Concepts and Scheme for Multilaterally Secure, User-Friendly Attribute-Based Messaging

21.10.2010

Stefan G. Weber, Sebastian Ries, Max Mühlhäuser

TECHNISCHE UNIVERSITÄT DARMSTADT

21.10.2010

Technical Report No. TUD-CS-2010-2381
Technische Universität Darmstadt

Telecooperation Report No. TR-13,
The Technical Reports Series of the TK Research Division, TU Darmstadt
ISSN 1864-0516
http://www.tk.informatik.tu-darmstadt.de/de/publications/

Concepts and Scheme for Multilaterally Secure, User-Friendly Attribute-Based Messaging

Stefan G. Weber[1,2], Sebastian Ries[1,2] Max Mühlhäuser[1,2]

[1] Telecooperation Group, TU Darmstadt,
Hochschulstrasse 10, 64289 Darmstadt, Germany
[2] CASED, Mornewegstrasse 32, 64293 Darmstadt, Germany
{firstname.lastname}@cased.de

Abstract. Efficient emergency communication is of high practical importance, but has specific challenges: unpredictable local emergency situations harden the establishment of communication structures, legal requirements dictate the use of end-to-end secure and documentable approaches, while end users demand user-friendliness. Dealing with these challenges, the contribution of this paper is three-fold: first, together with emergency practioners we define security requirements and patterns for efficient communication. Second, we propose a new hybrid encryption technique for expressive policies, which efficiently combines ciphertext-policy attribute-based encryption with location-based encryption. Third, we devise a multilaterally end-to-end secure, user-friendly attribute-based messaging scheme for one-to-many communication. The application of the new encryption technique enables to harness continuous dynamic location attributes as user-friendly selectors for targeted messaging with dynamic groups of mobile and anonymous receivers.
Key words: Attribute-Based Messaging, Attribute-Based Encryption, Mobile Communication Security, User-Friendly Security

1 Introduction

Mobile communication has become an integral part of our modern information society. Personal communication devices enable locally distributed users to participate in communication contexts of everyday's life and work. In some application scenarios, such communication means even constitute a critical service: considering e.g. the case of a sudden emergency, efficient communication support often means the difference between success and failure of rescue missions, possibly between life and death of affected persons and between the loss and safeguard of infrastructure and property. Currently, dedicated digital communication networks for emergency communications are under establishment, e.g. in Europe according to the TETRA standard[3], promising to reliably connect organizations, parties and individuals involved in rescue efforts. Such networks require adequate security mechanisms, yet their final realization and secure use

[3] Cf. www.tetramou.com

still raise a number of major research challenges. Two of these challenges are the implementation of *multilateral secure* and *user-friendly* security mechanisms. The first objective accentuates that secure systems need to consider the security goals of all involved parties [16], in and along with legal and individual usage contexts. The latter one points out that "the goal (..) is not to build systems that are theoretically securable, but to build systems that are actually secure" [21] when real users deal with them in real application scenarios. We resort to these issues, stating that the realization of a (mostly ideal) system for secure mobile and pervasive one-to-many communication does not only require paying attention to several explicit security requirements like mutual authentication and end-to-end encryption, but also to the more implicit security requirement of user-friendliness of the mechanisms. This paper addresses the research question, whether and how it is possible to design and realize a multilaterally secure yet practical approach that enables pervasive communication in dynamic scenarios *at ease*.

Our Approach and Contributions: We follow the approach that designing user-friendly security mechanisms in this application context requires *first* identifying human-adequate levels of abstraction and communication patterns and *second* realizing them in an end-to-end secure and efficient manner. Thus, in the first part of this work, we derive realistic use cases and security requirements for emergency one-to-many communication, by taking into account experiences with real users as well as legally implied security requirements. Based on these findings, in the second part, we propose a novel end-to-end secure attribute-based messaging scheme. As a main building block, we introduce a new hybrid encryption technique for expressive logical policies. It efficiently combines ciphertext-policy attribute-based encryption and location-based encryption. Applying it on the end-to-end encryption layer of the TETRA security infrastructure allows to realize the envisioned ABM scheme. Overall, the proposed concepts enable the realization of communication mechanisms that are *user-friendly*, i.e. supporting intuitive communication even with dynamic groups of mobile and anonymous receivers, by introducing location as a human-adequate level of abstraction into the selection of receivers; *multilaterally end-to-end secure*, i.e. combining end-to-end confidential messaging with documentation and accountability means as they are required in the emergency communication domain, while also handling replay attacks on the end-to-end-encryption layer; *practical*, i.e. complying with identified real emergency communication patterns, while being efficient for the use with a wide range of mobile devices.

Traditionally, end-to-end encryption layers only protect user data against confidentiality threats. Within our attribute-based messaging (ABM) scheme, the end-to-end encryption layer is also used as a *key management and identity abstraction layer*. While this work advances the study of secure attribute-based messaging systems, it also details practical methods for cryptographic key and access control management in large-scale distributed systems.

The remainder of this paper is structured as follows. Section 2 describes related work. Section 3 analyses emergency communication and sets up require-

ments. Afterwards, building blocks are presented in section 4. Then, a novel hybrid encryption technique is introduce in section 5. A complete ABM scheme is described in section 6. The concepts are discussed and evaluated in section 7. Finally, the paper is concluded in section 8.

2 Related Work

Previous related work on secure and confidential one-to-many messaging started with the introduction of secure role-based messaging [7, 12]. The scheme [7] allows specifying the recipients of a message based on a single organizational role. It employs traditional PKI and RBAC [18] authorization concepts, but does not achieve end-to-end encryption, since a trusted entity is required for each message decryption. The proposal [12] allows to combine several roles to form a logical policy for recipient selection. The scheme builds on identity-based encryption [10], such that logical policies are mapped to single cryptographic keys. Furthermore, it requires interaction with an online trust authority to receive a message decryption key.

In [3], the concept of attribute-based messaging was presented. It allows to logically specify the group of receivers of a message in form of a flexible combination of attributes. It is a natural generalization of role-based messaging. The approach builds on ABAC [24] as main security mechanism and does not provide end-to-end encryption. After the introduction of attribute-based encryption techniques [17, 11], end-to-end encrypted attribute-based messaging schemes [23, 4] were proposed. Both schemes employ ciphertext-policy attribute-based encryption [1], which allows for a flexible cryptographic encoding of logical policies. Especially, [4] extends [3], by integrating encryption into ABAC mechanisms, but did not address handling of dynamic attributes.

Generally, the application of ABE enables a flexible specification of receivers and content. Yet, due to the inherent use of computational demanding pairing-based cryptography, the practical applicability of ABE concepts in scenarios with mobile and resource-constrained devices remains highly challenging.

We presented our first proposal of an attribute-based messaging scheme for emergency communication in [23, 22, 6]. While it was limited w.r.t. handling continuous dynamic attributes, a prototype was used to initiate discussions with real users, enabling a cognitive walkthrough[4][2] of typical emergency communication scenarios. This paper presents a major revision, extension and follow up work on our previous research. To the best of our knowledge, we are the first to address the complex issue of enabling multilaterally end-to-end secure yet user-friendly one-to-many communication through attribute-based messaging in a realistic scenario under practical assumptions.

[4] A cognitive walkthrough, an usability evaluation method, builds on practical user experiments with a system. This helped to understand how real users interact by and with an emergency communication system. Findings contributed to section 3.

3 Analysis of Emergency Communication

From experiences and discussions with real users (first responders, decision makers and trainers from police and fire departments as well as relief organizations), we extracted the characteristics of emergency communications. This resulted in a set of main communication patterns (`CPs`) and a set of security requirements (SReqs) that are presented in this section.

Communication Patterns: Generally, the participation in a disaster response depends on both the nature and location of the disaster. In order to handle large-scale disasters, several parties and organizations also need to collaborate and communicate based on location (`CP1: Communication through location addressing`). Some rescue efforts require the participation of local relief agencies, while others require local specialists to participate. Some parties are involved in most responses, like fire and police departments, but since the geographical scope of a disaster cannot be pre-determined before it actually happens, the real identities of responsible people are not directly clear (`CP2: Requests to unknown entities`). The same is true on lower levels, when decision makers need to communicate with local groups of first responders, the actual identities are not known beforehand, or groups are even dynamically formed (`CP3: Communication with dynamic groups of entities`). Also, in some cases, information has to be deposited for entities that are known to join operations in future (`CP4: Deposition of information for future use`).

Security Requirements: In emergency communication, mutual authentication, message integrity, availability and revocation of devices are basic requirements, detailed by the TETRA standard (`SReq1: Basic security`). Beyond that, preserving end-to-end confidentiality through encryption (`SReq2: End-to-end encryption`) is mandatory, also means that protect against replay attacks (`SReq3: Protection against replay attacks`) are required. Emergency communication legally requires to document who sent messages (`SReq4: Accountability of senders`) and who received and read messages, requests and commands (`SReq5: Documentation of readers`). Security mechanisms also need to be suitable for resource-constrained mobile devices that are widely used in emergency communications (`SReq6: Efficiency of security mechanisms`). In order to foster end user acceptance, mechanisms must be user-friendly (`SReq7: User-friendliness of security mechanisms`). For senders, this implies minimum learning efforts and an intuitive use. Since many participants involved in responses, like specialists, doctors or volunteers, are only available on request via their mobile communication devices, receiver participation also depends on a seamless integratability into personal lives, i.e. especially receivers prefer not to be continuously tracked.

3.1 Sketch of Solution

The last section detailed the central research question: how to enable a sender to securely and comfortably communicate with unknown receivers, that may locally form dynamic groups? This section gives a first sketch of our proposed solution.

For a sender in a certain messaging task, it is not immediately known with which actual parties and entities to communicate, but the sender can elaborate *which kind* of organizations, roles and specializations are appropriate and *where* they should be present. Thus, we propose to allow the sender to specify the group of intended receivers of a message on a high level of abstraction. Especially, we propose to use the *selectors* as depicted in figure 1 in logical combination. Such a logical combination is what we call a *logical messaging policy*. It is used to specify the group of receivers in the messaging.

Fig. 1. Proposed Logical Selectors for One-to-Many Communication

Communication mechanisms that allow for a flexible highlevel specification of receivers in form of an attribute-based description are known as attribute-based messaging (ABM) [3, 23, 4]. The ABM concept potentially allows to implement a single approach that handles all major communication patterns, minimizing learning efforts and may combine the selection of location and further attributes. In order to realize secure ABM, we can make use of the existing TETRA security infrastructure, which provides basic security services for emergency communication and implies the existence of secure mobile devices on the receiver side. However, realizing the required end-to-end security leads to new challenges: traditional asymmetric encryption schemes and PKI concepts are not practical for communication with dynamic groups of unknown receivers. Especially, they do not provide the required flexibility and means for expressing complex policies. To overcome these issues, we propose to leverage ciphertext policy attribute-based encryption (CP-ABE) [1]. This is a recent asymmetric certificate-less encryption technique that directly supports a cryptographic realization of flexible *attribute*[5] *policies*. Yet, CP-ABE has practical limitations w.r.t. the handling of dynamic and continuous attributes. In emergency management, the use of augmented digital maps is inherent [8]. An integration of location selection into a digital map, illustrated in figure 2, was proposed by real users as a basic mean for intuitive use.

Fig. 2. Location Selection on Digital Map

In the following, we introduce our concepts that enable to practically and securely incorporate location into receiver selection. They are used to devise a novel attribute-based messaging scheme.

[5] Note that the cryptographic attributes of CP-ABE techniques are not equal to the logical attributes/selectors of ABM schemes, but belong to different conceptual layers of the messaging system.

4 Building Blocks

In this section, we introduce important building blocks of our work, namely the TETRA security architecture and employed encryption techniques.

4.1 TETRA Security Architecture

TETRA (Terrestrial Trunked Radio System) is an open standard for digital radio [15]. It has been adopted in emergency communications by a number of national European administrations. It was especially designed with security as one of its principal features, including mutual authentication, air interface encryption and disabling of mobile devices. However, in its basic form, it only protects the air interface layer. Thus, additional, end-to-end encryption mechanisms are required for application contexts with end-to-end confidentiality requirements. The end-to-end encryption key management is in the user domain, especially, the underlying key management infrastructure is unable to decode end-to-end encrypted messages or access the end-to-end keys.

For the receivers, we assume that they are equipped with mobile communication devices, that provide a digital communication channel to operational headquarters by means of TETRA. The mobile devices are uniquely identifiable and equipped with dedicated smart cards including TPM chips, rendering them tamper-resistant. End-to-end encryption keys are individually issued, e.g. along with the distribution of these devices.

In the following, we focus on broadcast-based one-to-many communication between a sender in an operational headquarter and mobile receivers. Since the TETRA communication infrastructure does not provide confidential point-to-point channels, end-to-end security of broadcasted messages is guaranteed by means of end-to-end encryption layer security mechanisms.

4.2 Ciphertext Policy Attribute-Based Encryption

Attribute-based encryption (ABE) [17] is an encryption technique which generalizes the functional role of identities and keys. In traditional asymmetric encryption schemes, identities relate to distinct public key / private key tuples. In ABE, both public key and private key concepts are replaced by *sets of attributes*, which abstract from actual user properties. Moreover, ABE is certificateless and the cryptographic credentials are issued by a central trusted party called *attribute authority*, which is in possession of a global *master key* for key generation. Since users are associated with sets of attributes, they might try to trade some attributes and related private key components to gain more decryption powers. However, ABE systems are *collusion resistant* [1], i.e. keys of different users are incompatible due to the cryptographic construction. Like identity-based encryption, ABE cryptographically builds on pairings [5], i.e. bilinear maps that provide an extra structure on special elliptic curves. While pairings enable attribute-based encryption, they are inherently computational

demanding. From a practical point of view, the goal is to minimize pairing-related operations, in order to enable use on resource-constraint devices.

Ciphertext policy attribute-based encryption (CP-ABE) [1] is a special form, which associates a set of attributes used in the encryption process with logical access structures[6], also called *attribute policies*. Thus, the encryption algorithm takes as input a message and an attribute policy. The algorithm encrypts the message and produces a ciphertext, such that only a receiver possessing a set of attributes that satisfies the attribute policy is able to decrypt that message. In the following, we assume that the ciphertext implicitly contains the policy. In practical applications, CP-ABE is used as *hybrid encryption*: a message itself is encrypted with a random symmetric secret key. Only this *session key* is then CP-AB encrypted under a policy.

CP-ABE concepts can be the basis to realize a combined cryptographic *key management and identity abstraction layer*, which makes them interesting for the use in messaging applications. However, CP-ABE alone is practically inefficient for handling of dynamic attributes, i.e. attributes that change their values of time, with continuous values, like location.

4.3 Location-Based Encryption

The concept of location-based encryption (LBE) according to [19, 9] aims at securing mobile communication by limiting the area inside which the intended recipient can actually decrypt a message. In order to implement this, it adds a layer of security to the symmetric encryption of a message: the session key is combined with the targeted recipient's geographic location L, producing a location-locked key, which is then sent along with the encrypted message.

As a result, the ciphertext can only be decrypted if the session key can be recovered from the location-locked key. In turn, LBE requires that this is only possible if the receiver's device is physically presented at location L, or respectively inside an geographic area associated with L. Location verification hinges on a tamper-resistant GPS receiver inside the recipient's mobile device.

In LBE, the sender has to transmit parameters which define the area where decryption is permitted and may specify further dynamic constraints like time periods or receiver velocity that have to be verified upon decryption. In general, location-based encryption techniques require an efficient mapping from location areas to symmetric keys, which is called *location lock* in the following.

5 Hybrid Encryption Technique for Expressive Policies

In this section, we introduce a new efficient hybrid encryption technique for expressive policies. The technique is hybrid, as it combines CP-ABE with LBE on the level of symmetric keys. It enables to encrypt under expressive policies,

[6] Due to the use of secret sharing [20], the access structures are trees with nodes that represent t-out-of-n combinations of attribute child nodes, naturally including conjunctions (n-out-of-n) and disjunctions (1-out-of-n).

since it can efficiently handle logical attributes with continuous values, like location[7]. We use the following notation: $E_{AP}^{L^{(P_1,P_2)}}(M)$ denotes the encryption of a message M under a logical conjunction of a CP-ABE attribute policy AP and a LBE location area attribute $L^{(P_1,P_2)}$. Hereby, $L^{(P_1,P_2)}$ specifies an geographic area with the shape of an rectangle, defined by GPS coordinates $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$. Finally, $D_{\{A\}_R}^{P_R}(CT)$ denotes the decryption of a ciphertext CT initiated by a receiver R, using his private attribute set $\{A\}_R$, while being positioned at GPS coordinate $P_R = (x_R, y_R)$. Decryption succeeds if R's attribute set $\{A\}_R$ satisfies the attribute policy AP and R is positioned within $L^{(P_1,P_2)}$, i.e. if $x_2 \geq x_R \geq x_1$ and $y_2 \geq y_R \geq y_1$ hold. Figure 3 depicts the basic operations of the encryption technique. It employs a *location lock mapping* $f_{LL}(L^{(P_1,P_2)})$, according to the following principle: first, GPS coordinates P_1, P_2 are concatenated. Second, the resulting string $s_{LL^{(P_1,P_2)}} = x_1||y_1||x_2||y_2$ is hashed, $h(s_{LL^{(P_1,P_2)}})$, to a 128 bit string[8], the location lock value. The *hybrid encryption scheme* works as follows: first, a random session key Key_S is generated. Second, the message is symmetrically encrypted under Key_S, producing ciphertext CT_1. Third, Key_S is XORed with the location lock value, generating a hybrid key Key_H. Fourth, the output is concatenated with an encoding of the location area. Fifth, the resulting string is CP-AB encrypted under an attribute policy AP, producing ciphertext CT_2. CT_1 concatenated with CT_2 form the ciphertext CT. CT is transferred to a receiver R. The *scheme for hydrid decryption* works as follows: first, receiver R tries to decrypt CT_2, using his private attribute set $\{A\}_R$. Second, on successful decryption, the location area $s_{LL^{(P_1,P_2)}}$ is extracted. Third, R's current GPS position P_R is verified to be inside the location area by means of a tamper-resistant GPS receiver. On success, the location lock value is computed. It is then XORed with the recovered Key_H, in order to reconstruct Key_S. Finally, Key_S is used to symmetrically decrypt CT_1 to M.

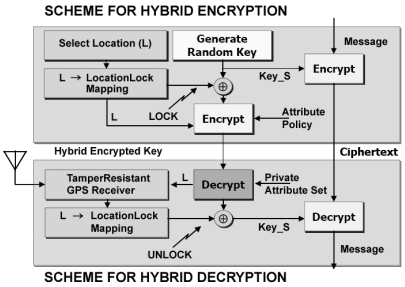

Fig. 3. Overview of Hybrid Encryption Technique for Expressive Policies

6 Approach to Attribute-Based Messaging

In this section, we describe our overall ABM approach in a conceptual and schematic view.

[7] We restrict the description to location, however, further continuous attributes can be handled analogous.

[8] We assume 128 bit symmetric keys.

6.1 Conceptual View

Our approach consists of two main conceptual layers: on the *logical messaging policy layer*, senders specify logical messaging policies, in order to select receivers in the communication via an ABM system. The *access control layer* provides security mechanisms that enforce the logical constraints specified by the messaging policies. It employs encryption techniques and tamper-resistant access control support mechanisms.

Logical Messaging Policy Layer: When interacting with the ABM system, in any messaging act, a sender selects attributes representing organizations (e.g. police), roles (e.g. group leader) and specializations (e.g. specialist for toxic matters), from a central attribute database. The sender also selects a location area (cf. figure 2) or a specific location, e.g. a city by name, as a logical attribute. The sender has in principle flexibility[9] in combining the logical attributes. We omit details here, yet, we set up the basic construction rule for messaging policies, that a location attribute shall always be used in conjunction with at least one further attribute. Also, the sender has to select a communication pattern from `CP1,..,CP4`.

Fig. 4. Simple policy

Access Control Layer: Dependent on the selection of the communication pattern, the access control layer chooses an enforcement method: direct communications (`CP1,CP3`) and requests (`CP2`) are secured using the hybrid encryption technique (cf. section 5), depositions (`CP4`) are handled with CP-ABE[10] (cf. section 4.2). In the following, descriptions focus on the realization of `CP1-CP3`.

6.2 Schematic View

We next detail registration and messaging phases of the ABM scheme[11]. We denote the entities in the scheme: AA, a central attribute authority, S, a sender, R, a receiver. Beyond that, the following system components are involved: $RegL$, a registration list, ML, a message log and RL, a readers list. Log and lists are append-only.

Registration Phase: In this phase, each relevant receiver interacts with the AA in order to receive a private attribute set $\{A\}_R$. Upon proof of eligibility, the AA creates attributes according to organization and role memberships as well as specializations that R actually satisfies. $\{A\}_R$ is transferred to R's personal mobile device for emergency communication. In turn, R's distinct mobile

[9] Logical disjunctions as root node are also possible. The system would resolve this into several messaging acts with the same content.

[10] In this case, location attributes are not necessarily continuous, enabling direct mapping to CP-ABE policies, even as combined attributes, e.g. PoliceHonululu.

[11] For simplicity reasons, we omit setup and auditing phases.

subscriber identity ($IMSI_R$) is added to the registration list $RegL$, along with the real world identity and assigned attributes. In this phase, R also receives a key for symmetric encryption of replys, K^{RS}_{Ack}, and registers two keys for mutual message authentication with S, denoted K^{R}_{MAC} and K^{S}_{MAC}.

Messaging Phase: The messaging phase is depicted figure in 5. Basically, it consists of a broadcast of an end-to-end encrypted message M_{E2E} and answer back steps. Messages and acknowledged readers are documented on ML and RL. The end-to-end encryption incorporates a unique message ID, ID_M, to prevent replay attacks, symmetric accountability is supported by MACs.

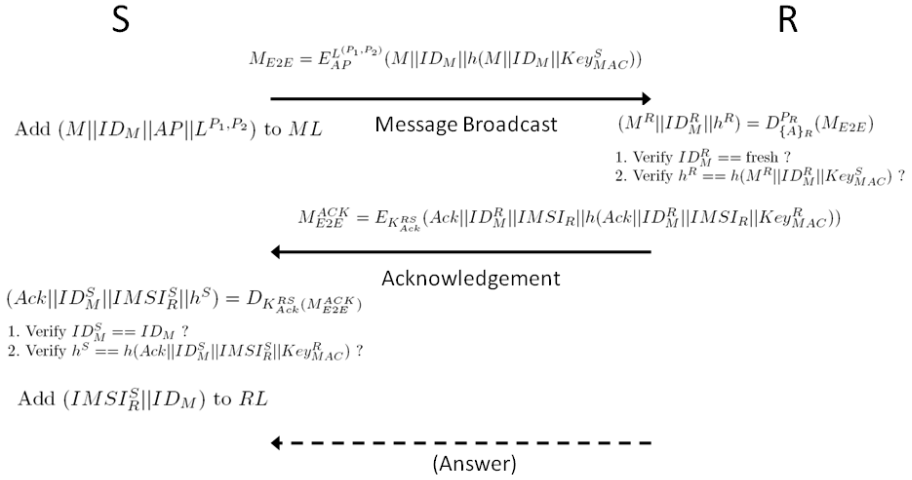

Fig. 5. Protocol for Messaging Phase

7 Security Analysis

This section sketches the security analysis of the proposed concepts.

7.1 Discussion of Hybrid Encryption Technique

The design of the hybrid encryption technique follows two main goals: efficiency in handling continuous attributes and minimizing trust in attribute authorities. First, handling dynamic attributes requires means for providing keys on mobile devices. An *online AA* could principally solve the problem, but does not scale. An *offline AA* only allows handling dynamic attributes by pre-registering all

possible attributes to a local trusted activator. This is inefficient for continuous attributes. An *embedded AA* could be implemented locally on tamper-resistant hardware. However, it locally requires the master key and could generate all attributes of all users, such that the key escrow risk associated to a compromise is extremely high. Within our approach, we propose to conceptually split the role of the single *AA*: an *offline CP-ABE AA* issues all static attributes in a registration phase, while an *embedded LBE AA* handles dynamic location attributes, based on tamper-resistant hardware. Since policies always include conjunctions of location and further CP-ABE attributes, this approach retains encryption of messages even in case the *embedded LBE AA* would be compromised. Also, this technique minimizes the use of pairings in the end-to-end encryption, which broadens the applicability to a broad range of mobile devices. In turn, the hybrid encryption technique looses full cryptographic collusion resistance w.r.t. the expressive policy. Yet, collusion between receivers or attackers that try trading CP-ABE attributes, e.g. in order to gain access to messages of further organizations, fails. The hybrid encryption assumes tamper-resistant hardware, especially tamper-resistant GPS receivers. In the emergency domain, this assumption is practically fulfilled by all given TETRA mobile communication devices. The application logic required to implement the location lock mapping and the location verification procedure is small, such that means to guarantee correctness based on certification procedures can easily be applied. Together with the secure software stack due to the TPM chip of the device [6], additional practical security guarantees can be given.

Practical Extendability to Distributed Authorities: The hybrid encryption scheme inherits its main features from LBE and CP-ABE. Also, it inherits the single *AA* for handling static attributes. As a consequence for the ABM scheme, all receivers have to register with the same central *AA*. In a practical context, organizations involved in disaster management would have to agree on a single authority to issue all keys for arbitrary users. In fact, this does not scale well and may also lead to problems in case involved organizations do mutually distrust each other. With concepts proposed in [13, 14], it is actually possible to implement multi-authority CP-AB encryption, such that independent authorities can issue attribute keys. A large scale real world deployment of the proposed ABM scheme could be based on our hybrid encryption technique incorporating these extended CP-ABE mechanisms.

7.2 Security Requirements

- `SReq1:` The basic security mechanisms of mutual authentication, message integrity and availability are implemented by the TETRA security architecture. Since the ABM scheme is realized on the TETRA end-to-end encryption layer, they apply to it, too. Especially, device revocation is possible by means of TETRA, without relying on cryptographic application level mechanisms.
- `SReq2:` End-to-end encryption in the messaging is given due to and implemented by the use of the proposed hybrid encryption scheme on the end-to-end encryption layer. Computation security reduces to the same computa-

tional assumptions as in CP-ABE. Collusion resistance is given as discussed in section 7.1.

- `SReq3:` Replay attacks are handled on the end-to-end encryption layer: after decryption, the receiver verifies the freshness of the included message ID, ID_m. The receiver rejects messages that contain an ID_m that he already decrypted.
- `SReq4:` Accountability of senders is assured due to two mechanisms: first, each message sent is added to ML, for additional security digitally signed by S. This record can later be audited. Second, messages include a MAC, such that it can be linked to the sender, given that registration is trustworthy.
- `SReq5:` Readers, i.e. the subset of all receivers of a message that satisfied the logical messaging policy, are documented via RL. Unique mobile subscriber identities, $IMSI_R$, can be resolved to real world identities of readers, via linking to information present on $RegL$.
- `SReq6:` Efficiency of the scheme has computational and organizational factors. Regarding computational efficiency, our approach has a low pairing complexity[12] due to the hybrid policy encryption, which renders decryption practically on resource-constraint devices. From the organizational perspective, no online AA is required, such that the interactions in end-to-end key management are reduced to a registration phase.
- `SReq7:` User-friendliness for senders is given in the sense that ABM allows a single, combined realization of all necessary communication patterns `CP1-CP4`, thus minimizing learning efforts. Further, our approach integrates continuous location attributes into the selection of receivers, which are intuitive selectors for senders. From the receivers' perspective, the approach allows for a seamless integratability into personal lifes. Specialist can be contacted and requested without requiring them to continuously provide current location information.

8 Conclusion

This paper dealt with security issues inherent to one-to-many communication with mobile receivers. We used the context of emergency communication as a descriptive real world application scenario. First, we contributed to this context by elicitating requirements of emergency practioners. Second, we proposed a hybrid encryption technique for expressive policies that enables devising end-to-end secure yet user-friendly communication mechanisms. Third, we introduced and analyzed an approach to multilaterally secure, user-friendly attribute-based messaging.

[12] Session key decryption requires one XOR operation for the LBE part. To decrypt the CP-ABE part of the policy, two pairing operations for every attribute that is matched by one of R's attributes are required. For policies with additional internal AND-/OR-levels, one exponentiation operation is required for each internal node from an attribute in the leaf to the root node of the CP-ABE policy part.

We believe that ABM concepts have the potential to become an important communication paradigm in mobile and pervasive computing scenarios, due to inherent user-friendliness, practicality and flexibility. Further efficiency evaluations and user trials of our work will follow.

Acknowledgment

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

References

1. Bethencourt, J., Sahai, A., Waters, B.: Ciphertext-Policy Attribute-Based Encryption. In: IEEE Symposium on Security and Privacy (SP '07). pp. 321–334. IEEE CS (2007)
2. Blackmon, M.H.: Cognitive Walkthrough. In: Bainbridge, W.S. (ed.) Encyclopedia of Human-Computer Interaction - Volume 1, pp. 104–107. Berkshire Publishing Group (2004)
3. Bobba, R., Fatemieh, O., Khan, F., Gunter, C.A., Khurana, H.: Using Attribute-Based Access Control to Enable Attribute-Based Messaging. In: Annual Computer Security Applications Conference (ACSAC '06). pp. 403–413. IEEE CS (2006)
4. Bobba, R., Fatemieh, O., Khan, F., Khan, A., Gunter, C.A., Khurana, H., Manoj, P.: Attribute-Based Messaging: Access Control and Confidentiality. ACM Trans. Inf. Syst. Secur. (TISSEC) 14, to appear (2010)
5. Boneh, D., Franklin, M.K.: Identity-Based Encryption from the Weil Pairing. SIAM J. Comput. 32(3), 586–615 (2003)
6. Brucker, A.D., Petritsch, H., Weber, S.G.: Attribute-Based Encryption with Break-Glass. In: Workshop in Information Security Theory and Practice (WISTP'10). pp. 237–244. Springer (2010)
7. Chadwick, D., Lunt, G., Zhao, G.: Secure Role Based Messaging. In: IFIP Conference on Communications and Multimedia Security (CMS '04). pp. 303–316 (2004)
8. Committee on Planning for Catastrophe (ed.): Successful Response Starts With A Map: Improving Geospatial Support for Disaster Management. National Academy Press (2007)
9. Denning, D.E., Scott, L.: Geo-Encryption - Using GPS to Enhance Data Security. GPS World (2003)
10. Gentry, C.: IBE (Identity-Based Encryption). In: Bidgoli, H. (ed.) Handbook of Information Security - Volume 2, pp. 575–592. John Wiley and Sons (2006)
11. Goyal, V., Pandey, O., Sahai, A., Waters, B.: Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data. In: ACM Conference on Computer and Communications Security (CCS '06). pp. 89–98. ACM (2006)
12. Mont, M.C., Bramhall, P., Harrison, K.: A Flexible Role-Based Secure Messaging Service: Exploiting IBE technology for Privacy in Health Care. In: Workshop on Database and Expert Systems Applications (DEXA '03). pp. 432–437. IEEE CS (2003)
13. Müller, S., Katzenbeisser, S., Eckert, C.: Distributed Attribute-Based Encryption. In: Internation Conference on Information Security and Cryptology (ICISC'08). pp. 20–36. Springer (2008)

14. Müller, S., Katzenbeisser, S., Eckert, C.: On Multi-Authority Ciphertext-Policy Attribute-Based Encryption. Bulletin of the Korean Mathematical Society 46(4), 803–819 (2009)
15. Murgatroyd, B.W.: End to End Encryption in Public Safety TETRA Networks. IE Seminar on Secure GSM and Beyond: End to End Security for mobile Communication (Digest No. 2003/10059) (2003)
16. Rannenberg, K.: Multilateral Security - a Concept and Examples for Balanced Security. In: Workshop on New Security Paradigms (NSPW '00). pp. 151–162. ACM (2000)
17. Sahai, A., Waters, B.: Fuzzy Identity-Based Encryption. In: Advances in Cryptology: EUROCRYPT '05. pp. 457–473. Springer (2005)
18. Sandhu, R.S., Coyne, E.J., Feinstein, H.L., Youman, C.E.: Role-Based Access Control Models. IEEE Computer 29(2), 38–47 (1996)
19. Scott, L., Denning, D.E.: A Location Based Encryption Technique and Some of Its Applications. In: ION National Technical Meeting 2003. pp. 730–740 (2003)
20. Shamir, A.: How to Share a Secret. Communications of the ACM 22(11), 612–613 (1979)
21. Tognazzini, B.: Design for Usability. In: Cranor, L., Garfinkel, S. (eds.) Security and Usability: Designing Secure Systems That People Can Use, pp. 31–96. O'Reilly Media (2005)
22. Weber, S.G.: Secure and Efficient First Response Coordination based on Attribute-based Encryption Techniques. ISCRAM2009 Student Poster Session (2009)
23. Weber, S.G.: Securing First Response Coordination with Dynamic Attribute-Based Encryption. In: Conference on Privacy, Security and Trust (PST '09) in conjunction with World Congress on Privacy, Security, Trust and the Management of e-Business (CONGRESS '09). pp. 58 – 69. IEEE CS (2009)
24. Yuan, E., Tong, J.: Attribute Based Access Control (ABAC) for Web Services. In: Conference on Web Services (ICWS'05). pp. 561 – 569. IEEE CS (2005)