Secure and Efficient First Response Coordination based on Attribute-based Encryption Techniques

Stefan G. Weber
Telecooperation Group, TU Darmstadt
Darmstadt, Germany
sweber@tk.informatik.tu-darmstadt.de

EXTENDED ABSTRACT

In a large-scale emergency situation, incident reactions need to be quick. Every minute saved in emergency management processes and first response coordination workflows (cp. Fig. 1) can save additional lives of affected victims. Dealing with this issue, future response support systems alike the SoKNOS platform (www.soknos.de) promise to improve the collection and processing of large amounts of relevant information. Supported by such a system, a decision maker in an emergency management headquarter may harness the resulting integrated view on the disaster situation, visualized on a large digital map [1], in order to effectively coordinate the incident reactions of mobile first responders. This requires efficient means to communicate between the emergency staff in the headquarter and mobile first responders out in the field. However, an exchange of tactical information between the rescue parties has to meet a strong security requirement: it must preserve end-to-end confidentiality in order to prevent malicious third parties from disrupting the reactions.
At this point, a failure on the *data security* level may become a threat *to public security*. Actually, the lives of first responders partly depend on correct tactical information. Injured persons, that shall be immediately rescued, and physical assets the first responders are chosen to protect, may be affected by data security vulnerabilities in the tactical messaging, as well.
Our work [2,3] focuses on the issue of providing a secure and efficient mean to support the secure coordination of mobile first responders. Therefore, we describe concepts to implement a secure ubiquitous tactical communication based on the concept of *attribute-based messaging*. In our approach, decision makers may target dynamic groups of intended receivers, i.e. relevant first responders out in the field, directly on a digital map by selecting spatial regions and attributes (cp. Fig. 2). Beyond location, the decision maker may include further attributes alike current status, role, organization or group leader skills, to specify the group of receivers in an intuitive way. The actual tactical instructions for the mobile forces are textually specified in form of a message.
The attribute-based selection of the receivers translates to underlying cryptographic operations in the end-to-end encryption. Especially, our concept harnesses *ciphertext-policy attribute-based encryption* (CP-ABE) techniques [4]. We extend current CP-ABE proposals [4,5] by additionally taking into account dynamic factors: our proposed system is able to efficiently handle dynamic attributes, like location or the health status to address mobile first responders, in a secure fashion, while end-to-end encryption for the transmission of tactical information is still satisfied.

Emergency staff members with decision making responsibilities may use our approach to target groups of receivers in a secure and intuitive way, in order to efficiently coordinate their reactions, in the face of rapidly changing situations of large scale disasters.

A prototype implementation on standard hardware plattforms (Windows Mobile and Android) is currently under development. We integrate our first response coordination concepts into the next generation of our first response testbed [6], which will allow us to simulate and evaluate emergency scenarios and respective tactical messaging on a large scale.

This extended abstract and the corresponding poster (see: http://www.slideshare.net/sweberTK/secure-and-efficient-first-response-coordination-based-on-attributebased-encryption-techniques-1521383) briefly introduces our research on securing first response coordination to the ISCRAM community. For more details we refer to [2].

Keywords

First Response Coordination, Secure Communication, Attribute-Based Messaging, Attribute-Based Encryption

Figure 1. First Response Coordination Workflow

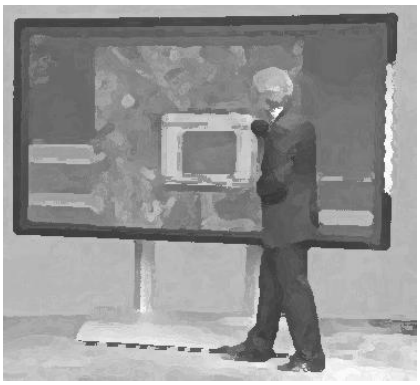

Figure 2. Vision of First Response Coordination

ACKNOWLEDGMENTS

This work was supported by the German Federal Ministry of Education and Research in the context of the project SoKNOS (www.soknos.de) and by CASED (www.cased.de). The author is responsible for the content of this publication.

REFERENCES

1. Committee on Planning for Catastrophe, Ed., Successful Response Starts With A Map: Improving Geospatial Support for Disaster Management. National Academy Press, 2007
2. Stefan G. Weber: Securing First Response Coordination With Dynamic Attribute-Based Encryption, *Proceedings of the Seventh Annual Conference on Privacy, Security and Trust (PST 2009) in conjunction with 2009 World Congress on Privacy, Security, Trust and the Management of e-Business (CONGRESS 2009)*, p. 58 - 69, IEEE Computer Society, August 2009. ISBN 978-0-7695-3805-1.
3. Felix Flentge, Stefan G. Weber, Alexander Behring, Thomas Ziegert: Designing Context-Aware HCI for Collaborative Emergency Management, *Proceedings of the International Workshop on HCI for Emergencies, in conjunction with CHI 2008*, Florence, Italy, 2008.
4. John Bethencourt, Amit Sahai, Brent Waters: Ciphertext-Policy Attribute-Based Encryption, *Proceedings of the 2007 IEEE Symposium on Security and Privacy*, Washington, DC, USA, 2007
5. Matthew Piretti, Patrick Traynor, Patrick McDaniel, Brent Waters: Secure Attribute-Based Systems, *Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS'06)*, 2006
6. Dirk Bradler, Immanuel Schweizer, Kamill Panitzek, Max Mühlhäuser, M.: First Response Communication Sandbox, Proceedings of the 11th Communication and Networking Simulation Symposium, pp. 115-122, 2008.