UPGRADE is the European Journal for the Informatics Professional, published bimonthly at <http://www.upgrade-cepis.org/>

Publisher
UPGRADE is published on behalf of CEPIS (Council of European Professional Informatics Societies, <http://www.cepis.org/>) by Novática <http://www.ati.es/novatica/>, journal of the Spanish CEPIS society ATI (*Asociación de Técnicos de Informática*, <http://www.ati.es/>)

UPGRADE monographs are also published in Spanish (full version printed; summary, abstracts and some articles online) by Novática

UPGRADE was created in October 2000 by CEPIS and was first published by Novática and INFORMATIK/INFORMATIQUE, bimonthly journal of SVI/FSI (Swiss Federation of Professional Informatics Societies, <http://www.svifsi.ch/>)

UPGRADE is the anchor point for UPENET (UPGRADE European NETwork), the network of CEPIS member societies' publications, that currently includes the following ones:
- InfoRewiew, magazine from the Serbian CEPIS society JISA
- Informatica, journal from the Slovenian CEPIS society SDI
- Informatik-Spektrum, journal published by Springer Verlag on behalf of the CEPIS societies GI, Germany, and SI, Switzerland
- ITNOW, magazine published by Oxford University Press on behalf of the British CEPIS society BCS
- Mondo Digitale, digital journal from the Italian CEPIS society AICA
- Novática, journal from the Spanish CEPIS society ATI
- OCG Journal, journal from the Austrian CEPIS society OCG
- Pliroforiki, journal from the Cyprus CEPIS society CCS
- Tölvumál, journal from the Icelandic CEPIS society ISIP

Editorial correspondence: Llorenç Pagés-Casas <pages@ati.es>
Advertising correspondence: <novatica@ati.es>

UPGRADE Newslist available at
<http://www.upgrade-cepis.org/pages/editinfo.html#newslist>

ISSN 1684-5285

Monograph of next issue (April 2010)

"Information Technology inTourism Industry"

(The full schedule of **UP**GRADE is available at our website)

CEPIS UPGRADE
The European Journal for the Informatics Professional
http://www.upgrade-cepis.org

Vol. XI, issue No. 1, February 2010

* This monograph will be also published in Spanish (full version printed; summary, abstracts, and some articles online) by **Novática**, journal of the Spanish CEPIS society ATI (*Asociación de Técnicos de Informática*) at <http://www.ati.es/novatica/>.

Digital Identity and Privacy in some New-Generation Information and Communication Technologies

Agustí Solanas, Josep Domingo-Ferrer, and Jordi Castellà-Roca

The use of the new information and communication technologies (ICT) has led to significant changes in the daily development of the information society. Although most of those changes tend to improve our lives, ICT can endanger some of our fundamental rights. In this article, we describe the threats related to the identity of ICT users, and we summarize the countermeasures that can be applied in three especially important areas: Internet search engines, vehicular networks, and location-based services.

Keywords: Digital Identity, Location-Based Services, Privacy, Search Engines, Vehicular Network,.

1 Introduction

The new information and communication technologies (ICT) have become progressively more important in our society. Mobile phones, vehicles with on-board computers, laptops and PDAs have become our inseparable partners in work and leisure.

The use of mobile communication networks is now commonplace. It is currently possible to retrieve information from virtually everywhere, at any time. Moreover, the significant increase of the information storage and processing capabilities of mobile devices gives rise to increasingly so-

Authors

Agustí Solanas received his BSc and MSc degrees in Computer Engineering from the *Universitat Rovira i Virgili* (URV), Tarragona, Spain, in 2002 and 2004, respectively, and his Diploma of Advanced Studies (Master) and PhD degrees with honours (cum laude) in Telematics Engineering from the *Universitat Politècnica de Catalunya*, Barcelona, Spain, in 2006 and 2007, respectively. He is currently a researcher with the CRISES Research Group and the United Nations Educational, Scientific, and Cultural Organization Chair in Data Privacy, and a tenure-track lecturer with the Department of Computer Science and Mathematics, URV. His fields of activity include data privacy, data security, and artificial intelligence, specifically clustering and evolutionary computation. He is a participant researcher in the Consolider Ingenio 2007 "ARES" project. He has also participated in several research projects funded by the Governments of Spain and Catalonia. He has authored over 60 publications and has delivered several talks. He has served as chair, programme committee member, and reviewer for several conferences and journals. <agusti.solanas@urv.cat>

Josep Domingo-Ferrer is a Full Professor of Computer Science and an ICREA-Acadèmia Researcher at *Universitat Rovira i Virgili*, Tarragona, Catalonia, where he holds the UNESCO Chair in Data Privacy. His research interests are in data privacy, data security and cryptographic protocols, with a focus on the reconciliation of individual privacy with corporate/national security. He earned his MSc and PhD degrees in Computer Science from the *Universitat Autònoma de Barcelona* in 1988 and 1991 (Outstanding Graduation Award). He also holds an M.Sc. in Mathematics. He has received four entrepreneurship awards and three research awards, among the latter the ICREA-Acadèmia 2008 Research Prize awarded by the Government of Catalonia. He has coordinated or served as principal researcher in R&D projects funded by the Catalonian government, the Spanish Government, the European Commission, the United States Bureau of the Census, and Cornell University. He currently coordinates the CONSOLIDER "ARES" team on security and privacy, one of Spain's 34 strongest research teams. He has chaired 9 international conferences and has served on the programme committee of 85 conferences on privacy and security. He is a co-editor-in-chief of "Transactions on Data Privacy" and an Associate Editor of three international journals. In 2004, he was a visiting fellow at Princeton University. <josep.domingo@urv.cat>

Jordi Castellà-Roca is a tenure-track lecturer at *Universitat Rovira i Virgili*, Tararagona, Spain, where he currently works with the UNESCO Chair in Data Privacy. He received his BSc in Computer Engineering from the *Universitat de Lleida*, Spain, in 1998, his MSc in Computer Engineering from *Universitat Rovira i Virgili* in 2000 and his PhD in Computer Science from the *Universitat Autònoma de Barcelona*, Spain, in 2005. His research focuses on cryptography (cryptographic protocols) and privacy. He has produced over 40 publications in international journals, book chapters, and international and national conferences. He is currently a member of the advisory board of an international journal, and he has been a member of the scientific and organization committees of several international conferences. He has participated in research projects funded by the Governments of Spain and Catalonia. He is the main researcher in two research projects funded by the *Universitat Rovira i Virgili* and one funded by the Spanish Ministry of Industry, Trade and Tourism. He has also participated in several technology transfer projects, and he is the author of six patents, five of them international and commercialized. He is a founding partner of three technology-based companies. <jordi.castella@urv.cat>

phisticated applications and services. It is common to use navigation systems that tell us how to reach a given destination in real time, to drive vehicles able to self-adapt to traffic conditions so as to improve their energy efficiency, and even to rely on intelligent systems that help us find the information we need more efficiently and rapidly.

Although ICT is a major advance that helps improve our productivity and efficiency, its massive use by non-expert users can endanger some of their fundamental rights such as privacy.

In this article we describe the main threats related to the identity of ICT users and the possible countermeasures that can be applied in three especially important areas. In Section 2 we consider the problems related to Internet search engines. Section 3 presents several ways of managing digital identities in vehicular networks. Section 4 describes the threats related to using location-based services. The article concludes in Section 5 with some final comments.

2 Identity Protection vs. Web Search Engines

Nowadays, almost 25% of the world's population has access to the global network, i.e. the Internet, and by the end of 2008 there were about 187 million web pages.

We cannot conceive of accessing this source of information without the help of web search engines (e.g. Google, Yahoo, Microsoft Live search, etc.). The essential mission of *web search engines* (WSEs) is to facilitate the search for information about one or several terms, providing a result list with links to web pages that have information about the searched terms.

Some studies show that 68% of users click on a search result in the first page of results, and 92% in the first three pages of search results. For this reason, web search engines will offer a better user experience if they place the links that are most interesting to users in the first result pages.

However, it is not easy to know what a user is interested in. The searched terms can have several meanings (ambiguous terms). For example, if we search "Mercury" we may refer to the planet of the solar system or the chemical element with atomic number 80. Every user will have their own interests, and they may change over time.

In the main WSEs, users do not collaborate with the WSE by sending their interests explicitly when they do a search. Thus, the WSE tries to obtain them using the browsing history, click-through data, web community information, or a client-side application, which stores users' interests. However, the most successful approach for web search engines is the use of queries previously submitted by the users in order to create user profiles.

In the literature, the process of improving the accuracy of the web search engines by profiling users is known as *personalized search* (PS) or *personalized web search* (PWS). While the use of profiles improves the users' experience, WSEs can use the users' profile to include advertising in the search results that ties in with the users' interests. It is reasonable to suppose that a good personalization will increase the number of users and, hence, profits from advertising.

Utilizing users' profiles can threaten users' privacy directly, because they contain information that can be considered private and personal. For example, if a certain user has searched for a certain place, it can be inferred that he or she lives there. If they look up a certain disease, it can be deduced that they (or someone close to them) suffers from that disease.

In 2006, 20 million queries made by 658,000 users of AOL were publicly disclosed; the company stated that queries were properly protected in order to avoid user identification. The New York Times journalists M. Barbaro and T. Zeller identified a user after studying those queries [1]. In [2], five levels of privacy protection are defined and analysed: *straightforward way, pseudo-identity, group identity, no identity and no personal information*.

2.1 The Straightforward Way

The first approach to provide anonymity is to prevent profile creation by using dynamic IP addresses and a controlled/clean web browser without cookies. However, this approach has the following drawbacks. The renewal policy of the dynamic IP address is not controlled by the user but by the network operator. This operator can always give the same IP address to the same Media Access Control (MAC) address.

Certain users require static IP addresses. Finally, a browser without cookies loses its usability in a large number of web applications. This situation may not be acceptable to certain users.

2.2 Pseudo-identity

In the pseudo-identity level, the user identity is replaced by a pseudo-identity. The WSE can create a profile associated to the pseudo-identity which contains less sensitive information. However, this level offers a low level of protection because queries still contain sensitive information that can be used to identify the real user. For example, AOL [1] replaced IP addresses with pseudo-identities in their query logs.

2.3 Group Identity

The third level of privacy corresponds to the group identity level. In this case, a group of users share a single identity. WSE are only able to build a group profile. They cannot profile single users. Thus, this mechanism improves the privacy protection but reduces the effectiveness of the service because personalized web searches are not accurate.

Nowadays, there are three ways to implement this level of privacy: i) using a proxy to construct the group; ii) using an obfuscation mechanism such as submitting random queries; and iii) sending queries which have been generated by other users.

The proxy does not solve the problem, but hands it over from the WSE to the proxy. The proxy can build individual profiles.

TrackMeNot [3] and GooPIR [4] submit random queries that introduce noise in the profiles of the users. Both

proposals are fast because they do not create groups. However, they have some drawbacks. TrackMeNot submits fake queries to WSEs when the users' activity is low. In this case, WSEs are able to sort all queries depending on whether they have been submitted during working hours.

Sending fake queries increases the network traffic and overloads the WSEs. GooPIR submits fake keywords to the WSEs together with the authentic one. This procedure does not overload the WSEs, but GooPIR requires a Thesaurus in order to decide which words can be added to the search. Accordingly, GooPIR can only submit keywords. Full sentences are not addressed because they cannot be formed by random keywords.

The proposals [5] and [6] provide a "group identity" by submitting queries generated by other users.

The system proposed in [5] uses memory sectors, which are shared by a group of users. When a user wants to send a query, they store their encrypted query in one of their memory sectors. If another user who shares that memory sector, wants to send a query, they find the query of the previous user and submit it to the WSE. When they obtain the answer, they store it in the same memory sector. The system uses an efficient procedure to create and share keys.

In [6] every time that *k* users want to submit a query a group is created, and they carry out a cryptographic protocol to obtain a query of another group member.

They do not know which query belongs to each user, thanks to the cryptographic protocol. Next, the users submit the queries to the WSE and forward the answers to the group. They obtain their answers in a reasonable time, and their profiles are obfuscated, hence preserving their privacy.

2.4 No Identity

In this level, either the identity of the user or the term searched is not available to the search engine.

Almost all the proposals that hide the user identity use an anonymous channel implementation. The Tor Project is an example of this. The main drawback of this approach is the response time which, on average, is 25 times slower than performing a direct search.

The proposals that hide the term searched from the WSE use Private Information Retrieval (PIR) schemes [7]. PIR schemes require the WSE to collaborate with the users. The database (DB) is usually modelled as a vector and the user wants to retrieve the value stored in the *i*-th position of the vector. These assumptions are not realistic because WSEs have no motivation for collaborating, their DBs are not vectors, and the user does not know where the WSEs store the information.

2.5 No Personal Information

In the no personal information level, neither the identity of the users nor the description of the data they desire is available to the WSE. This level provides the highest privacy protection to users. However, the computational and communication costs required by these mechanisms make them unusable in practice [2].

3 Identity Management in Vehicular Networks

Vehicular *ad hoc* networks (known as VANETs) is a technology that in the near future will enable communications between cars, and between cars and the traffic system.

The basic objective of VANETs is to improve traffic safety. To that end, the messages sent over this type of networks (e.g. warning of a nearby traffic jam, car accident or frozen road) must be trustworthy.

The self-organized nature of VANETs makes getting rid of false messages a non-trivial issue. The problem is further complicated by the privacy requirements of vehicles. Vehicles wish to remain anonymous and this makes them unidentifiable in the event of malicious behaviour. Several proposals can be found in the literature to reduce the number of false messages, which can be classified into two categories: *a posteriori* and *a priori* techniques. Both categories are similar as far as identity management is concerned.

3.1 *A Posteriori* Countermeasures

A *posteriori* countermeasures consist of punishing vehicles which have been proven to originate false messages. To make them compatible with privacy preservation, such countermeasures require a trusted third party able to open the identities of dishonest vehicles, which are thereafter excluded from the system.

This category of countermeasures relies on cryptographic authentication technologies. Some proposals use standard digital signatures [8][9][10][11] to enable malicious vehicles to be tracked.

To that end, a public-key infrastructure (PKI) is needed, which raises the problem of revocation. In [10] three revocation protocols are proposed for VANETs: revocation using compressed certificate revocation lists, revocation using a tamper-proof device and a distributed revocation protocol.

A critical issue in authentication of vehicular messages is the driver's privacy. Since the public key used to authenticate messages can be related to a specific user, an attacker may track vehicles by observing vehicular communications. Therefore, mechanisms should be adopted which guarantee the privacy of each vehicle/driver while allowing the rest of vehicles to authenticate messages.

This can be achieved either by using pseudonyms or group signatures. With the pseudonymous approach, the certification authorities (CAs) produce several pseudonyms for each vehicle, in such a way that the attackers cannot trace the vehicles producing signatures at different moments under different pseudonyms, except if the certification authorities open vehicle identities. The IEEE 1609.2 draft standard proposes distributing short-lived certificates to provide vehicles with privacy.

In [10], the use of a set of anonymous keys is proposed. These keys are frequently updated (e.g. every couple of minutes), at a frequency which depends on the driving speed. Each key can be used only once after which it expires, and only one key can be used at the same time.

The keys for a long period (for example one year, up to

the next annual vehicle service) are preloaded in a tamper-proof device (TPD) embedded in the vehicle. The TPD takes care of all operations related with key management. Each key is certified by the issuing CA and, with the help of the CAs, it is possible to determine the real identity of a vehicle if required by a judge.

There are several other works, which explore other aspects of pseudonyms. [12] recommends forcing a silence period to prevent a link being established between the various pseudonyms of the same vehicle. As an alternative, the creation of vehicle groups is suggested, in such a way that the vehicles from one group do not hear messages from other groups.

The conditional anonymity of pseudonymous authentication helps establish driver liability in the event of an accident. The drawback of this approach is the need to generate such pseudonyms ahead of time; that is, to generate, distribute, store and verify certificates for all pseudonymous public keys of each car. Group signatures would appear to be a solution to mitigate this problem.

In [13] a secure and privacy-preserving VANET protocol is presented which integrates group signatures and identity-based signatures (ID-based, whose public key does not need a certificate).

In order to provide security and privacy in car-to-car communication, a group signature is used, whereby messages are anonymously signed by senders, whose identities can be traced by the authorities if the sent message turns out to be false.

To provide security and privacy in car-to-infrastructure communication, the traffic infrastructure uses an ID-based signature to sign each message it generates and thereby ensure its authenticity. In this way, the burden of certificate management is greatly reduced.

3.2 *A Priori* Countermeasures

As a complement to *a posteriori* countermeasures, *a priori* countermeasures aim to thwart the generation of false messages. Most proposals in this category use a threshold, which will be denoted by *t*.

The idea is that, when a vehicle wants to send an announcement message informing of road conditions, it must get the message endorsed by at least *t* nearby vehicles. A message thus endorsed is thereafter broadcast over a mid- or long-range, in order to reach a large number of vehicles; in this broadcasting process, the cars act as repeaters. The underlying assumption is that there is a majority of honest vehicles, which endorse only true messages. The message generator as well as the endorsers must sign the message digitally, so that what was said in the previous section about signatures and certificates also applies here.

In particular, the process of generating and endorsing a message should not entail any privacy loss either for the generator or for the endorsers: if informing about traffic conditions discloses who is where, there will be little incentive to collaborate in the common good. The system [14] offers very efficient *a priori* countermeasures and guarantees the anonymity of generators and endorsers by means of secret sharing (partial signatures). The drawback of this system is that it provides irrevocable anonymity. In the recent paper [15], a system meeting all requirements is presented: *a priori* countermeasures are offered with security, privacy and revocable anonymity, and in addition the system permits the combination with *a posteriori* countermeasures.

4 Identity and Privacy Protection in LBS

The great development of mobile telephony has caused the appearance of multiple services for mobile devices users. To read the newspaper on-line, to check the stock markets in real time, or even to watch our favourite TV shows on our mobile phone are actions that have become commonplace. In addition, following the inclusion of global positioning systems (GPS) within mobile devices, location-based services (LBS) have gained importance and market share.

It is easy to list hundreds of situations in which having an information system based on the location of the user could be of great usefulness: determining where the closest pharmacy is, finding the best route to reach a given destination, retrieving information about buildings or monuments close to us, or locating gas stations located within 1 kilometre are examples of the variety of services that we can use on our mobile phones.

Beyond any shadow of a doubt such services are very useful. However, they can be a threat to the privacy and identity of users. In order to illustrate some of the threats that we have to face we will first consider two possible example scenarios; then, we will summarize some techniques that can be used to protect users, before concluding with a brief discussion about them.

4.1 Scenarios

We contextualize the threats to the identity and privacy of users related to location-based services by considering two illustrative situations.

4.1.1 A Fan of Italian Restaurants

Let us imagine a user (call him "Giorgio") who usually visits Italian restaurants. After enjoying a meal with abundant food and wine, Giorgio feels a bit disoriented and uses his mobile phone to contact a location-based service provider to retrieve information about the closest bus station to get back home.

Due to the fact that Giorgio is sending his real location to the location-based server, after repeating this action several times (remember that Giorgio is a frequent client of Italian restaurants), the LBS provider could easily infer that Giorgio is a fan of Italian restaurants. If this provider does not behave honestly, it can sell this information to a third party (e.g. a spammer) that will send Giorgio undesired "information" about Italian restaurants.

4.1.2 The Patient

Let us consider the case of a chronic patient (from now on, Dolores) who, due to her poor health, regularly has to

visit several doctors at different hospitals. Once Dolores leaves a hospital, she has to buy some new medicines. To that end, Dolores uses her mobile phone to contact a location-based service provider that shows her how to reach the closest pharmacy to her location. Note that if Dolores repeats this procedure several times, the LBS provider could determine that Dolores has some health problems (because she is always asking for pharmacies when she is located close to hospitals). If the provider misbehaves, it could sell this information to insurance companies which will be reluctant to accept Dolores as a new client.

4.2 Identity and Privacy Protection Techniques

In the above section we have considered two examples in which, due to the use of localization technologies, the privacy of the users is endangered. In the first example, the consumer habits of Giorgio have been discovered, whilst in the second, the poor health of Dolores has been revealed. A considerable number of methods have been proposed to prevent this privacy invasion. In the following sections we briefly describe the main proposals and we group them according to their use of trusted third parties (TTP) [16].

4.2.1 TTP-Based Methods

There are several methods based on trusting the LBS provider or intermediate entities. We go on to describe three of the main schemes.

Policy-based Methods

Policy-based methods are widely used. These methods assume that the provider is honest and adheres to a set of privacy policies previously agreed with the user. If an improper behaviour of the provider is detected, the user can take legal actions against the provider.

Pseudonym-based Methods

Pseudonym-based methods consider the addition of an intermediate entity between users and providers. This entity (known as "pseudonymizer") hides the real identity of users by using pseudonyms. The LBS provider can no longer analyze the behaviour of the client because his/her pseudonym is changed in each query. Notwithstanding, it is worth noting that pseudonymizers know the users and their queries, thus, users must trust them. It can be said that trust is handed over from providers to pseudonymizers [17].

k-Anonymity-based Methods

These methods, like the previous one, use an intermediate entity (an anonymizer) that distorts users' queries to assure k-anonymity (i.e. to assure that queries are undistinguishable from other *k-1* queries). Once the anonymizer has anonymized users' queries, they are sent to the provider. Note that the provider cannot determine which user sent each query because there are, at least, *k-1* other equal queries [18].

4.2.2 TTP-free Methods

TTP-based methods may raise concerns among users (remember that they have to trust intermediate entities and it is not always desirable to do that). Consequently, TTP-free methods have been proposed. In the following sections we describe some of the most relevant TTP-free proposals.

Obfuscation-based Methods

Obfuscation-based methods are based on the distortion of the real location information of the user prior to the sending of the query to the provider. This distortion is mainly achieved by adding random noise or by replacing the real location by approximate areas including the real location of the user. By doing so, the provider can no longer determine the exact location of users and, consequently, it becomes more difficult to infer information about them.

Collaboration-based methods

Collaboration-based methods try to achieve the same results as pseudonymizers and anonymizers by means of the collaboration of users rather than by using intermediate entities. A possible solution consists of sharing the location of *k* users so that it is possible to compute a common location (e.g. the average of the individual locations) or a shared clocking area that protects the privacy of all users against the provider. Note that, by collaborating, users can achieve privacy levels similar to the ones of anonymizers without using intermediate entities [19].

Private-information-retrieval-based Methods

Private information retrieval (PIR)-based methods allow users to obtain information from the database of the provider without revealing which information has been retrieved [20][21]. Although this proposal is very interesting from a theoretical point of view, it has serious practical problems due to its high computational costs. In addition, providers must collaborate with users to implement the PIR protocol, which does not seem to be a realistic scenario.

4.3 Discussion

In general, all the proposed methods could be used to improve the privacy of LBS users. However, using TTPs may be annoying to many users and, consequently, it seems reasonable to suppose that TTP-free proposals will gain importance in the near future.

Considering TTP-free techniques from a computational point of view, the simplest method is the one based on obfuscation because it requires neither collaboration nor complex protocols. Theoretically speaking, the most secure method is the one based on PIR, but would seem to be difficult to use it practically. Probably the methods that provide the best balance between cost and privacy are the collaboration-based ones.

5 Conclusions

In this article we have addressed some of the problems that can appear when ICT is used in three especially important areas: Internet, vehicular networks, and location-based

services.

It is important to emphasize that the use of ICT, while it is generally very beneficial, could endanger some fundamental rights such as privacy. Thus, it is necessary to investigate and develop systems and methods that allow users to utilize ICT securely and efficiently.

We have described some of the countermeasures that can be used to minimize the threats that users face. Nevertheless, it is necessary to keep studying and developing new systems to improve services and to reduce the identity and privacy threats suffered by ICT users.

Acknowledgement and Disclaimer

This work was partly supported by the Spanish Government through projects CONSOLIDER INGENIO 2010 CSD2007-00004 "ARES" and TSI2007-65406-C03-01 "E-AEGIS", and by the Government of Catalonia under grant 2009 SGR 1135. The second author is also partially supported as an ICREA-Acadèmia Researcher by the Government of Catalonia. The authors are members of the UNESCO Chair in Data Privacy but their views do not necessarily reflect UNESCO's opinion or position.

References

[1] M. Barbaro, T. Zeller. "A face is exposed for AOL searcher No 4417749". New York Times, August 2006.

[2] X. Shen, B. Tan, C.X. Zhai. "Privacy Protection in Personalized Search". ACM SIGIR Forum, vol. 41, no. 1, pp. 4-17, 2007.

[3] D. C. Howe, H. Nissenbaum. "TrackMeNot: Resisting surveillance in web search". En Lessons from the Identity Trail: Privacy, Anonymity and Identity in a Networked Society. I. Kerr, V. Steeves and C. Lucock (eds.). Oxford University Press, Oxford UK, 2009 (in press).

[4] J. Domingo-Ferrer, A. Solanas, J. Castellà-Roca. "h(k)-Private Information Retrieval from Privacy-Uncooperative Queryable Databases". Journal of Online Information Review, vol. 33, no. 4, pp. 1468-4527, 2009.

[5] J. Domingo-Ferrer, M. Bras-Amorós, Q. Wu, J. Manjón. "User-Private Information Retrieval Based on a Peer-to-Peer Community", Data and Knowledge Engineering (in press).

[6] J. Castellà-Roca, A. Viejo, J. Herrera-Joancomartí. "Preserving user's privacy in web search engines". Computer Communications, vol. 32, no. 13–14, pp. 1541–1551, 2009.

[7] B. Chor, O. Goldreich, E. Kushilevitz, M. Sudan. "Private information retrieval". IEEE Symposium on Foundations of Computer Science – FOCS, pp. 41-50, 1995.

[8] F. Armknecht, A. Festag, D. Westhoff.K. Zeng. "Cross-layer privacy enhancement and non-repudiation in vehicular communication". 4th Workshop on Mobile Ad-Hoc Networks (WMAN), Berna, Switzerland, March 2007.

[9] M. Raya, J.-P. Hubaux. "Securing vehicular ad hoc networks". Journal of Computer Security (special issue on Security of Ad Hoc and Sensor Networks), vol. 15, no. 1, pp. 39-68, 2007.

[10] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, J.-P. Hubaux. "Eviction of misbehaving and faulty nodes in vehicular networks". IEEE Journal on Selected Areas in Communications, vol. 25, no. 8, pp. 1557-1568, 2007.

[11] M. Raya, P. Papadimitratos, J.-P. Hubaux. "Securing vehicular communications". IEEE Wireless Communications Magazine, vol. 13, no. 5, pp. 8-15, 2006.

[12] K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura, K. Sezaki. "CARAVAN: Providing Location Privacy for VANET". Proceedings of Embedded Security in Cars, ESCAR 2005, November 2005.

[13] X. Lin, X. Sun, P.-H. Ho, X. Shen. "GSIS: A secure and privacy preserving protocol for vehicular communications". IEEE Transactions on Vehicular Technology, vol. 56, no. 6, pp. 3442-3456, 2007.

[14] V. Daza, J. Domingo-Ferrer, F. Sebé, A. Viejo. "Trustworthy privacy-preserving car-generated announcements in vehicular ad hoc networks". IEEE Transactions on Vehicular Technology, vol. 58, no. 4, pp. 1876-1886, 2009.

[15] Q. Wu, J. Domingo-Ferrer, Ú. González-Nicolás. "Balanced trustworthiness, and privacy in vehicle-to-vehicle Communications". IEEE Transactions on Vehicular Technology (in press).

[16] A. Solanas, J. Domingo-Ferrer, A. Martínez-Ballesté. "Location privacy in location-based services: Beyond TTP-based schemes". Proceedings of the 1st International Workshop on Privacy in Location-Based Applications (PILBA), pp. 12-23. Málaga, España, October 2008.

[17] P. A. Pérez-Martínez, A. Solanas. "Location Privacy Through Users' Collaboration: A Distributed Pseudonymizer". Proceedings of the Third International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies. UBICOMM 2009, pp. 338-341. Sliema, Malta, 11-16 October, 2009.

[18] B. Gedik, L. Liu. "Protecting Location Privacy with Personalized k-Anonymity: Architecture and Algorithms". IEEE Transactions on Mobile Computing vol. 7, no. 1 pp. 1-18, January 2008.

[19] A. Solanas, A. Martínez-Ballesté. "A TTP-Free Protocol for Location Privacy in Location-Based Services". Computer Communications, 31(6), pp. 1181–1191, 2008.

[20] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, K. Tan. "Private queries in location based services: Anonymizers are not necessary". SIGMOD '08: Proceedings of the 2008 ACM SIGMOD international conference on Management of data, Vancouver, BC, Canada, pp. 121–132, June 2008.

[21] G. Ghinita, "Private queries and trajectory anonymization: a dual perspective on location privacy". *Transactions on Data Privacy*, vol. 2, no. 1, pp 3-19, 2009.