Journal of Ambient Intelligence and Smart Environments 4 (2012) 135–136
DOI 10.3233/AIS-2012-0140
IOS Press

Thesis

Multilaterally secure pervasive cooperation

Stefan G. Weber
Center for Advanced Security Research Darmstadt (CASED), Mornewegstr. 32, 64293 Darmstadt, Germany
E-mail: StefanGeorgWeber@Gmail.com

Abstract. The present paper summarizes the PhD thesis of Stefan G. Weber.

Keywords: Multilateral security, privacy, accountability, pervasive computing, emergency response

1. PhD thesis abstract

People tend to interact and communicate with others throughout their life. In the age of pervasive computing, information and communication technology (ICT) that is no longer bound to desktop computers enables digital cooperations in everyday life and work in an unprecedented manner.

However, the privacy and IT security issues inherent in pervasive computing are often associated with negative consequences for the users and the (information) society as a whole.

Addressing this challenge, this thesis demonstrates that carefully devised protection mechanisms can become enablers for multilaterally acceptable and trustworthy digital interactions and cooperations [1,2]. It contributes to the design of multilaterally secure cooperative pervasive systems by taking a scenario-oriented approach.

Within our reference scenario of ICT-supported emergency response [3], we derive the following scientific research questions. Firstly, we investigate how to enable real-world auditing in pervasive location tracking systems, while striking a balance between privacy protection and accountability. Secondly, we aim to support communication between a sender and mobile receivers that are unknown by identity, while end-to-end security is enforced. The required concepts and mechanisms define the scope of what we denote as *multilaterally secure pervasive cooperation*.

We take a novel *integrated approach* and provide the supporting security techniques and mechanisms. The main contributions of this thesis are

(i) *pseudonyms with implicit attributes* [4], which is an approach to multilevel linkable transaction pseudonyms that is based on a combination of threshold encryption techniques, secure multiparty computation and cryptographically secure pseudo-random number generators,
(ii) *multilaterally secure location-based auditing* [7], a novel consideration of auditing mechanisms in the context of real-world actions that reconciles privacy protection and accountability while proposing location traces as evidence,
(iii) a *hybrid encryption technique for expressive policies* [8,9], which allows encrypting under policies that include a continuous dynamic attribute, leveraging an efficient combination of ciphertext-policy attribute-based encryption, location-based encryption and symmetric encryption concepts, and
(iv) *end-to-end secure attribute-based messaging* [5,6,9], a communication mechanism for end-to-end confidential messaging with receivers unknown by identity that is suitable also for resource-constrained mobile devices.

Harnessing these buildings blocks, we present an integrated architecture that supports *location-aware first response*. We therein consider location as the central integrating concept for pervasive cooperations. Both communication during incident handling as well as ex-post auditing are conceived as being location-based.

Our research draws from experiences with potential real users (first responders and emergency decision makers) and from an interdisciplinary study. We contribute results derived from simulated court cases, indicating the trustworthiness and practicality of our proposal.

Experiments conducted with prototype systems support the claim that our concepts are suitable for resource-constrained devices.

In a theoretical analysis, we show that our security requirements are fulfilled. Our proposals have multiple further applications, e.g. to pseudonym-based access control.

2. PhD defense

On December 1st, 2011, the author successfully defended his PhD thesis at the Center for Advanced Security Research Darmstadt (CASED) / TU Darmstadt.

The defense committee members included

- Prof. Max Mühlhäuser (principal advisor),
- Prof. Simone Fischer-Hübner (second advisor),
- Prof. Marc Fischlin (chair),
- Prof. Chris Biemann, and
- Prof. Christian Bischof.

Acknowledgements

The author would like to thank all people and institutions that provided support in the creation of this thesis.

References

[1] S.G. Weber, S. Ries, and A. Heinemann, Inherent tradeoffs in ubiquitous computing services, in: *INFORMATIK 2007*, GI, 2007, pp. 364–368.

[2] S.G. Weber, A. Heinemann, and M. Mühlhäuser, 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)*, IEEE CS, 2008, pp. 958–964.

[3] F. Flentge, S.G. Weber, A. Behring, and T. Ziegert, Designing context-aware HCI for collaborative emergency management, in: *Workshop on HCI for Emergencies in Conjunction with CHI 2008*, 2008.

[4] S.G. Weber, Harnessing pseudonyms with implicit attributes for privacy-respecting mission log analysis, in: *Conference on Intelligent Networking and Collaborative Systems (INCoS 2009)*, IEEE CS, 2009, pp. 119–126.

[5] S.G. Weber, Securing first response coordination with dynamic attribute-based encryption, in: *Conference on Privacy, Security and Trust (PST 2009) in Conjunction with World Congress on Privacy, Security, Trust and the Management of e-Business (CONGRESS 2009)*, IEEE CS, 2009, pp. 58–69.

[6] A.D. Brucker, H. Petritsch, and S.G. Weber, Attribute-based encryption with break-glass, in: *Workshop on Information Security Theory and Practice (WISTP 2010)*, Springer, 2010.

[7] S.G. Weber and M. Mühlhäuser, Multilaterally secure ubiquitous auditing, in: *Intelligent Networking and Collaborative Systems and Applications*, SCI 329, Springer, 2010, pp. 207–233.

[8] S.G. Weber, L.A. Martucci, S. Ries, and M. Mühlhäuser, Towards trustworthy identity and access management for the future internet, in: *Workshop on Trustworthy Internet of People, Things & Services (Trustworthy IoPTS 2010) in Conjunction with Internet of Things Conference (IoT 2010)*, 2010.

[9] S.G. Weber, Y. Kalev, S. Ries, and M. Mühlhäuser, MundoMessage: Enabling trustworthy ubiquitous emergency communication, in: *International Conference on Ubiquitous Information Management and Communication (ICUIMC 2011)*, ACM Press, 2011, pp. 29:1–29:10.