Enhancing Privacy-Preserving Access Control for Pervasive Computing Environments

Emmanouil Magkos and Panayiotis Kotzanikolaou

[1] Department of Informatics, Ionian University,
Plateia Tsirigoti 7, Corfu, Greece, 49100,
emagos@ionio.gr
[2] Department of Informatics, University of Piraeus,
80, Karaoli-Dimitriou, 18534, Piraeus, Greece,
pkotzani@unipi.gr

Abstract. The exchange of user-related sensitive data within a Pervasive Computing Environment (PCE) raises security and privacy concerns. On one hand, service providers require user authentication and authorization prior to the provision of a service, while at the same time users require anonymity, *i.e.*, untraceability and unlinkability for their transactions. In this paper we discuss privacy and security requirements for access control in PCEs and show why a recently proposed efficient scheme [1] fails to satisfy these requirements. Furthermore, we discuss a generic approach for achieving a desired level of privacy against malicious insiders, while balancing with competing demands for access control and accountability.

Key words: Privacy and Security, Pervasive Computing Environments, Unlinkability, Accountability

1 Introduction

The integration of computing and communication into a mobile and dynamic environment is seen as one of the most exciting aspects of the not so far future. Within a *Pervasive Computing Environment* (PCE), a typical scenario involves mobile users equipped with low-cost handheld devices with limited computing, storage and communication capabilities. These devices enable mobile users to have seamless access to value-added services, anytime and anywhere [2], typically by connecting to wireless access points. Due to the unique characteristics of the dynamic PCE environment, such as the looseness of physical boundaries and the ad-hoc interaction with devices of undefined trust, security will naturally be required as an inherent property by consumers, companies and organizations. Security issues involve message and entity authentication, access control, confidentiality and integrity protection of the communication channel [3, 4].

The protection of personal and sensitive data such as identity and location information is also seen as an important criterion for large-scale deployment of PCEs [3, 5, 6]. With the advent of pervasive devices and technologies (*e.g.*, wireless sensors, fusion, RFIDs), individuals are wary of "Big Brother" technologies,

that monitor their transactions without their consent [7, 8]. For example, the identity of a user that participates in a supposedly anonymous transaction may be traced back, or different transactions between the system and the user may be linked in order to build a profile.

Clearly, there is an inherent tradeoff between *privacy and access control* in PCEs [9, 10]. Indeed, from the point of view of a user, no one should be able to: (a) trace the real identity of the user, (b) link different sessions between the user and the system, (c) obtain context information (location, time and duration, type of service etc). On the other hand, the need for access control is threefold. Service providers may need message, entity or context authentication [11] in order to: (a) authorize access to a service (*e.g.*, to prevent abuse, or for billing purposes), (b) provide personalized, context-aware services, (c) trace back an identity for accountability or liability (*e.g.*, service abuse, privilege revocation, unlawful acts).

To balance this tradeoff, it has been proposed that anonymity in PCEs should be *conditional*, *i.e.* under well-defined conditions the real identity of a user should be exposed. In addition, given the pervasiveness of resource-constrained devices, security mechanisms should be efficient in terms of storage, communication and computation. As a result, access control with privacy preservation in PCEs is still an open research area [12, 3, 5, 13, 7, 14, 1].

Our Contribution In this paper we discuss privacy and security requirements for PCEs and show how a recently proposed efficient solution fails to satisfy these requirements. Specifically we review the recent scheme proposed by Ren and Lou [1], hereinafter called the *RL scheme*, which has been recognized as the first attempt to provide a secure model for privacy-preserving access control in PCEs. We discuss how the RL scheme fails to satisfy the unlinkability and untraceability criteria, and show that the (claimed) accountability and non-repudiation assurances of the scheme are weak. To enhance privacy, we discuss a generic scheme for privacy-preserving access control in PCEs, aiming to achieve a desired level of privacy against malicious insiders (users, front-end and back-end entities), while balancing with competing demands for access control and accountability.

2 Design and security requirements

2.1 System model

Our model extends the system model of [1] to support a typical scenario where a mobile user is able to dynamically access a service among a list of available service types. The system entities are users, front-end entities, and back-end authorities:

– *Users* equipped with hand-held devices request access to different kinds of services at anytime and from anywhere.

– *Front-end entities* are typically wireless access points (AP) that handle the communication with the user, collect the service request messages and mediate between the user and a back-end authority.
– *Back-end authorities* involve application Service Provider(s) (SP), an authentication server (AS), and occasionally a Trusted Third Party (TTP). The task of the SP and the AS is to control access and provide the service data. For simplicity we will assume that the SP will also act as an AS. The TTP is usually an offline authority that is invoked in exceptional circumstances (*e.g.*, dispute resolution, anonymity revocation).

2.2 Threat model

We model our adversary as a global passive observer that monitors all communications within the network to extract private information. This information may be used to link past and future message exchanges in order to track and/or trace users. The adversary may also compromise APs and/or the SP(s), and extract their logs in order to facilitate tracking/tracing, or in order to steal user credentials. The adversary will also attempt to modify messages in transit, or replay past messages in order to impersonate a user or disrupt the network. All components of the network (the users, the AP(s), and the SP(s)), including the adversary, are modeled by probabilistic, polynomial-time Turing machines.

We assume that the adversary will not try to exploit any weaknesses in the underlying algorithms for public key and symmetric key cryptography. In addition, we assume the communication channel between the APs and the SP(s) to be secure. Finally, as in [1] we assume that users are capable of manipulating the source address of layer 2 (MAC) frames, or else untraceability and unlinkability are trivially defeated at the access point.

2.3 Privacy versus security

At a minimum, communication between a user and the system in a PCE should be mutually authenticated, and its confidentiality and integrity protected. Furthermore, we emphasize on two subtle aspects of privacy in PCEs:

– *Untraceability*: No unauthorized entity, or a reasonably-sized coalition of unauthorized entities should be able to trace the real identity of the user, unless the user has explicitly permitted it.
– *Unlinkability* (also known as *tracking protection*): it should not be possible[1] for internal (users, APs, SPs) or external entities, to link different sessions of the same user, unless otherwise stated by the systems's policy.

Untraceability by itself is not enough for privacy in PCEs. If a set of distinct, authorized credentials can be linked to the same anonymous entity, then a customer profile can be built and this is considered a privacy violation. In this case,

[1] Of course, as also noted in [15], anonymity-protected communications are unlinkable as long as application content does not enable linkage.

and in order to completely undermine privacy, the adversary will only have to trace one particular link of this chain (*e.g.*, after the customer uses a credit card, with use of a camera, physical pursuit etc). As a result, unlinkability protection is also crucial for privacy preservation. Compared to other models (*e.g.*, [9, 1]), our requirement for unlinkability is *privacy-enhanced*: the unlinkability of a user's transactions needs to be protected not only from outsiders, but also from malicious insiders (for example, rogue APs or SPs).

From a security point of view, if user access is completely anonymous, service providers may worry about possible service abuse. For example, malicious users may attempt to access a service with stolen credentials. In such cases a user may be challenged by the system to prove the validity of a specific credential. This process was defined as *dispute resolution* in [1]. To balance with privacy, we require that at the end of dispute resolution, the SP must not be able to link other credentials to the disputed credential, or trace the identity of the user.

In addition, there are cases where the anonymity of a specific credential must be revoked and a real identity be traced, in order to establish *accountability*. For example, in case of service abuse/misuse, when the SP suspects that a user is potentially illegal (*e.g.*, the SP may observe some abnormal access pattern of the user) or when a credential is linked to an unlawful act. To balance with privacy, the goal is the provision of *conditional untraceability* where the protection of the link between a specific credential and an identity will be broken under well defined conditions. Typically, anonymity revocation will be an off-line protocol, where a SP and/or a TTP, given a credential and transaction information, are able to trace the real identity of the owner of the credential.

3 Related work

A number of aspects for security and privacy preservation in pervasive environments have been investigated by recent research –see for example [4, 7] for general security requirements and challenges, [3] for privacy definitions, [6] for a survey of privacy enhancing technologies.

The privacy vs access control tradeoff has also been explored in the literature [16, 17] and particularly in the context of wireless mesh networks (*e.g.*, [18, 19, 20, 21]), where it was suggested that a long list of short-lived pseudonyms is generated during registration in such a way that the pseudonyms cannot be linked to each other by non-authorized entities. However, as noted in the literature, the use of independent pseudonyms is not always a panacea [5, 18]. For example, changing identity does not guarantee unlinkability in telematics or indoor PCEs, where a global adversary has access to context (*e.g.*, spatiotemporal) information and performs traffic analysis against a mobile user. Another possible scenario is when the user is tracked down through a unique set of preferences for a specific service. From our point of view the latter is more related to PCEs, where the device interaction is transient and ad-hoc in nature and the traffic emitted by a user is not as periodic and frequent as in MANETs.

The preservation of context privacy in pervasive environments has also been explored in some recent works (*e.g.*, [5, 8, 22], also refer to [23] for a survey). For example in [5] the concept of a MIX zone was proposed, based on Chaum's mix network [24], in order to hide the identity of a user belonging to a group of users with similar characteristics. In this paper, we consider works of the above category, as well as some recent proposals on machine readable privacy policies (*e.g.*, [25, 22]) for controlling the information that is revealed to a third party, or on anonymizing the communication channel (*e.g.*, the Mist routing project [3]) as rather orthogonal to our work.

Recently, a number of security protocols for privacy-preserving access control in PCEs have been proposed [9, 26, 1, 10, 27, 28]. A representative scheme of this category is the RL scheme [1], which was the first attempt to provide a secure communication model for privacy-preserving access control in PCEs. The RL scheme uses blind signatures [29] and hash chains [30] at the application layer in order to provide mutual authentication while preserving privacy against malicious outsiders. In [27, 28] the RL scheme is tweaked to increase performance while in [28], an impersonation attack against the RL scheme was described and addressed. Finally, the work in [10] where non-unique temporal IDs are issued by the access point to system users, achieves authentication and unlikability against back-end authorities, but fails to establish accountability and untraceability against front-end entities.

4 Reviewing the RL scheme

The RL scheme [1] is a set of protocols executed between a Service Provider (SP) and a mobile user (*e.g.*, Alice) that communicate via an access point (AP). The (claimed) basic security services in [1] are: mutual authentication, anonymity, unlinkability, non-repudiation, and accountability. We recall the two distinct phases of the protocol (see also figure 1), while avoiding a few (non-crucial) details and slightly changing the notation.

User registration. Alice registers as a legal user, obtains an authentic public-key certificate $Cert_A$ for her real identity, and the public key(s) of the service(s) she is entitled to use. In Step 1 and for a specific service SID, Alice computes the anchor value C^0 and the end value of the credential chain as $C^n = H^n(C_0)$, where H^n denotes a hashing operation H that is performed n times (*i.e.*, for n future service accesses). Then, Alice prepares a blinded version of C^n as $C_A = \{r'_A\}_{PK_{SID}} \times C^n$, where r'_A is a random nonce and $\{\}_{PK_{SID}}$ denotes encryption with the public key of service SID. Alice submits C_A, her (real) identity A and public key certificate $CERT_A$, together with SID, to the SP. In Step 2, the SP verifies that Alice is an eligible user for the service identifier SID and then signs C_A with the private signature key of the service SID. The SP sends the blindly signed message to Alice, who unblinds it, in Step 3, by dividing with r'_A. In order to access different service types, Alice may generate and authorize several different credential chains.

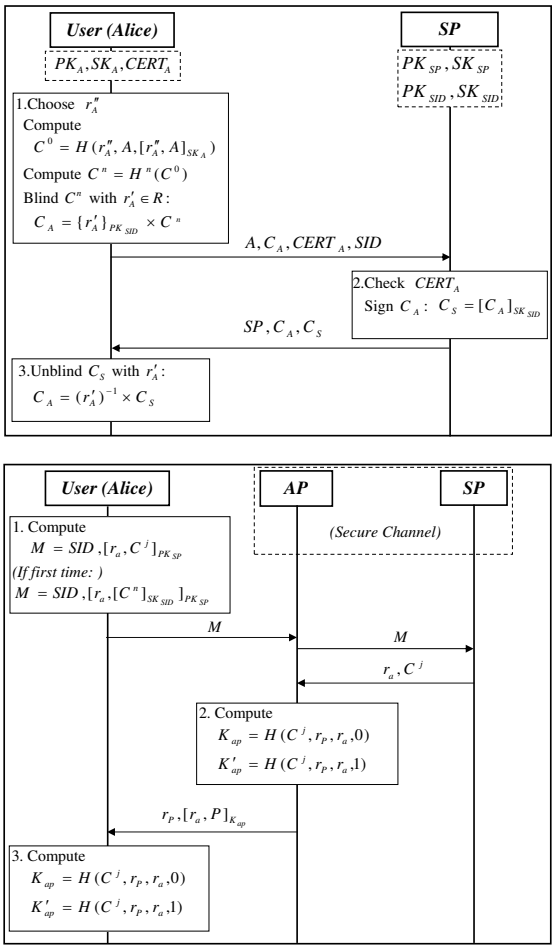

Fig. 1. The registration and user access phases of the Ren & Lou scheme

Service access. This phase is run between Alice, an Access Point (AP) and the Service Provider (SP), and can be viewed as the execution of two different sub-protocols:

1. The first sub-protocol achieves mutual entity authentication between Alice and the SP, mediated by the AP who just relays messages: Alice chooses a challenge r_a, concatenates with a credential C^j, where $1 < j \leq n-1$, encrypts them with the public key PK_{SP} of the SP, and sends the result, together with the service SID, to the SP, via the AP. The SP decrypts, uses hash chain verification to check whether C^j is a fresh, valid credential for the specific service type, and returns r_a and C^j to the AP. The AP will use them in the sequel to agree a session key with Alice.

2. The second sub-protocol achieves authenticated key agreement between Alice and the AP, with implicit key authentication. The AP chooses a random challenge r_p, and computes two session keys for encryption and message authentication, namely $K_{ap} = H(C^j, r_p, r_a, 0)$ and $K'_{ap} = H(C^j, r_p, r_a, 1)$. The AP symmetrically encrypts r_a and its identity P with K_{ap} and sends $r_p, [r_a, P]_{K_{ap}}$ to Alice. After this point, communication between Alice and the AP will be encrypted and authenticated with keys K_{ap} and K'_{ap}.

Dispute resolution. To deal with situations where a credential C^j gets compromised or stolen, the authors in [1] suggest that the anchor value contains a message that is digitally signed with Alice's private key SK_A. That is, $C_0 = H(r''_a, A, \{A, r''_a\}_{SK_A})$, where r''_a is a fresh nonce selected by Alice during registration, and A is her identity. Then, in case of a dispute, a resolution protocol is run between a TTP, the SP and Alice. The SP presents the TTP with the disputed credential and the real Alice will reveal to the TTP a valid pre-image value of C_0, *i.e.*, her authentic signature on the nonce r''_a. The claimed property for the above enhancement is *non-repudiation* for the system users [1].

4.1 Weaknesses of the RL scheme

We will discuss how the RL scheme fails to satisfy the unlinkability and untraceability criteria, within our threat model. Then we will show that the (claimed) accountability and non-repudiation assurances of the RL scheme are weak.

Tracking by front-end entities. The remarks below also apply to [9, 27, 28]. The scheme in [1], does not provide unlinkability against front-end system entities. Indeed, assume that the access point AP sees[2] an authorized credential C^j of Alice for the epoch j. At some future epoch i, where $i > j$, Alice uses AP to access the same service using the anonymous credential C^i. If AP keeps a database of authorized credentials, it will effectively link the two transactions by performing $j - i$ hashing operations. Similarly, two or more cooperating APs will be able to jointly link some or all of Alice's transactions.

Tracking by back-end authorities. The scheme in [1], does not provide unlinkability against back-end system entities. Indeed, the SP will be able to link all transactions for all services that it offers, by efficiently performing hashing operations on the authorized credentials and checking whether there is a match with any value stored in its database.

Tracking and tracing after dispute resolution. During dispute resolution for a challenged credential C^j, Alice reveals the anchor value C_0 and proves her real identity by digitally signing a unique message. The side-effect is that the TTP will be able not only to trace Alice's identity but also to re-construct all components C^j, $0 \leq j \leq n-1$, of the hash chain of credentials. This information

[2] This attack assumes that the AP has application-level capabilities. Typically, a compromised AP will forward traffic data to a capable adversary.

may be used to link and trace Alice's past and future transactions for a given service, not only the disputed one. Although in [1] the TTP is assumed to be trusted, we believe that security should be based on less strong assumptions.

Non-repudiation and accountability. In [1] it is claimed that the dispute resolution sub-protocol establishes non-repudiation for a disputed transaction, since users, when challenged by the TTP, generate an authentic signature on a random nonce, and this signature is securely linked to the challenged credential chain. We argue that this perception of non-repudiation is wrong. First of all, it is true that dispute resolution will expose[3] an adversary that has stolen a credential from a valid user. However, it also true that any adversary, whether a valid system user or an outsider who has stolen some credentials, will avoid to participate in the dispute resolution protocol. The same argument will also hold for any valid user, who used an authentic credential during a transaction, but for some reason chooses to falsely deny participation in this transaction or in other, past transactions. In this way, non-repudiation is not achieved in the RL protocol.

Finally, the (claimed) property of accountability is also not supported in the RL scheme. There is not a way for the SP and/or the TTP, when they are given a specific credential and transaction information, to work off-line and trace the real identity of the owner of the credential.

5 A privacy-preserving access control protocol for PCEs

We propose a generic scheme for privacy-preserving access control in PCEs. Our motive is the need to enhance privacy by achieving unlinkability against malicious insiders and enhance security by achieving conditional traceability of user credentials. We present an approach that is based on lists of short-lived, uncorrelated pseudonyms, in order to enhance unlinkability for the user. Specifically any handheld device A is installed with a list of anonymous public/private signature key pairs (PK_j, SK_j) for multiple service accesses, where $1 \leq j \leq n$, together with the corresponding certificates $CERT_j$. In order to provide conditional traceability and accountability, we propose the engagement of a Trusted Party TTP, during the user registration. Bellow we describe the registration and the user access protocols. The protocols are depicted in figure 2.

5.1 User registration

Each user will participate in the registration protocol with the TTP, in order to issue its anonymous public key certificates. In order to minimize the cost of user authentication during the user access protocol, our approach combines both public-key and symmetric-key credentials. Specifically, the user will generate n independent random binary strings $h_j, j \in [1, n]$ of bounded length[4] that will be

[3] Of course, if the adversary has stolen *all* of the user's secrets –including her signature keys– then he will always be able to impersonate her.

[4] For example $|h_j| = 128$ bit

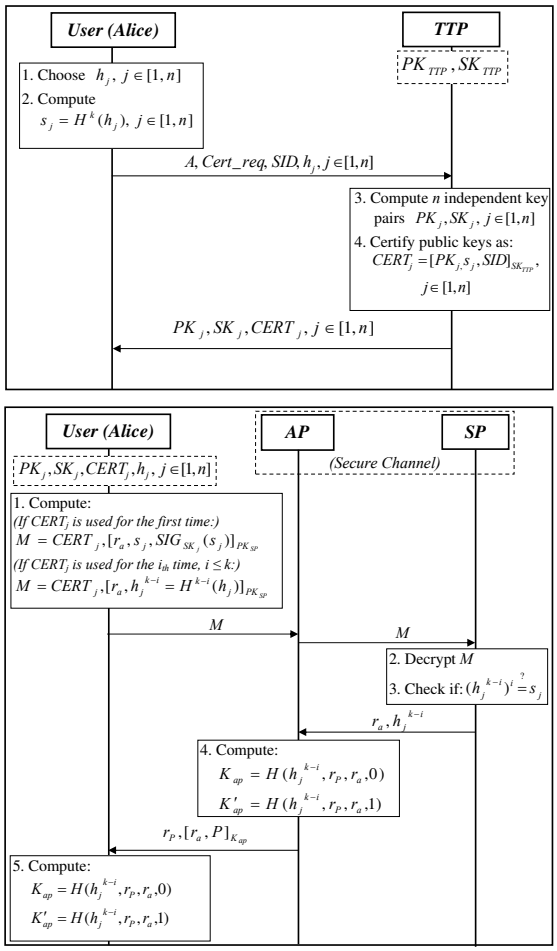

Fig. 2. The registration and user access phases of the proposed scheme

used as seeds of hash chains, one for each corresponding public/private key pair. Also the user will compute for each value h_j the k-th element of each hash chain, i.e., $s_j = H^k(h_j),\ \ j \in [1,n]$ are the anchor values of each random seed. Then, the user will send a certificate request to the TTP, along with its real identifier A, the service id SID, the random seeds h_j and the parameter k.

After the TTP has authenticated the user, it will generate n independent public/private key pairs PK_j, SK_j. These keys will then be certified. Each anonymous user certificate $CERT_j$ will contain the public key PK_j, the anchor value s_j (this is computed by the TTP as the k-th element of the hash chain on h_j) and the service identified SID. At the end of the protocol, the user will be employed with the credentials $PK_j, SK_j, CERT_j$, which can be used at maximum for $n \times k$ user accesses. The credentials can be distributed to the handheld devices either *statically* or *dynamically*. In the static mode [18] a number of credentials

are pre-loaded to a device offline *e.g.*, by the TTP. In the dynamic mode, the key pairs are updated by executing an online protocol between the device and a TTP periodically or when needed [31]. Each pair of keys has a (relatively) short life time, depending on the desired privacy level. Without loss of generality, we assume that a new pair is used at the beginning of each new transaction with the SP for service access.

5.2 User access

In order to access a service with identifier SID, the user will use an anonymous certificate issued by the TTP for that service, say $CERT_j$. The user will choose a random nonce r_a. If $CERT_j$ is used for the first time, the user will compute a signature on the anchor value s_j with the private key SK_j. If the certificate is used for the i-th time ($i \leq k$), then the user will compute the value $h_j^{k-i} = H^{k-i}(h_j)$. The user encrypts this with the public key of the SP and sends it to the SP via the access point AP, along with the corresponding anonymous certificate. The SP will decrypt the message, verify the signature (for the first use) and check whether $(h_j^{k-i})^i = s_j$. If the verification is successful, the SP will forward h_j^{k-i} and r_a to the AP. Then the AP will choose a nonce r_p and both the user and the AP will compute the common keys K_{ap} and K'_{ap}, as shown in figure 2.

5.3 Protocol analysis

The proposed protocol preserves all the security properties of the RL scheme and furthermore extends the untraceability and the accountability properties. Within the proposed scheme a malicious SP (and AP), will not be able to link different transactions of the same user, if different anonymous certificates are used for different transactions. In the RL scheme, a malicious SP or AP can link user transactions if it maintains the user credentials, since the credentials of a particular user will resolve to the same anchor value. Of course in the proposed scheme, if a user uses the same anonymous certificate in one SP for multiple times, then the unlinkability of the scheme is lost.

The use of the TTP also improves the accountability of system users. Indeed, if a user must be set accountable for a transaction, the TTP can be employed in order to reveal the real identity of the user. For conditional traceability, all exchanged messages can be traced, under (assumingly) well-defined conditions, to their sender. Indeed, the SP may submit a set of transaction data to the TTP, who will look up in the database for matching between an anonymous public key certificate and the real identity of a handheld device (user).

The tradeoff for the privacy enhancements offered by the proposed scheme is the increased storage cost for the user. In comparison with the RL scheme, in the proposed scheme the user must store n instead of one public key credentials and also the corresponding n anonymous certificates. Finally, the proposed scheme requires the active involvement of a TTP during the registration phase. Note however that the TTP is off-line during the user access phase.

6 Conclusions

Achieving privacy and access control in PCEs is a hard problem, with a range of challenges to be addressed. In this paper we defined a threat model as well as requirements for enhanced privacy and security in controlling access to pervasive computing environments. We reviewed the related work on the subject and shown that a recent scheme, the RL scheme has privacy and security vulnerabilities under our threat model. Finally, we described a generic scheme for privacy-preserving access control in PCEs.

References

1. Ren, K., Lou, W.: Privacy-enhanced, attack-resilient access control in pervasive computing environments with optional context authentication capability. Mobile Networks and Applications **12** (2007) 79–92
2. Weiser, M.: The computer for the 21st century. ACM SIGMOBILE Mobile Computing and Communications Review **3** (1999) 3–11
3. Al-Muhtadi, J., Campbell, R., Kapadia, A., Mickunas, M., Yi, S.: Routing through the mist: privacy preserving communication in ubiquitous computing environments. In: 22nd International Conference on Distributed Computing Systems, IEEE (2002) 74–83
4. Campbell, R.H., Al-Muhtadi, J., Naldurg, P., Sampemane, G., Mickunas, M.D.: Towards security and privacy for pervasive computing. In: ISSS International Symposium on Software Security. (2002) 1–15
5. Beresford, A., Stajano, F.: Location privacy in pervasive computing. Pervasive Computing, IEEE **2** (2003) 46–55
6. Ackerman, M.S.: Privacy in pervasive environments: next generation labeling protocols. Personal Ubiquitous Comput. **8** (2004) 430–439
7. Ranganathan, K.: Trustworthy pervasive computing: The hard security problems. In: PERCOMW '04: Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops, Washington, DC, USA, IEEE Computer Society (2004) 117
8. Gorlach, A., Heinemann, A., Terpstra, W.W.: Survey on location privacy in pervasive computing. In Robinson, P., Vogt, H., Wagealla, W., eds.: Privacy, Security and Trust within the Context of Pervasive Computing. The Kluwer International Series in Engineering and Computer Science (2004)
9. Ren, K., Lou, W., Kim, K., Deng, R.: A novel privacy preserving authentication and access control scheme for pervasive computing environments. Vehicular Technology, IEEE Transactions on **55** (2006) 1373–1384
10. Diep, N.N., Lee, S., Lee, Y.K., Lee, H.: A privacy preserving access control scheme using anonymous identification for ubiquitous environments. In: RTCSA '07: Proceedings of the 13th IEEE International Conference on Embedded and Real-Time Computing Systems and Applications, Washington, DC, USA, IEEE Computer Society (2007) 482–487
11. Creese, S., Goldsmith, M., Roscoe, B., Zakiuddin, I.: Authentication for pervasive computing. In: SPC. (2003) 116–129
12. Langheinrich, M.: Privacy by design - principles of privacy-aware ubiquitous systems. In: UbiComp '01: Proceedings of the 3rd international conference on Ubiquitous Computing, London, UK, Springer-Verlag (2001) 273–291

13. Chan, H., Perrig, A.: Security and privacy in sensor networks. Computer **36** (2003) 103–105
14. Juels, A.: Rfid security and privacy: a research survey. Selected Areas in Communications, IEEE Journal on **24** (2006) 381–394
15. Stubblebine, S.G., Syverson, P.F., Goldschlag, D.M.: Unlinkable serial transactions: protocols and applications. ACM Trans. Inf. Syst. Secur. **2** (1999) 354–389
16. Jakobsson, B.M.: Privacy vs. authenticity. PhD thesis, La Jolla, CA, USA (1998)
17. Bangerter, E., Camenisch, J., Lysyanskaya, A.: A cryptographic framework for the controlled release of certified data. In: Security Protocols Workshop. (2004) 20–42
18. Raya, M., Hubaux, J.P.: The security of vehicular ad hoc networks. In: SASN '05: Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks, New York, NY, USA, ACM (2005) 11–21
19. Rahman, S., Hengartner, U.: Secure crash reporting in vehicular ad hoc networks. In: Third International Conference on Security and Privacy in Communication Networks (SecureComm 2007), New York, NY, USA, To appear (2007)
20. Sun, J., Zhang, C., Fang, Y.: An id-based framework achieving privacy and non-repudiation in vehicular ad hoc networks. Military Communications Conference, 2007. MILCOM 2007. IEEE (29-31 Oct. 2007) 1–7
21. Burmester, M., Magkos, E., Chrissikopoulos, V.: Strengthening privacy protection in vanets. In: WIMOB '08: Proceedings of the 2008 IEEE International Conference on Wireless & Mobile Computing, Networking & Communication, Washington, DC, USA, IEEE Computer Society (2008) 508–513
22. Kapadia, A., Henderson, T., Fielding, J.J., Kotz, D.: Virtual walls: Protecting digital privacy in pervasive environments. In: Pervasive. (2007) 162–179
23. Liu, L.: From data privacy to location privacy: models and algorithms. In: VLDB '07: Proceedings of the 33rd international conference on Very large data bases, VLDB Endowment (2007) 1429–1430
24. Chaum, D.: Untraceable electronic mail, return addresses, and digital pseudonyms. Commun. ACM **24** (1981) 84–88
25. Myles, G., Friday, A., Davies, N.: Preserving privacy in environments with location-based applications. IEEE Pervasive Computing **2** (2003) 56–64
26. Wakeman, I., Chalmers, D., Fry, M.: Reconciling privacy and security in pervasive computing: the case for pseudonymous group membership. In: MPAC '07: Proceedings of the 5th international workshop on Middleware for pervasive and ad-hoc computing, New York, NY, USA, ACM (2007) 7–12
27. Kim, J., Kim, Z., Kim, K.: A lightweight privacy preserving authentication and access control scheme for ubiquitous computing environment. In: ICISC. (2007) 37–48
28. Li, C.T., Hwang, M.S., Chu, Y.P.: Further improvement on a novel privacy preserving authentication and access control scheme for pervasive computing environments. Computer Communications **31** (2008) 4255–4258
29. Chaum, D.: Blind signatures for untraceable payments. In Chaum, D., Rivest, R., Sherman, A., eds.: Advances in Cryptology Proceedings of Crypto 82. (1983) 199–203
30. Lamport, L.: Password authentication with insecure communication. Commun. ACM **24** (1981) 770–772
31. Parno, B., Perrig, A.: Challenges in securing vehicular networks. Workshop on Hot Topics in Networks (HotNets-IV) (2005)