Multilaterally Secure Ubiquitous Auditing

Stefan G. Weber and Max Mühlhäuser

Abstract. Tracking information of individuals is a useful input to many Ubiquitous Computing (UbiComp) applications. Consider the example of a smart emergency management application: once mobile first responders are continuously tracked, a precise and safe coordination of rescue missions is possible, and also mission logs can be created for audit purposes. However, continuously tracking users and storing the data for later use is often in conflict with individual privacy preferences. This may ultimately lead to the non-acceptance and rejection of these new technologies by their users. In order to reconcile privacy and accountability requirements in location tracking systems, we introduce and evaluate the approach of using auditing mechanisms on two levels. We illustrate that, by employing carefully designed cryptographic mechanisms for selective pseudonym linkability based on efficient techniques of secure multiparty computation, it is possible to balance the conflicting interests to a certain extent. Our work, motivated by and applied to smart emergency management systems, is a step towards the realization of multilaterally secure and thus multilaterally acceptable UbiComp systems supporting collaborative work.

1 Introduction

Creating ICT systems to foster and support collaborative work is a complex issue. Inspired by Mark Weiser's vision of Ubiquitous Computing (UbiComp) which proclaims "a powerful shift in computation, where people live, work, and play in

Stefan G. Weber
CASED,
Darmstadt, Germany
e-mail: stefan.weber@cased.de

Max Mühlhäuser
Telecooperation Group,
TU Darmstadt, Germany
e-mail: max@informatik.tu-darmstadt.de

S. Caballé, F. Xhafa & A. Abraham (Eds.): INCoS 2009, SCI 329, pp. 207–233.
springerlink.com

a seamlessly interweaving computing environment" [56], researchers around the globe try to devise technological solutions that are highly distributed, but still connected, intuitively and non-obtrusively usable, and that aim at preserving data security and privacy while making use of information only when needed and appropriate. While all these issues along with mutual dependencies and system integration aspects need to be taken into account, in order to implement efficient and functional systems, to achieve acceptance among its users, and finally, to obtain commercial success [37], in this chapter, we approach this topic from two specific perspectives:

- in the motivating application context of mission-critical applications, i.e smart collaborative systems that support emergency management work, and
- with a conceptual and technical focus on multilateral security, accountability and data privacy issues.

While true UbiComp requires, on technical levels, efficient and *scalable connectivity* of a multitude of devices and network nodes [2] and means for *intuitive human computer interaction* [38], we believe that, on organizational, legal and social levels, also some support for a *seamless collaboration* of a multitude of users and parties is necessary. However, we stress that multi-user and multi-party applications tend to be also multi-interest applications. Especially, such collaborative applications often highlight inherent conflicts w.r.t. underlying data security and privacy requirements, that are due to different organizational, legal and personal backgrounds of the participants. Obviously, there is no simple answer on how to deal with such inherent security conflicts. The fundamental research question, that our work addresses, is how and to which extend it is possible to realize multilaterally secure [43], i.e. balanced and thus trustworthy, collaborations supported by modern ICT. In this chaper, we focus on collaborations between individuals with strong privacy preferences and organizations with legal documentation and accountability requirements.

1.1 Perspective: Mission-Critical Applications

As forerunners of UbiComp applications, a large range of applications has been proposed during the last years which benefit from fine-grained user tracking in multiple ways. Consider the example of a smart emergency management application: once mobile units are continuously tracked, e.g. by sending their GPS positions and further data to a headquarter, a precise coordination of rescue missions is possible [53] and vital signs of first responders can be monitored. Moreover, units can act as mobile sensors to monitor levels of air pollution, also mission auditing can be supported by creating digital mission logs based on the collected GPS traces [52].

1.2 Inherent Tradeoff: Privacy versus Accountability

While, firsthand, the application scenario strongly indicates benefits of fine-grained user tracking, there is also a further aspect that needs to be taken into account: once it comes to the collection of data related to individuals, organizational and legal

documentation and accountability requirements can get in conflict with individual privacy preferences [7]. In the emergency work example, the continuous tracking can also create digital mission logs that document real-world events and that can be analyzed afterwards - even for the detection of inappropriate real-world behaviour. Thus, a mission log could contain information that help to answer questions like ”Did an entity act beyond her competences and authorisations and exploit the current situation with inappropriate, suspicious or even malicious purpose?”. This is a highly critical issue, since, in real-world rescue missions, first responders actually need to break laws in some cases in order to save lives, and the underlying decisions often have to be made under time pressure. Therefore, the psychological burdens of possibly having to face legal consequences due to being digitally accountable need to be addressed, in order to foster acceptance for the use of tracking technologies.

More generally, aspects related to privacy preservation and resulting acceptance issues have been identified as one of the greatest barrier to the success of upcoming UbiComp applications that inherently rely on continuous large scale data collection, like location or employee tracking [44, 9, 49]. We believe that it is a major challenge to design data security mechanisms that allow to reconcile the conflicting goals of accountability for legal and organizational reasons and individual privacy protection [55, 54, 52].

1.3 Approach and Contributions

In this chapter, we describe a new approach for implementing multilaterally secure auditing functionalities for Ubiquitous Computing scenarios. Our work is motivated by and applied to collaborative mission-critical applications, hereby realizing multilaterally secure mission logs, i.e. audit logs for real-world events with special security requirements. Conceptually, the approach consists of two main parts, dealing with data collection and data access issues. The first part, a cryptographic pseudonym construction, allows to build up audit logs, which contain pseudonymized tracking information.

Especially, it enables a mobile user within a location tracking system:

- to protect her location privacy using short-lived transaction pseudonyms that can be created on a personal mobile device, and
- to selectively access audit log content that relates to herself, for own sake.

Second, our work comprises mechanisms for audit log analysis, supporting

- internal audit officers (within an organization) to iteratively analyze the location data logs in a privacy-respecting manner, in case suspecting facts have been reported,
- a lawful disclosure functionality, i.e. an attorney authority may globally revoke privacy protection of individual users, once convincing evidences have been identified.

We stress that, additionally, auditability of the log analysis process is given. Especially, the non-compliance of auditors w.r.t. actions allowed in the log analysis can be detected and reacted upon. Thus, in our work, the principle of *accountability by auditability* is prominent on two conceptual layers, first regarding real world-actions of mobile users as well as regarding the use of auditing functionalities itself. The approach is designed to fit into the framework of context-aware Ubiquitous Computing applications, i.e. it allows for alert generation to support context awareness [27] *on the content level*, while the protection mechanisms are tailored *on the identity level*. Variants of our approach can easily be integrated into existing location tracking infrastructures.

Technically, our work combines pseudo-random number generators, which are used to generate and authenticate transaction pseudonyms, with efficient methods from the area of secure multiparty computation to enable privacy-respecting yet verifiable log analysis. This conceptual combination balances the conflicting security requirements of privacy and accountability in location tracking application to a high extent, hereby implementing a what we claim to be multilaterally secure approach.

1.4 Organization of the Chapter

In the following section, we introduce the background and formulate requirements for multilaterally secure auditing functionalities. Then, in section 3, we sketch an approach to fulfill these requirements. This is followed by a description of necessary building blocks in section 4. Section 5 introduces the main tools and concepts for pseudonym generation and log analysis. This is followed by a presentation of the complete approach in section 6. A discussion and evaluation of our proposal with regards to the security requirements fulfilled and practical aspects can be found in section 7, followed by a discussion of related work in section 8. Finally, in section 9, we sum up and conclude our work.

2 Background and Requirements

In this section, we describe the paradigm of multilateral security, reflect it to our application contexts and derive requirements for multilaterally secure auditing functionalities.

2.1 Multilateral Security and the Role of Accountability

In computer-supported transactions, security requirements of involved parties are often contradicting. Multilaterally secure systems take into account security requirements of all involved parties and aim at balancing contrary interests in an acceptable way [43].

Consequently, after conflicting security requirements have been traded against a multilaterally accepted compromise, the parties should have an incentive not to cheat and only need to minimally trust in the honesty of others, which is, more generally, an ultimate goal in designing security protocols and systems [17]. Rather, the parties can concentrate on reaching a common goal. However, apart from this academic point of view, the actual implementation of multilaterally secure system is a difficult task and active area of research, especially concerning highly distributed and dynamic systems [41].

A basic fact often exploited in the design of multilaterally secure systems and used to enforce correct behaviour is that already the detectability of inappropriate actions and accountability for origination suffices to prevent misbehaviour from happening. In the context of this work, this is what we call the *accountability by auditability* principle.

Traditional technical means to deal with this issue are audit logs [46, 51]. Basically, in an IT system, an audit log contains tamper evident entries that aim at recording irrefutable evidences of all users' actions. While the log content helps to detect inappropriate actions, also users behaving appropriately could use it to defend themselves against false accusations.

2.2 Examples within the Application Scenario

We return to our application scenario of the smart emergency management system. In this system, mobile units and first responders are continuously tracked for the duration of their missions. While the *current* tracking information supports the coordination of rescue missions in the headquarter, collected *historical* position information also creates a log which documents the rescue missions, and thus documents real-world actions. This kind of audit log is what we call a *mission log* throughout this chapter.

The mission log can be analyzed for several purposes in the postprocessing phase of an emergency. In the following, we assume a mission log to obey to a simple structure: it contains several entries in the form *entity ID - time - location*. The organization which accounts for the emergency management wants to be able to analyze processes after a mission, and also, the goal of mission logs is to be able to assign responsibility for real-world actions, since organizations tend to verify compliance. We next describe two motivating real-world use cases of a mission log.

2.2.1 Example: Emergency Car Driving

During the course of a rescue mission, ambulance vehicles or rescue vans sometimes are in need of breaking traffic rules, such as disregarding traffic lights. This may lead to road accidents or injured pedestrians. Usually, emergency cars beckon their emergency missions with sirens, however, there may be situations where no acoustic signals is available.

2.2.2 Example: Cases of Omitted Assistance

Several rescue scenarios involve mobile first responders. While such forces are on their mission, they strongly priorize actions, according to given instructions. However, sometimes they depart from that. Also, when it comes to dealing with injured persons, rescue forces act according to triage regulations, i.e. according to the severity of injuries they postpone or even skip treatment, which might be considered by eye witnesses as cases of omitted assistance. Moreover, there are a lot of situations that entail the destruction of properties, like breaking doors to enter a building, that are relevant to after mission warranty and accountability discussions.

2.3 Towards Balanced Auditing Functionalities

Having introduced the concept of the mission log, as a special kind of audit log for real-world actions during emergency missions, we next discuss and derive basic security requirements that have to be met to implement a *multilaterally secure mission log*. Thereby, multilateral security is considered in the sense that we want to take into account security and privacy requirements of mobile users, emergency management organizations and law enforcement agencies, as well.

First, allowing the mobile units to be tracked pseudonymously[1] instead of by means of a fixed ID implements a very basic kind of privacy protection in our application. This is necessary to address the inherent privacy issue in the location tracking. Consequently, following this approach also requires auditing functionalities that are compatible with pseudonymized log data. While this is the starting point for designing the system, however, in order to achieve a multilaterally secure solution, a more complex security design is required. According to [21], two important facts have to be dealt with in the context of creating privacy-respecting log analysis functionalities:

1. "The controlled disclosure of pseudonyms is the controlled ability to make pseudonymized objects accountable again. This ability is controlled by controlling who can use the ID to pseudonym mapping."
2. "The disclosure of pseudonyms should be bound to a priori specified purposes."

Thus, a central point is to implement a selective control functionality regarding the pseudonym linkability for users, organizations and authorities. Moreover, mechanisms that allow for the detection of suspicious evidences inside such a log are required. According to our previous discussion, we propose the following set of functionalities in order to reconcile privacy and accountability as fair and as far as possible.

[1] Historically, the term *pseudonymous* relates to the Greek word *pseudonymos*, which means *having a false name* [19]. In a technical sense, a pseudonym is an identifier of an entity that is used instead of the entity's real-world name [42]. Pseudonymity is the use of pseudonyms as identifiers.

First, regarding the perspective of the user:

- The user should be tracked under short-lived transaction pseudonyms [42] to provide some kind of basic location privacy protection.
- The user should be able to authenticate a pseudonym, that he has been tracked under. In dispute cases, this functionality allows her to access the mission log in order to repudiate false accusations by providing evidences of exoneration.

Second, regarding the perspective and role of third parties, e.g. emergency management organizations[2]:

- It should be possible to selectively analyze the entries that are recorded in a log in a privacy-respecting manner. Therefore, the logs should contain only pseudonymized entries that hide the real-world identities of tracked persons.
- It should be possible to link sample entries, i.e. to verify if they belong to the same user.
- It is desirable to check if one entry relates to a common organizational structure or function.
- If legally convincing pieces of evidence for misbehavior have been identified in the course of this analysis, it should be possible to reveal the true identity of a tracked person.
- An operational separation of duty should be enforced, i.e. no single entity should be able to (mis)use the audit functionalities.
- The whole process of log analysis should also be auditable, i.e. it should be detectable if the parties that are responsible for it do not comply with the rules set up for the privacy protection of the individual user.

Third, the legal perspective needs to be taken into account:

- It should be possible to exercise a global lawful disclosure functionality, i.e. an attorney authority may revoke privacy protection of any users in question, once convincing evidences of inappropriate behaviour have been identified. This is a requirement for many ICT applications, that actually may lead to court proceedings for accused offences.

3 Construction Idea

As discussed in section 2.3, pseudonymous auditing can balance the conflict between accountability and privacy to a certain extent. From a different point of view, a pseudonym implements the central reference point to evidences in an audit log.

It is known that techniques from the area of secure multiparty computation (SMPC) can theoretically be applied to a large range of problems in the area of privacy-preserving data analysis [30, 35]. Basically, SMPC [57] allows for implementing privacy-respecting multiparty protocols that do not rely on a single trusted third party

[2] The parties that actually exercise the log analysis functionalities for the organizations are called *audit officers* throughout this chapter.

(TTP). The intention of these cryptographic techniques is that a number of distinct, but connected parties may jointly compute an agreed function of their inputs in a secure way. Hereby, the correctness of the output as well as the privacy of each input shall be preserved, even if some participants cheat[3]. Generally, secure multiparty computation is an approach to distribute the functionality and powers of a single TTP among several parties. However, this is traditionally only achieved with very high computational costs [35], due to the intensive use of secret sharing [47] and operations on secret shared data in SMPC protocols. However, more efficient special purpose approaches to SMPC have been proposed, e.g. in the *mix-and-match* approach [31], secret sharing techniques are replaced by operations on encrypted data.

Our approach follows the spirit of the *mix-and-match* approach. Thus, we formulate the pseudonym generation in terms of specific encryption operations. This enables us to apply efficient concepts from SMPC for realizing privacy-respecting log analysis functionalities *on the pseudonym level*. Additionally, we make use of seeded PRNGs to control random factors inside the encryption operations. This allows us to implement a further direct identity-to-pseudonym-mapping, that can be exploited by individual users, in order to access log entries that relate to herself.

4 Building Blocks

In this section, we briefly describe the main building blocks that are employed in our approach.

4.1 Cryptographically Secure PRNGs

A pseudo-random number generator (PRNG) [34] is a deterministic algorithm for generating sequences of numbers. Hereby, the created numbers apparently exhibit the properties of real random numbers. PRNGs incorporate an internal source of entropy, which is called a seed, to derive and compute their output. Cryptographically secure PRNGs are special kinds of PRNGs that produce sequences of numbers with strong security requirements, i.e. it is actually impossible to guess or derive any forward or backward numbers by analyzing the output of such a PRNG. Our constructions actually employ cryptographically secure PRNGs. However, in the following, we often simply refer to them as PRNGs.

4.2 Threshold ElGamal Cryptosystem

A key primitive in our approach is the ElGamal cryptosystem [16], over subgroups $\mathbb{G}_q$ of order q of the multiplicative group $\mathbb{Z}_p^*$, for large primes $p = 2q + 1$. We treat the primes p, q and a generator g of $\mathbb{G}_q$ as common system parameters. ElGa-

[3] A classic example of SMPC is the millionaires' problem due to Yao [57]: some millionaires (*the parties*) want to find out, who is the richest (*agreed function*) without revealing the precise amount of their individual wealth (*input privacy*).

mal encryption is know to be semantically secure in $\mathbb{G}_q$, under certain complexity assumptions [50]. Practically, semantic security means that no partial information about a plaintext is leaking from the corresponding ciphertext. More specifically, we utilize a threshold variant of the ElGamal cryptosystem, according to Cramer et al. [13], which allows to distribute cryptographic operations and thus offers robustness and distributed trust. In the system, a private key $s \in_R \mathbb{Z}_q$ can be defined in two ways: first, it can be initially generated by a trusted dealer and then be secret shared [47] among all n participating authorities. Second, it can be generated via the distributed key generation protocol of Pedersen [40], whereby no single party knows the complete key. In both ways, w.r.t. the participating authorities, the power to decrypt is distributed among all of them, and a quorum, i.e. a minimal majority of t out n authorities need to cooperate to perform a threshold decryption. The authorities common public key is $h = g^s \bmod p$. A message $m \in \mathbb{G}_q$[4] is non-deterministically encrypted by choosing $r \in_R \mathbb{Z}_q$ and by computing $(g^r, h^r m)$.

In our work, the communication model in the threshold cryptosystem consists of a broadcast channel with memory. This channel is used to store and exchange information in any protocol involving distributed computations, e.g. partial decryptions and identifiers of each authority in a threshold decryption. Moreover, in our setting, the broadcast channel is append-only, i.e. once the information is sent over it, it is stored and cannot be changed or deleted afterwards. Thus, its content can later be analyzed for audit purposes.

4.3 Non-interactive Zero Knowledge Proofs

Zero knowledge proofs (ZKPs) [24], which are basically generalized challenge-response authentication protocols, are used to guarantee correctness of and participation in distributed cryptographic operations and protocols. Especially, we use non-interactive zero knowledge proofs (NIZKPs) by applying the Fiat-Shamir heuristic [18]. See e.g. [12] for discussions of these techniques. NIZKPs can be stored, and may be verified, comparable to digital signatures, after a protocol run. Thus, incorrect actions can be deduced by looking at those digital transcripts. NIZKPs are a common cryptographic approach to implement auditability[5].

4.4 Plaintext Equality Tests

A plaintext equality tests (PET) [31] is a primitive for pairwise blind comparison of ciphertexts of non-deterministic threshold cryptosystems like ElGamal. A PET allows to test whether two ciphertexts represent the same plaintext by performing algebraic operations on the ciphertext, but without revealing the plaintext. PETs and generalizations thereof are key primitives to implement privacy-respecting log analysis functionalities. The use is described in detail in section 5.3.

[4] Messages that are not in $\mathbb{G}_q$ can efficiently be mapped onto $\mathbb{G}_q$ [31]. Thus, arbitrary strings can be encrypted.

[5] In research dealing with cryptographic protocols, this is often referred to as *verifiability*.

4.5 Reencryption Mixnets

A mixnet, originally introduced by Chaum [10], is a cryptographic tool to anonymize sets of ciphertexts. In our work, we employ ElGamal based reencryption mixnets [39], which basically reencrypt and permute ciphertexts in order to anonymize them. In this setting, reencryption can be done without a private key. Moreover, we also require the mixnets to be verifiable, i.e. to provide NIZKPs of correctness of their operations. We do not go into details here, but point to the proposal of Furukawa et al. [23], that implements such cryptographic auditability for reencryption mixnets. We apply the underlying concept of reencryption in two stages of our work, first to derive transaction pseudonyms (cf. section 5.1), second, to build up anonymous reference sets used in re-identification steps of our scheme (cf. section 5.3).

5 Basic Tools and Concepts

We now introduce the basic constructions and protocols of our approach. These constructions implement functionalities for pseudonym mapping and linking, for all considered parties, i.e. users, organizations and law enforcement agencies.

5.1 Registration and Generation of Pseudonyms

In this section, we introduce the concepts for pseudonym generation. Basically, we propose to encode a static attribute inside malleable pseudonyms, by generating pseudonyms as encryptions of an attribute under the public key of a threshold ElGamal cryptosystem. The resulting construction is what we call a *pseudonym with implicit attribute*.

First, each user must participate in a registration phase, which is depicted in Figure 1. In this phase, each user receives a trusted personal device which includes

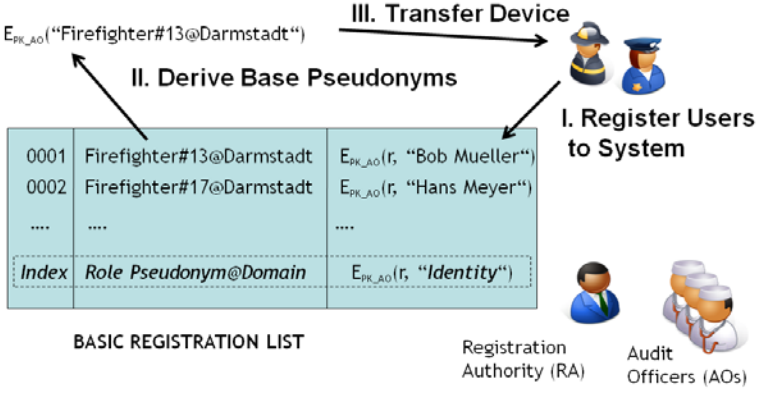

Fig. 1 Registration Phase

a cryptographically secure PRNG. Therefore, the user interacts with a trusted registration authority (RA). The registration phase consists of the following main steps:

I. Each user is added to an integrity protected registration list. He receives a distinct role pseudonym, which associates the user with the issuing organization. For example, a user can be registered as *Firefighter*#13@*Darmstadt*. The user's real-world identity, e.g. *Bob Mueller*, is encrypted and stored together with the role pseudonym on the registration list.
II. The RA derives the base pseudonym by encrypting the unique role pseudonym. Thus, each base pseudonym encodes a distinct implicit attribute.
III. The RA uploads the base pseudonym to a personal device. The user receives this personalized device.
IV. The user generates and registers a unique seed in the PRNG of the device to enable it for pseudonym generation.

In the registration phase, the encryptions are done under the public key belonging to a set of so called audit officers[6] inside the organization, e.g. in the emergency management organization:

- The real-world identity ID is encrypted as: $E_{PK_{AO}}(ID) = (g^r, h^r ID)$.
- To generate the base pseudonym for a user, the registration authority encrypts the chosen attribute A as: $P = E_{PK_{AO}}(A) = (g^{r_s}, h^{r_s} A)$. Moreover, the random value r_s, the start value for pseudonym generation, is also transferred to the user and stored on her device.

The user is now able to derive *transaction pseudonyms* from her base pseudonym in the following way:

1. The seeded PRNG is used to generate a sequence of random numbers.
2. Each random number r_i is used to compute a randomization factor $F_{r_i} = (g^{r_i}, h^{r_i})$.
3. F_{r_1} is used to construct the *first* transaction pseudonym by multiplying it with the base pseudonym: $P_1 = (g^r, h^r A) * (g^{r_1}, h^{r_1}) = (g^{r+r_1}, h^{r+r_1} A)$.
4. Further transaction pseudonyms are created by repeated multiplications: $P_{i+1} = P_i * F_{r_{i+1}}$.

By this procedure, a user creates a set of different transaction pseudonyms that all contain the same implicit attribute. These pseudonyms are used instead of fixed IDs during the location tracking.

5.2 Log Attestation

Due to the construction, presented in the last section, users are also enabled to authenticate a transaction pseudonym that is stored in a mission log. Therefore, a

[6] Cryptographic keys have been generated in a previous setup phase, cf. section 6.1. The audit officers *share* the private key belonging to the single public key. Due to the use of threshold cryptography, variants with different distributions of power are possible, cf. section 7.

user needs to show that she is in possession of the base pseudonym and the correct aggregated random factor, which allows to reproduce a recorded pseudonym, thereby authenticating a complete log entry. This functionality is what we call *log attestation*.

5.3 Log Analysis

In this section, we introduce the concepts for privacy-respecting mission log analysis. Basically, we harness the possibility to do algebraic operations on the non-deterministic encrypted ciphertexts that represent pseudonyms.

Remember the structure of a mission log, as introduced in section 2.2: *entity ID - time - location*. Assuming that the *entity ID* values are actually values of *pseudonyms with implicit attributes*, we allow the audit officers of the responsible organization to execute *two basic operations* for privacy-respecting log analysis:

1. check if two log entries relate to the same entity but without revealing the actual ID of the entity;
2. check if one entry relates to a group of entities with a common organizational role or function.

The first operation is implemented by executing a *plaintext equality test* on the pseudonym values of two log entries. Suppose that $P_a = (g^{r_a}, h^{r_a} A_a)$ and $P_b = (g^{r_b}, h^{r_b} A_b)$ represent two entries of that kind. If they relate to the same entity, they contain the same implicit attribute. In order to verify this, the pseudonyms can be algebraically divided: $P_c = P_a / P_b = (g^{r_a - r_b}, h^{r_a - r_b} A_a / A_b)$. Given that A_a equals A_b, this is an encryption of the attribute "1". By performing a threshold decryption, the audit officers yield an explicit attribute which is either "1" or a meaningless different value.

The second operation is an extension of the procedure above to a global instead of pairwise comparison of pseudonyms. It allows to test if one log entry relates to a certain organizational unit, function or even place. For example, it can be tested whether the entry relates to "Response Team Alpha" or "fire department Darmstadt". Especially, this test does not disclose which of the possibly involved entities is the actual originator of the log entry.

The method of the *generalized blind plaintext equality test* is introduced next. Again, it is based on operations of an ElGamal threshold cryptosystem. Basically, it works as following:

1. First, all participating audit officers jointly generate a shared key z.
2. Then, the authorities select all attribute values that are relevant to the organizational function or role and create base pseudonyms for each relevant attribute.

3. Next, all base pseudonyms are processed by a reencryption mixnet. This creates an anonymized list of base pseudonyms, i.e. the positions of the individual attributes in the list as well as ciphertext representations are changed.
4. The audit officers cooperatively apply their shares of z to each anonymized base pseudonym. This process achieves blinding of the attribute inside the pseudonyms.
5. After that, each blinded pseudonym is jointly decrypted. This yields a blinded attribute, which is used as a deterministic yet blind fingerprint of the original attribute related to a relevant base pseudonym.
6. After processing all base pseudonyms that need to be considered, they can be compared without leaking information about the implicit attribute by comparing only the blind fingerprints.
7. In order to do so, the authorities also derive a blind attribute fingerprint for the pseudonym value of a log entry that is to be verified.

Having outlined the abstract steps of the method, we next go into more details. The whole scheme makes use of secret sharing techniques according to Shamir [47] and of the distributed key generation according to Pedersen [40]. First, to jointly generate the secret shared key z used for blinding, the audit officers employ the distributed key generation protocol due to Pedersen. In this protocol, each audit officer AO_j receives a share z_j of the key z. Also, each officer is publicly committed to the share z_j by a public value $\rho_{z_j} = g^{z_j}$, due to the execution of the protocol.

In the following, we describe the complete protocol for *distributed blinding*, which is analog to the distributed decryption protocol [13] of the ElGamal threshold cryptosystem. This protocol can be used to blind an arbitrary element $x \in \mathbb{G}_q$ using the shared key z. The following method is used to apply z cooperatively to the pseudonyms[7]:

1. Each officer computes $b_j = x^{z_j}$, a partial blinding of x, by applying its secret z_j. Also, each officer publishes b_j together with a NIZKP that

$$\log_g \rho_{z_j} = \log_x b_j$$

   The latter is realized using a proof of knowledge for equality of discrete logs [11]. The proof assures that the officer indeed utilized the correct share to produce the partial blinding[8].
2. For any subset Λ of t authorities with valid zero-knowledge proofs, the complete blinded value x^z is reconstructed using the discrete Lagrange interpolation

$$x^z = \prod_{j \in \Lambda} b_j^{\lambda_{j,\Lambda}} \bmod p$$

[7] Pseudonyms are effectively encoded as two elements of $\mathbb{G}_q$, whereas the second element is directly derived from the implicit attribute.

[8] Otherwise, the use of a fake share would lead to an incorrectly blinded value, which could not be used for blind matching purposes.

where

$$\lambda_{j,\Lambda} = \prod_{l \in \Lambda \setminus \{j\}} \frac{l}{l-j} \bmod q$$

are the appropriate Lagrange coefficients.

Now, let $A_i \in \mathbb{G}_q$ be an attribute plaintext[9], and $(g^r, h^r A_i)$ an pseudonym with implicit attribute A_i with $r \in_R \mathbb{Z}_q$, the authorities produce the deterministic fingerprint through the following steps:

1. To each component of $(g^r, h^r A_i)$ the distributed blinding protocol is applied, blinding it to a fix secret shared exponent $z \in \mathbb{Z}_q$: $((g^r)^z, (h^r A_i)^z) = (g^{rz}, h^{rz} A_i^z)$.
2. The blinded pseudonym is jointly decrypted to the blinded attribute A_i^z using the distributed decryption protocol of the threshold ElGamal cryptosystem.

Now, A_i^z represents a deterministic fingerprint produced with a key z. It is used to blindly compare attributes encoded in the pseudonyms.

5.4 Disclosure of Pseudonyms

As stated earlier, "the disclosure of pseudonyms should be bound to a priori specified purposes" [21]. In the last sections, we provided methods for analyzing entries of a mission log with regard to linkability of pseudonyms to chosen attributes. Rules and conditions for the actual detection of inappropriate behaviour and misuse must be defined in the organizational and legal context of the application, according to which the audit officers have to decide on whether detected patterns inside the log provide convincing evidences. However, we propose to design the rules according to the need-to-know principle [3], i.e. to do a step-wise analysis of the log with the highest possible anonymity restrictions.

In order to complement the two operations for log analysis, we describe the operation for the complete disclosure of pseudonyms next:

- Upon misuse detection, the audit officers decide to completely disclose the identity associated with a pseudonym.
- First, they cooperatively decrypt the pseudonym part of the relevant entry of the mission log. This yields the plaintext of the distinct attribute encoded in the pseudonym.
- Next, the audit officers select the corresponding entry on the registration list. Then, they cooperatively decrypt the deposited ciphertext to reveal the real-world identity.

The lawful disclosure functionality works in a comparable way. Basically, we assume that the global attorney also plays the role of the trusted dealer in the key generation process (cf. section 4.2), thus this authority is in possession of the private key of the audit officers.

[9] We simplify the description at that point, $A_i \in \mathbb{G}_q$ is actually only the algebraic representation of an attribute. Mapped back to a string representation, it could be "Firefighter #13@Darmstadt".

- First, the global attorney decrypts the pseudonym part of the relevant entry of the mission log. This yields the plaintext of the distinct attribute encoded in the pseudonym.
- Second, the authority selects the corresponding entry on the registration list. Then, it decrypts the deposited ciphertext in order to disclose the real-world identity.

6 Complete Approach

This section presents our complete approach. First, we sum up the phases. Then, we depict the overall scheme in more detail.

6.1 Phases

- *Setup Phase:* In this phase, system parameters for the threshold cryptosystem and cryptographic keys used for pseudonym generation and auditing are created.
- *Registration phase:* Each user receives a personal device. Also, a base pseudonym with an implicit attribute is registered to each user. The user locally creates and registers a unique seed in the PRNG of the device. The base pseudonym, together with the seeded PRNG, allows to derive transaction pseudonyms in the next phase.
- *Pseudonym Generation Phase:* A user creates transaction pseudonyms locally on the personal device. Each transaction pseudonym is a non-deterministic threshold encryption of the same implicit attribute. The devices PRNG provides random factors used in the pseudonym creation.
- *Tracking Phase:* During a mission, the user is regularly tracked under transaction pseudonyms. The pseudonym in use is regularly changed, according to the preference of the user.
- *Log Analysis Phase:* In this phase, entries of the log are processed by audit officers for organizational and legal reasons. Upon convincing detection of inappropriate actions, pseudonyms can be disclosed.
- *Log Attestation phase:* After the mission, a user may authenticate single entries of the mission log by providing the correct keying material that allows to reconstruct the pseudonyms of the log entries.
- *Officer Auditing Phase:* In this phase, the appropriateness and correctness of the actions of the audit officers in the log analysis phase is verified. This done by checking the NIZKP stored on the broadcast channels with memory,
- *Lawful Disclosure Phase:* This phase is optional. If a mission log analysis leads to court proceedings, a global attorney can re-identify any log entries that may support returning a verdict.

6.2 Scheme Description

We next describe our complete approach in detail. Thereby, we take into account the building blocks from section 4, and the operations described in section 5.

In the description, we denote the participants as: U_i a user of the location tracking system; *AO*s the n audit officers that share the private key SK_{AO} with the corresponding public key PK_{AO}; *RA* a trustworthy registration authority; *GA* a global attorney authority.

- *Setup:* The *GA* acts as trusted dealer, she selects system parameters p,q,g and generates PK_{AO}, and SK_{AO}, appropriate to the threshold ElGamal cryptosystem. PK_{AO} as well as the ElGamal system parameters are published. Once the participating audit officers (*AOs*) have been appointed[10], they receive individual shares of SK_{AO}. In addition, the *AOs* produce a shared key z.
- *Registration:* Each user U_i is registered by a trustworthy registration authority *RA*. First, a mobile device is selected for personalization. Then, each user receives a base pseudonym with an implicit attribute: $P_{U_i,B} = E_{PK_{AO}}(A_{U_i})$. The random factor $r_{i,B}$ used in the encryption process is stored on the user's device. The device is transferred to the user. The user generates an unique seed s_{U_i} and registers it to the PRNG of her mobile device. At the end of this phase the *RA* publishes a reference list C. It contains entries of all registered users (encrypted real world ID) and their assigned attributes: $C_{U_i} = E_{PK_{AO}}(U_i) - A_{U_i}$.
- *Pseudonym Generation:* Each user U_i derives from her base pseudonym $P_{U_i,B}$ a set of transaction pseudonyms $\{P_{U_i,j}\}$. In order to do so, first, the seeded PRNG is used to produce a set of random factors $\{r_{i,j}\}$. Then, the random factor inside the base pseudonym is updated with a random factor from the set: $P_{U_i,1} = P_{U_i,B} * (g^{r_{i,1}}, h^{r_{i,1}})$, $P_{U_{i,j+1}} = P_{U_i,j} * (g^{r_{i,j+1}}, h^{r_{i,j+1}})$.
- *Tracking:* When using the tracking system, each user is tracked under transaction pseudonyms from the set $\{P_{U_i,j}\}$. According to the preferences of each user, the pseudonym $P_{U_i,j}$ is changed to $P_{U_i,j+1}$ in a specified interval of time. Note that changing a transaction pseudonym does not change the implicit attribute an user is tracked under. In the tracking phase, a mission log is created. Its entries are in the form *entity ID - time - location*. The *entity ID* field records the value of a pseudonym with implicit attribute, i.e. a transaction pseudonym.
- *Log Analysis:* According to an organizationally and legally defined set of conditions and rules, the audit officers use the provided operations to detect evidences of misuse in the mission log. If convincing evidences have been identified, they induce a pseudonym disclosure. Therefore, the authorities cooperatively decrypt the pseudonym part of the relevant entry of the mission log. The resulting attribute plaintext is used to select the corresponding entry on the registration list. Then, the authorities cooperatively decrypt the deposited ciphertext to disclose the real world ID.

[10] This can be delayed in time, since the public key, which is needed to generate pseudonyms, has already been created.

- *Log Attestation:* In dispute cases after the tracking phase, a user U_i may access data recorded in the mission log. In order to do, she selects an entry k of the mission log by handing out authentication information in form of an aggregated random factor $r_{i,A} = \sum_{j=1}^{j=k} r_{i,j}$ and the base pseudonym $P_{U_i,B}$ to the audit officers. After verification, whether the pseudonym of the mission log entry k matches the reconstructed transaction pseudonym $P_{U_i,k}$, the user receives a tuple *time* - *location*, which is additionally certified by the audit officers. The user can use the tuple to repudiate location- and time-dependent accusations against her.
- *Officer Auditing:* Internal and external auditors may verify the appropriateness and correctness of actions of the audit officers in the log analysis phase. In order to do so, they read out the content of the broadcast channel with memory. The channel provides a log of the committed actions. Actions that do no comply with the allowed operations can be identified, as well as attempts to corrupt the cooperative operations, since stored NIZKPs cannot be verified correctly in that case.
- *Lawful Disclosure:* In case a mission log analysis did not clear all dispute cases, court proceedings can be initiated afterwards. Herein, the global attorney *GA* can re-identify any log entries that may support returning a verdict. The *GA* uses SK_{AO} to decrypt the pseudonym parts of any relevant entry of the mission log. Any plaintext, i.e. the implicit attribute, distinctly refers to one entry of the registration list. The *GA* decrypts any relevant entry of the registration list to recover the real-world identity of the originator of the log entry.

7 Example and Discussion

Having introduced the concepts and the complete scheme, in this section we first describe an application example. Then, we discuss the presented approach with respects to its main security requirements. Moreover, we elaborate on practical aspects that have to be considered in the course of implementing a system that actually employs our concepts.

7.1 Application Example

We next provide an example that illustrates how our approach can actually be employed in practice for analyzing mission log data. Hereby, we especially refer to section 5.3 w.r.t. the two basic operations of log analysis. We assume the scenario, that a large airport is affected by a large scale emergency. Several airplanes have caught fire due to an accident. The burning is spreading over to the terminal buildings. Since the fire brigade of the airport is unable to handle the situation on its own, additional forces from nearby fire departments are requested. Also, the fire department Darmstadt sends a group of 50 mobile first responders to support the rescue missions. Arriving at the airport, the first responders register to the tracking system, receiving base pseudonyms with implicit attributes *Firefighter* #247@*Darmstadt* to *Firefighter* #296@*Darmstadt*. During the course of the successful rescue mission,

their movements and actions are continuously tracked and stored in the mission log. In the postprocessing phase of the emergency, a group of airport officers is appointed to analyze a specific incident which has been reported to them by an anonymous eye witness: it is mentioned that a group of 4 firefighters suddenly disappeared from an important task to extinguish fire in an office wing, located in the vicinity of a jeweller in the shopping area. The store reports that expensive items have disappeared, and several offices have been destroyed due to the lack of man power. Analyzing the mission log, the officers manage to identify traces of 5 pseudonymous entities that move away from the office wing in question (*by using the first operation*). Moreover, these 5 pseudonymous entities can be identified to belong to *fire department Darmstadt* (*by using the second operation*). On request, the commander from Darmstadt asserts, that a special group of his first responders, that is known as *Response Team Alpha*, decided to change the mission task short-run, due to the observation of strange knocking sounds nearby. The audit officers define the *Response Team Alpha* unit and manage to relate the traces thereto (*by using the second operation*). While, in that case, the commander's information and the information from the audit process suffices to resolve the incident in question, the individual firefighter could have also used the *log attestation* functionality, to document scenes of the mission. After the audit, the firefighters access the transcripts of the audit officers' actions. They can recognize their appropriate behaviour during the log analysis.

7.2 Security Properties

- *Attacker Model:* Our work is specified as a multilaterally secure approach, i.e. firsthand, the involved parties are seen as mutual attackers. However, the intention of the approach is to provide an *enabling technology* that allows to realize an acceptable compromise between individual privacy and accountability. The protection mechanisms are devised on the application level, i.e. data that is leaking on lower layers is not explicitly considered and could be exploited by further attackers. However, the approach is tailored within the context of emergency communications where parties use dedicated digital radio networks with own security infrastructure, e.g. according to the TETRA standard[11]. Thus, complementary security measures are provided by the host network.
- *User Privacy and Pseudonym Linkability:* From the users' perspective, individual privacy within the location tracking application is protected due to the use of transaction pseudonyms. In fact, any user is able to adjust the frequency of pseudonym changes and also of location updates sent to the headquarter, thus she is empowered to adjust the level of linkability within a mission log. Generally, concerning the provided degree of linkability, pseudonyms can be classified into *transaction pseudonyms*, *role pseudonyms*, *role-relationship pseudonyms* and *person pseudonyms* [42]. Our approach can be seen as a conceptual combination of transaction and role pseudonyms. The ability to use short-lived random pseudonyms in a freely determined frequency relates to the first property, while

[11] Cf. WWW.TETRAMOU.COM

the implicit attribute can be interpreted as a role pseudonym that can be read out in several levels of granularity, e.g. "Firefighter", "Response Team Alpha", "Firefighter #13@Darmstadt".

- *Privacy-Respecting Log Analysis:* The basic pseudonym construction stems from a semantically secure encryption operation, thus pseudonyms by itself do not leak information about the implicit attribute. Moreover, no single audit officer is able to decrypt a pseudonym and thus to link a pseudonym to a user. This is achieved since both registration list and pseudonym creation are performed as encryption operations of a threshold cryptosystem. Therefore, audit officers have to cooperate in any step of the log analysis. This implements an operational separation of duty in our system. During the course of the analysis, the officers are able to build up reference sets of pseudonyms with implicit attributes, that they test log entries against. Since anonymity is defined according to the size of the anonymity set [42], interestingly, this method allows to obey regulations for log analysis that are formulated in terms of anonymity.
- *Pseudonym Authentication:* In order to implement a log attestation functionality, which aims at defending against false accusations and thus could actually entail legal effects, the pseudonym authentication needs to assure a uniqueness property. Especially, it must not be possible for an attacker[12] to provide authentication information for a pseudonym without being the real originator. This is achieved in our construction due to a two-factor authentication process: The users needs to provide both the base pseudonym and the aggregated random factor. An attacker could only guess both base pseudonym and matching aggregated random factor, but he cannot access a seed to derive correct values, since the seed is generated locally and the registration is assumed to be trustworthy. Moreover, the probability to succeed with such a bruteforce attack can be lowered by requiring a user to authenticate multiple entries in a log attestation. From a broader perspective, the final acceptance of tracking information as evidences in proceedings is a legal issue. Especially, in a trial, it has to be considered if evidences of *having been at a certain location* actually relate to *having committed a certain action*. From a security point of view, this boils down to the question, whether the location tracking infrastructure is trustworthy, which is, in fact, a core assumption of our approach.
- *Distribution of Powers:* The proposed construction allows to flexibly represent a large range of legal and organizational distributions of duties and powers. This is due to the use of a (t,n) threshold ElGamal cryptosystem as well as the distributed computation of fingerprints. Firsthand, the approach can also tolerate the failure of at maximum $n-t$ authorities, which may be due to unavailability or due to corruption. Additionally, the robustness of scheme stems from its ability to tolerate attacks against audit officers or failures of them, without corrupting the whole system. However, we require the registration phase of the scheme to be trustworthy, since it depends on a single registration authority *RA*, which is contrary to the distributed design of the rest of the scheme. Also, the global

[12] In that case, the attacker could be a further user of the location tracking system who tries to fake evidences.

attorney *GA* authority represents such a single TTP. However, the global attorney can also be avoided, if not required in a certain application context. In that case, the initial generation of SK_{AO} is executed according to the distributed key generation protocol of Pedersen [40]. Also, the power of the *AOs* to completely disclose pseudonyms can be avoided, by encrypting the registration list under PK_{GA} instead of PK_{AO}. Variants in the encryption of the registration list can also be used to impose higher computational cost on the final disclosure step, if necessary.

- *Accountability by Auditability:* The multilateral security property of the overall approach relies on the principle of *accountability by auditability*: mobile units can be held accountable for real-world actions during their missions, due to the existence of mission logs. Audit officers can be held accountable for their actions during the log analysis process, due to existence of transcripts of the distributed cryptographic operations. Especially, anyone who can read the broadcast channel can audit the log analysis process. The existence and correctness of each distributed computation step can be verified by checking the broadcast NIZKPs stored on the broadcast channel. However, due to the use of zero knowledge techniques, this does not leak additional information. Thus, only the correctness of the scheme and appropriateness of the process are made transparent to external parties.

7.3 Practical Aspects

- *Handling short-lived Identifiers:* In order to use transaction pseudonyms in the location tracking, we assume that the personal device of the user is able to handle changing identifiers. Especially, we assume that the tracking does not proceed under a static MAC address. The technical feasibility to implement such changing identifiers is a standard research assumption, we share this concept e.g. with [26, 28, 25]. Moreover, this approach requires the availability of special mobile devices. This is an organizational fact that is actually true in the emergency management context, where any user is handed out e.g. a personalized TETRA device before the missions start. Additionally, a variant of our approach can easily be integrated into existing location tracking infrastructures. In this *synchronized case*, the actual tracking can proceed under a static identifier. Instead, both the mobile devices as well as a trusted pseudonymizing module (for each user) compound to the location tracking system generate the same chain of transaction pseudonyms, in the same frequency, derived from the same seed value. Thus, pseudonymization of the mission log is achieved right after data collection, not within. This approach requires less specialized devices and is conceptually comparable to the *RSA SecurID time-based one time passcodes* [13], where PRNG-based reference values used for authentication are dually generated on user-owned hardware tokens as well as on trusted servers within a company.
- *Pseudonym Bit Size:* In the proposed scheme, pseudonyms are encoded as *two* elements of an underlying algebraic group. Therefore, the actual bit size of a

[13] Cf. HTTP://WWW.RSA.COM/NODE.ASPX?ID=1156.

pseudonym depends on the characteristics and chosen parameters of the group. In order to minimize the communication and storage overhead, it is possible to employ elliptic curve groups in order to implement the cryptographic operations of the ElGamal cryptosystem.

- *Mixnet Operators:* Reencryption mixnets are used within the log analysis in order to anonymize the list of base pseudonyms. We propose to use verifiable and thus auditable mixnets. Their operation is not a time critical issue, however it is an organizational question who actually operates the mixnets, i.e. which party provides the servers for their operation. In our scheme, a trustworthy registration authority is already required. Practically, this party can also operate the mix servers. Hereby, it can also share the broadcast communication channel with the threshold cryptosystem to store NIZKPs.
- *Context Awareness:* Generally, UbiComp applications entail some kind of proactive system behaviour. On a technical level, this partly requires that alerts can be generated, e.g. on acquired sensor data. In the application example of first responder tracking, vital data or air pollution can locally be sensed and also be send to the headquarters. There, the monitoring system can generate alerts if certain thresholds are exceeded, e.g. if physical parameters indicate injuries. Staff member can react upon such warnings. In order to realize such functionalities, *data content* must be efficiently analyzable. Our approach designs protection mechanisms in form of pseudonyms on the identity level, leaving the content level for real-time alert generation.

8 Related Work

In this section, we review and discuss representative related research approaches. Existing research can be classified into work regarding linkable pseudonyms, their applications in location privacy protection as well as in privacy-respecting audit log analysis.

8.1 Linkable Pseudonyms

Historically, Chaum [10] introduced digital pseudonyms as a basic tool for privacy protection in distributed systems, by implementing a firsthand unlinkability between a real-world identity and a pseudonymized identity. In the following years, several types of pseudonyms and applications have been identified, and a wide scope of scientific background has evolved [42]. Concerning the provided degree of linkability, pseudonyms can be classified into *person pseudonyms*, *role-relationship pseudonyms*, *role pseudonyms* and *transaction pseudonyms*, whereby the degree of unlinkability and thus anonymity is highest for transaction pseudonyms. Viewed differently, linkable pseudonyms are pseudonyms that additionally encode secret trapdoor information, to enable attribution of multiple pseudonyms to one or more real-world identities. Different from our work, linkability is usually only possible for either third parties or the user herself [45], not for both. Recent cryptographic

research abstracts from pseudonyms and focuses on separating authentication from identification issues [8], but also allows for reconciliation thereof, to construct so-called self-certified pseudonyms [36].

8.2 Location Privacy Protection

In the context of location tracking applications and UbiComp, pseudonyms have been proposed as one of the basic means for *location privacy protection*. Location privacy has been identified as a key factor to personal wellbeing and safety [15] and protection from intrusive inferences. In our work, location privacy is a key to resolve possible real-world accusations. In a traditional direction of research, pseudonyms are used to protect against attackers that try linking several pseudonyms in order to construct movement profiles and comprehensive user traces. In early work, Kesdogan et al. [33] proposed to use multiple short-lived, thus changing pseudonyms in mobile GSM networks. Beresford et al. [4] combined the use of changing pseudonyms with an geographic abstraction of mixnets, to form so called mix-zones. For users of location-based services, a mix-zone is a region without service use, in which the actual pseudonym change is done, to hinder profiling. Recent follow up work [22] addresses non-cooperative location privacy models and evaluates the effect of unsynchronized pseudonym changes on the degree of anonymity achieved. A bunch of efficient special purpose pseudonym constructions have been proposed, e.g. for RFID applications. Henrici et al. [29] propose a hash-based construction of pseudonyms, which allows for implementing changing pseudonyms. Gruteser et al. [26] also use hash-based constructions, called hash-chains, to construct short-lived pseudonyms. Comparable to our work, Juels et al. [32], use public key encryption and argue that this approach is efficient even for lightweight RFID applications, w.r.t. privacy protection. Notably, Heinemann [28] proposes to implement privacy-respecting opportunistic networks based on changing pseudonyms, whereby he proclaims that identifiers must be changeable within every communication layer. A different use of pseudonyms is presented by Delakouridis et al. [14], applying pseudonyms to the problem of storing and accessing location information in a privacy-preserving, decentralized manner. While our work shares the idea of using pseudonyms as reference points for data access, they propose to split the information to be protected according to Shamir secret sharing [47], and to distribute those shares on several servers, addressable via pseudonyms.

8.3 Privacy-Respecting Audit Log Analysis

The use of pseudonyms in audit logs was first suggested by Fischer-Hübner et al. [20]. Pseudonymous auditing is now a widely recognized approach to balance the conflicting security requirements of accountability and privacy, and often combined with intrusion detection systems, that automatically analyze pseudonymized logs [48, 21]. The analysis of pseudonymous logs inherently requires means for

linking the pseudonyms to each other, and finally to users. Research in this direction is about finding efficient mechanisms and models of operations. Biskup et al. propose to use transaction pseudonyms [6] in audit logs and a secret sharing method for the re-identification [5] in case a threshold of detected inappropriate actions is exceeded in the analysis. These concepts are applied within traditional computer security domains like Unix audit logs. We extend the application perspective to real-world audit logs, that emerge from location tracking applications. Technically, we also propose a new approach building on efficient secure multiparty computation techniques that we apply on the pseudonym level. The inherent use of verifiable threshold cryptography and reencryption mixnets, techniques with a long tradition of research in the area of cryptographic protocols, also allows us to provide a second level of auditability, in order to achieve multilateral security.

9 Summary and Conclusions

In this chapter, we presented and discussed a novel approach for realizing multilaterally secure auditing functionalities. The approach is tailored to be employed in location tracking applications and Ubiquitous Computing scenarios. Especially, we motivated our work by collaborative mission-critical applications. In this context, we proposed to realize so called multilaterally secure mission logs, which actually extend the traditional concept of computer audit logs to real-world audit logs. Hereby, we take into account the trend that computers pervade more and more parts of our everyday life and work, which broadens the actual scope of logging and auditing possibilities and also *required functionalities*.

On a conceptual level, our work combines pseudonyms with secure multiparty computation, both classic examples in the realm of privacy-enhancing technologies. Nevertheless, making them work in real-world application scenarios is a challenging area of research. Our approach builds on the principle of *accountability by auditability*. We employ it on two conceptual layers, first regarding real-world actions of mobile users as well as regarding the use of auditing functionalities by audit officers. Additionally, we support the individual user by enabling her to repudiate false accusations by means of log attestation. We also take into account a broader legal perspective. The lawful disclosure functionality allows a single attorney authority to globally revoke privacy protection of individual users. Regulations in some application domains, e.g. that of emergency management, demand such a functionality. However, in the light of key escrow discussions [1], we stress that it is also possible to instantiate our scheme without that property. We believe that the presented approach and its flexibility to tailor it to concrete application needs is a step towards the realization of multilaterally secure thus multilaterally acceptable UbiComp systems. Addressing inherent tradeoffs already in the construction of technologies that pervade everyday life more and more is essential for their acceptance. The introduction of new technologies should always comply with legal and social backgrounds.

Our general approach to deal with this issue is to analyze concrete application scenarios. Mission-critical applications, along with their multilaterally demanding requirements, are an important example to learn how to design ICT support for a *seamless collaboration*.

Acknowledgements. This work was supported by CASED (www.cased.de). The authors are responsible for the content of this publication.

References

1. Abelson, H., Anderson, R., Bellovin, S.M., Benaloh, J., Blaze, M., Diffie, W., Gilmore, J., Neumann, P.G., Rivest, R.L., Schiller, J.I., Schneier, B.: The Risks of Key Recovery, Key Escrow, and Trusted Third Party Encryption (1998), `http://www.cdt.org/crypto/risks98/`
2. Aitenbichler, E., Kangasharju, J., Mühlhäuser, M.: MundoCore: A Light-Weight Infrastructure for Pervasive Computing. Pervasive and Mobile Computing 3(4), 332–361 (2007)
3. Anderson, R.J.: Security Engineering: a Guide to Building Dependable Distributed Systems. John Wiley & Sons, Chichester (2008)
4. Beresford, A.R., Stajano, F.: Location Privacy in Pervasive Computing. IEEE Pervasive Computing 02(1), 46–55 (2003)
5. Biskup, J., Flegel, U.: Threshold-Based Identity Recovery for Privacy Enhanced Applications. In: ACM Conference on Computer and Communications Security, pp. 71–79. ACM, New York (2000)
6. Biskup, J., Flegel, U.: Transaction-Based Pseudonyms in Audit Data for Privacy Respecting Intrusion Detection. In: Debar, H., Mé, L., Wu, S.F. (eds.) RAID 2000. LNCS, vol. 1907, pp. 28–48. Springer, Heidelberg (2000)
7. Burmester, M., Desmedt, Y., Wright, R.N., Yasinsac, A.: Accountable Privacy. In: Security Protocols Workshop 2004, pp. 83–95. Springer, Heidelberg (2004)
8. Camenisch, J., Lysyanskaya, A.: An Efficient System for Non-Transferable Anonymous Credentials with Optional Anonymity Revocation. In: Pfitzmann, B. (ed.) EUROCRYPT 2001. LNCS, vol. 2045, pp. 93–118. Springer, Heidelberg (2001)
9. Cas, J.: Privacy in Pervasive Computing Environments - A Contradiction in Terms? IEEE Technology and Society Magazine 24(1), 24–33 (2005)
10. Chaum, D.: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. Communications of the ACM 24(2), 84–88 (1981)
11. Chaum, D., Pedersen, T.P.: Wallet Databases with Observers. In: Brickell, E.F. (ed.) CRYPTO 1992. LNCS, vol. 740, pp. 89–105. Springer, Heidelberg (1993)
12. Cramer, R., Damgard, I., Schoenmakers, B.: Proofs of Partial Knowledge and Simplified Design of Witness Hiding Protocols. In: Desmedt, Y.G. (ed.) CRYPTO 1994. LNCS, vol. 839, pp. 174–187. Springer, Heidelberg (1994)
13. Cramer, R., Gennaro, R., Schoenmakers, B.: A Secure and Optimally Efficient Multi-Authority Election Scheme. In: Fumy, W. (ed.) EUROCRYPT 1997. LNCS, vol. 1233, pp. 103–118. Springer, Heidelberg (1997)
14. Delakouridis, C., Kazatzopoulos, L., Marias, G.F., Georgiadis, P.: Share The Secret: Enabling Location Privacy in Ubiquitous Environments. In: Strang, T., Linnhoff-Popien, C. (eds.) LoCA 2005. LNCS, vol. 3479, pp. 289–305. Springer, Heidelberg (2005)

15. Duckham, M., Kulik, L.: Location Privacy and Location-Aware Computing. In: Dynamic & Mobile GIS: Investigating Change in Space and Time, pp. 34–51. CRC Press, Boca Raton (2006)
16. ElGamal, T.: A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. IEEE Transactions on Information Theory 31(4), 469–472 (1985)
17. Ferguson, N., Schneier, B.: Practical Cryptography. Wiley Publishing, Inc., Chichester (2003)
18. Fiat, A., Shamir, A.: How to Prove Yourself: Practical Solutions to Identification and Signature Problems. In: Odlyzko, A.M. (ed.) CRYPTO 1986. LNCS, vol. 263, pp. 186–194. Springer, Heidelberg (1987)
19. Fischer-Hübner, S.: Pseudonymity. In: Encyclopedia of Database Systems, p. 2207 (2009)
20. Fischer-Hübner, S., Brunnstein, K.: Combining Verified and Adaptive System Components Towards More Secure System Architectures. In: Workshop on Computer Architectures to Support Security and Persistance of Information. Springer, Heidelberg (1990)
21. Flegel, U.: Privacy-Respecting Intrusion Detection. Springer, Heidelberg (2007)
22. Freudiger, J., Manshaei, M.H., Hubaux, J.-P., Parkes, D.C.: On Non-Cooperative Location Privacy: a Game-Theoretic Analysis. In: ACM Conference on Computer and Communications Security, pp. 324–337. ACM, New York (2009)
23. Furukawa, J., Sako, K.: An Efficient Scheme for Proving a Shuffle. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 368–387. Springer, Heidelberg (2001)
24. Goldwasser, S., Micali, S., Rackoff, C.: The Knowledge Complexity of Interactive Proof-Systems. SIAM Journal on Computing 18(1), 186–208 (1989)
25. Greenstein, B., McCoy, D., Pang, J., Kohno, T., Seshan, S., Wetherall, D.: Improving Wireless Privacy with an Identifier-Free Link Layer Protocol. In: Conference on Mobile Systems, Applications, and Services (MobiSys 2008), pp. 40–53. ACM, New York (2008)
26. Gruteser, M., Grunwald, D.: Enhancing Location Privacy in Wireless LAN through Disposable Interface Identifiers: a Quantitative Analysis. Mob. Netw. Appl. 10(3), 315–325 (2005)
27. Hartmann, M., Austaller, G.: Context Models and Context-Awareness. In: Ubiquitous Computing Technology for Real Time Enterprises, pp. 235–256. IGI Global Publisher (2008)
28. Heinemann, A.: Collaboration in opportunistic networks. Ph.D. thesis, Technische Universität Darmstadt (2007)
29. Henrici, D., Müller, P.: Hash-Based Enhancement of Location Privacy for Radio-Frequency Identification Devices Using Varying Identifiers. In: Conference on Pervasive Computing and Communications Workshops (PERCOMW 2004). IEEE Computer Society, Los Alamitos (2004)
30. Hirt, M.: Multi-party computation: Efficient protocols, general adversaries, and voting. Ph.D. thesis, ETH Zurich (September 2001), `ftp://ftp.inf.ethz.ch/pub/crypto/publications/Hirt01.pdf`
31. Jakobsson, M., Juels, A.: Mix and Match: Secure Function Evaluation via Ciphertexts (Extended Abstract). In: Okamoto, T. (ed.) ASIACRYPT 2000. LNCS, vol. 1976, pp. 162–177. Springer, Heidelberg (2000)
32. Juels, A., Pappu, R.: Squealing Euros: Privacy Protection in RFID-Enabled Banknotes. In: Wright, R.N. (ed.) FC 2003. LNCS, vol. 2742, pp. 103–121. Springer, Heidelberg (2003)

33. Kesdogan, D., Federrath, H., Jerichow, A., Pfitzmann, A.: Location Management Strategies Increasing Privacy in mobile Communication. In: IFIP International Information Security Conference (SEC 1996), pp. 39–48. Chapman & Hall, Boca Raton (1996)
34. Koeune, F.: Pseudo-Random Number Generator. In: Encyclopedia of Cryptography and Security, pp. 485–487 (2005)
35. Lindell, Y., Pinkas, B.: Secure Multiparty Computation for Privacy-Preserving Data Mining. Journal of Privacy and Confidentiality 01(01), 59–98 (2009)
36. Martucci, L.A., Kohlweiss, M., Andersson, C., Panchenko, A.: Self-Certified Sybil-Free Pseudonyms. In: Conference on Wireless Network Security (WISEC 2008), pp. 154–159. ACM, New York (2008)
37. Mühlhäuser, M., Gurevych, I. (eds.): Ubiquitous Computing Technology for Real Time Enterprises - Handbook of Research. IGI Global Publisher (2008)
38. Mühlhäuser, M., Hartmann, M.: Interacting with Context. In: Rothermel, K., Fritsch, D., Blochinger, W., Dürr, F. (eds.) QuaCon 2009. LNCS, vol. 5786, pp. 1–14. Springer, Heidelberg (2009)
39. Park, C., Itoh, K., Kurosawa, K.: Efficient Anonymous Channel and All/Nothing Election Scheme. In: Helleseth, T. (ed.) EUROCRYPT 1993. LNCS, vol. 765, pp. 248–259. Springer, Heidelberg (1994)
40. Pedersen, T.P.: A Threshold Cryptosystem without a Trusted Party (Extended Abstract). In: Davies, D.W. (ed.) EUROCRYPT 1991. LNCS, vol. 547, pp. 522–526. Springer, Heidelberg (1991)
41. Pfitzmann, A.: Multilateral Security: Enabling Technologies and Their Evaluation. In: Müller, G. (ed.) ETRICS 2006. LNCS, vol. 3995, pp. 1–13. Springer, Heidelberg (2006)
42. Pfitzmann, A., Hansen, M.: A Terminology for Talking about Privacy by Data Minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management. V0.32 (December 2009), `http://dud.inf.tu-dresden.de/Anon_Terminology.shtml`
43. Rannenberg, K.: Multilateral Security - a Concept and Examples for Balanced Security. In: Workshop on New Security Paradigms (NSPW 2000), pp. 151–162. ACM, New York (2000)
44. Satyanarayanan, M.: Privacy: The Achilles Heel of Pervasive Computing? IEEE Pervasive Computing 2(1), 2–3 (2003)
45. Schlott, S.: Privacy- und sicherheitsaspekte in ubiquitaeren umgebungen. Ph.D. thesis, Universität Ulm (2008)
46. Schneier, B., Kelsey, J.: Secure Audit Logs to Support Computer Forensics. ACM Trans. Inf. Syst. Secur. 2(2), 159–176 (1999)
47. Shamir, A.: How to Share a Secret. Communications of the ACM 22(11), 612–613 (1979)
48. Sobirey, M., Fischer-Hübner, S., Rannenberg, K.: Pseudonymous Audit for Privacy Enhanced Intrusion Detection. In: IFIP International Information Security Conference (SEC 1997), pp. 151–163. Chapman & Hall, Boca Raton (1997)
49. Stajano, F.: Security Issues in Ubiquitous Computing. In: Handbook of Ambient Intelligence and Smart Environments, pp. 281–314. Springer, Heidelberg (2010)
50. Tsiounis, Y., Yung, M.: On the Security of ElGamal based Encryption. In: Imai, H., Zheng, Y. (eds.) PKC 1998. LNCS, vol. 1431, pp. 117–134. Springer, Heidelberg (1998)
51. Waters, B.R., Balfanz, D., Durfee, G., Smetters, D.K.: Building an Encrypted and Searchable Audit Log. In: Network and Distributed System Security Symposium (NDSS 2004). The Internet Society (2004)

52. Weber, S.G.: Harnessing Pseudonyms with Implicit Attributes for Privacy-Respecting Mission Log Analysis. In: Conference on Intelligent Networking and Collaborative Systems (INCoS 2009), pp. 119–126. IEEE Computer Society, Los Alamitos (2009)
53. Weber, S.G.: Securing First Response Coordination with Dynamic Attribute-Based Encryption. In: World Congress on Privacy, Security, Trust and the Management of e-Business (CONGRESS 2009), pp. 58–69. IEEE Computer Society, Los Alamitos (2009)
54. Weber, S.G., Heinemann, A., Mühlhäuser, M.: Towards an Architecture for Balancing Privacy and Traceability in Ubiquitous Computing Environments. In: Workshop on Privacy and Assurance (WPA 2008) at Conference on Availability, Reliability and Security (ARES 2008), pp. 958–964. IEEE Computer Society, Los Alamitos (2008)
55. Weber, S.G., Ries, S., Heinemann, A.: Inherent Tradeoffs in Ubiquitous Computing Services. In: INFORMATIK 2007. LNI, vol. P109, pp. 364–368. GI (September 2007)
56. Weiser, M.: The Computer for the 21st Century. Scientific American 265(3), 94–104 (1991)
57. Yao, A.C.: Protocols for Secure Computations (Extended Abstract). In: 23th Annual Symposium on Foundations of Computer Science (FOCS 1982), pp. 160–164. IEEE Computer Society Press, Los Alamitos (1982)