. K. J. R. H. Schulzrinne, V. Gurbani. RPID: Rich Presence Extensions to the Presence Information Data Format (PIDF). RFC4480, July, 2006.

[18] N. Li, N. Zhang, S. Das, and B. Thuraisingham. Privacy preservation in wireless sensor networks: A state-of-the-art survey. Ad Hoc Networks, 7(8):1501{1514, 2009.

[19] K. LeFevre, D. DeWitt, and R. Ramakrishnan. Incognito: Efficient full-domain k-anonymity. In Proceedings of the 2005 ACM SIGMOD international conference on Management of data, page 60. ACM, 2005.

[20] V. Ciriani, S. De Capitani di Vimercati, S. Foresti, and P. Samarati. k-anonymity. Secure Data Management in Decentralized Systems, 2007.

[21] L. Sweeney. k-anonymity: A model for protecting privacy. Int. J. Uncertain. Fuzziness Knowl.-Based Syst., 10(5):557–570, 2002.

[22] Ghinita, G., Kalnis, P., and Skiadopoulos, S.: PRIVE: Anonymous Location-based Queries in Distributed Mobile Systems. In: Proc. 16th Int'l World Wide Web Conf. (WWW '07), pp. 371-380. ACM, New York, NY, USA (2007)

[23] Bamba, B., Liu, L., Pesti, P., and Wang, T.: Supporting anonymous location queries in mobile environments with privacygrid. In: Proceedings of 17th International World Wide Web Conference (WWW2008), pp. 237–248. ACM, New York, NY, USA (2008)

[24] Chow, C., Mokbel, M. F., and Liu, X.: A peer-to-peer spatial cloaking algorithm for anonymous location-based service. In: Proceedings of the 14th annual ACM international symposium on Advances in geographic information systems, pp. 171-178. ACM, New York, NY, USA (2006)

[25] P. Samarati: Protecting respondents' identities in microdata release. In: IEEE Transactions on Knowledge and Data Engineering, vol. 13, pp. 1010–1027 (2001)

Xin Huang was born in China, 1982. He received the B.S. degree in software engineering from Xi'an Jiaotong University, Xi'an, China, in 2004. He received the MSc. degree in computer security from Royal Institute of Technology, Stockholm, Sweden, in 2006.He will get his Lic degree in December 2010 at at Mid Sweden University, Sundsvall, Sweden. He is currently working toward the PhD degree at University of Oxford, Oxford, UK. His current research interests include wireless sensor network application security.

Yang Jiang was born in China, 1988. He received the B.S. degree in communication engineering from Beijing Jiaotong University, Beijing, China, in 2009. He is currently working toward the Master degree at Mid Sweden University, Sundsvall, Sweden. His current research interests include cryptography, authentication, access control and security proofs.

Zuguang Liu was born in China, 1986. He received the B.S. degree in communication engineering from Beijing Jiaotong University, Beijing, China, in 2010. He is currently studying as an exchange student at Mid Sweden University, Sundsvall, Sweden. His current research interests include information security, cryptographic protocols, authentication and wireless security.

TheoKanter received his MSc in electrical engineering, cum laude, from the University of Advanced Technology, the Netherlands in 1976. He completed studies in computer science and artificial intelligence at the University of Technology in Linköping in Sweden (1986, 1987), before pursuing a technical doctorate in computer communications, which he earned from the Royal Institute of Technology in Stockholm, Sweden in 2001. During his career, Theo has held a number of leading positions in telecommunications research, earlier at Ellemtel AB, Sweden (1996-1999), where he led research in agent-based service architectures for context-aware voice service on the Internet and holds a number of patents in this area. Between 1999 and 2007, he was a senior scientist at Ericsson Research in the area of Service Layer Technologies focusing on Adaptive Mobile Services and Mobile Presence, contributing to standardization in the Open Mobile Alliance (OMA) and Third Generation Partnership Project (3GPP). From September 2007, Theo holds the position of full Professor of Computer Science – Distributed Systems within the Department of Information Technology and Media at the Mid-Sweden University.

Tingting Zhang received the B.Sc. degree, and M.Sc. degree in computer science and engineering from Fudan University, Shanghai, China in 1982 and 1984, respectively. During 1985-1987, she worked as a lecturer in Fudan University. She received the Ph.D. in computer science and engineering from Link ping University, Sweden in 1993. Since 1993, she has been a senior lecturer and now professor in Mid-Sweden University. Prof. T. Zhang is interested in distributed systems, digital TV broadcasting and application systems in artificial intelligence.