Algorytmy ochrony informacji dla systemów urządzeń o ograniczonych możliwościach

Piotr Syga

Abstract

Recent years have seen more and more effort put into development and popularization of distributed systems consisting of severely constrained devices. Due to limited computational capabilities of nodes in such distributed systems, the use of traditional cryptographic methods is infeasible. In the following dissertation we focus on two specific systems of constrained devices: RFID systems and wireless sensor networks. Both of the aforementioned systems have wide range of applications, which present them to specific threats. Furthermore both of the mentioned distributed systems are not under constant physical supervision, making it more vulnerable to attacks. In the dissertation we focus on preserving privacy of the data we consider sensitive. By privacy one may understand confidentiality, anonymity or tracking resilience, the specific context is adjusted to the considered model of the system.

In sensor networks' model we consider a passive adversary, who eavesdrops communication inside the network in order to learn the execution of the protocol. We assume a communication model very common in research of ad hoc networks, namely Multiple Access Channel (MAC), in which all nodes are able to communicate directly via broadcasting. However the model allows that only one node can transmit in a single round, otherwise the message is lost. Despite vast research on security of wireless sensor networks, to the best of our knowledge the analysis of the passive adversary model has been neglected. In the dissertation however we point out how such an adversary may endanger the system. In order to face this threats we present MAO, an obfuscating meta–algorithm that provides *provable security* of execution of any distributed algorithm. Furthermore we provide an extension of MAO, that allows to adjust security guarantees and time complexity. Both variants of MAO have been formally analyzed. As MAO is a general framework that could be applied to any algorithm (randomized as well as deterministic or adaptive) and provides the same guarantees, it is not perfect in terms of time complexity. Since some basic protocols are used more often than others, we designed two specialized obfuscated algorithms, that require less additional communication rounds to provide obfuscation of their execution. Specifically, we have addressed *size approximation* protocol obtaining OSA algorithm and *initialization* protocol (however within it we contained a method to obfuscate *leader election*) resulting in MOC algorithm. Both algorithms have been formally analyzed and their security proven in terms of $(\alpha,\ \beta)$–*obfuscation*, which was inspired by the idea of *differential*

privacy presented in [5]. Moreover we have shown that OSA algorithm is suitable for the MAC model *without collision detection* and MOC algorithm provides security even against *strong adversary* (used in [4] among others). We have also proved the advantage of the specialized obfuscating algorithms over MAO in terms of time complexity for the same security guarantees. The last of the protocols presented in the part devoted to wireless sensor network, due to severely constrained device and communication model we assumed, is a smooth transition towards the second of the discussed systems – RFID. We provide a communication protocol suitable for severely constrained devices that allows encryption at message creation level. As we do not assume any signal modulation, in fact we base our protocol on carrier wave sensing, we consider *beeping model* [1] in our discussion. Moreover, we limit the assumed model to the point that the regular nodes may only send their messages (do not perform carrier sensing) and only distinguished, stronger device – sink (denoted $\mathcal{S}$) receives the messages via carrier sensing, yet it does not transmit. One can see that such one-way communication channel may be very useful in various scenarios involving user control (like proof of presence), since constantly silent $\mathcal{S}$ is hard to locate by the adversary. We uphold the basic assumptions of the beeping model, hence there are only two possible states on the communication channel, namely a `silence` (when no node sends it signal) and a `beep` (when at least one of the node transmits). We prove that the presented protocol provides information–theoretic security and prevents a passive adversary from linking different messages as being sent by the same node.

In the second kind of the considered systems, *Radio Frequency IDentifiers* system, we focus on protecting the privacy of the user (owner) of RFID tags. Due to popularity and small size of the tags, the user may be unaware of the presence of the tag, let alone the threats related to them. In the dissertation we focus on preventing unauthorized communication with the tag as well as tracking prevention. The first goal is achieved by three ideas that base on additional device introduced into the system. The main idea, the device called *Hedgehog blocker* can be treated as an extension of *Blocker tag* presented by Juels, Rivest and Szydlo. We present the formal model and prove security of Hedgehog blocker. The second concern – tracking prevention is addressed by an ultralight authentication protocol Chameleon. We have introduced a protocol that allows authentication of a tag (database keeps track of current RFID identifier, but what is important the size of the database does not increase), however it protects tags from being tracked by an adversary. We assume that the adversary is global however it is not omnipresent, hence he has to miss some communication rounds. We proved that the number of missed rounds of communication does not have to be large, in order to mislead the adversary.

The results described above constitute the main part of the dissertation described in Chapters 5 to 10, additionally the dissertation includes auxiliary chapters that contain introduction to the considered field and models, establish the notation and recall some mathematical facts and techniques used in this work.

Following dissertation is based on three published articles and two articles awaiting publication. Below we present the list of those articles:

- M. Klonowski, M. Kutyłowski, P. Syga: *Chameleon RFID and Tracking Preven-*

tion [8].

- M. Kardas, M. Klonowski, P. Syga, Sz. Wilczek: *Obfuscated Counting in Single-Hop Radio Network* [7].
- P. Błaskiewicz, M. Klonowski, K. Majcher, P. Syga: *Blocker-Type Methods for Protecting Customers' Privacy in RFID Systems* [3].
- M. Kardas, M. Klonowski, P. Syga: *How to Obfuscate Execution of Protocols in a Single Hop Radio Network?* [6].
- P. Błaśkiewicz, M. Klonowski, M. Kutyłowski, P. Syga: *Lightweight Protocol for Trusted Spontaneous Communication*[2].

Literatura

[1] Yehuda Afek, Noga Alon, Ziv Bar-Joseph, Alejandro Cornejo, Bernhard Haeupler, and Fabian Kuhn. Beeping a maximal independent set. *Distributed Computing*, 26(4):195–208, 2013.

[2] Przemysław Błaśkiewicz, Marek Klonowski, Mirosław Kutyłowski, and Piotr Syga. Lightweight protocol for trusted spontaneous communication. In *paper accepted to INTRUST*, 2014.

[3] Przemyslaw Blaskiewicz, Marek Klonowski, Krzysztof Majcher, and Piotr Syga. Blocker-type methods for protecting customers' privacy in rfid systems. In *CyberC*, pages 89–96. IEEE, 2013.

[4] Gianluca De Marco and Dariusz R. Kowalski. Towards power-sensitive communication on a multiple-access channel. In *ICDCS*, pages 728–735. IEEE Computer Society, 2010.

[5] Cynthia Dwork. Differential privacy: A survey of results. In *Proceedings of the 5th international conference on Theory and applications of models of computation*, TAMC '08, pages 1–19, 2008.

[6] Marcin Kardas, Marek Klonowski, and Piotr Syga. How to obfuscate execution of protocols in a single hop radio network? *Theor. Comput. Sci.*, to be published.

[7] Marcin Kardas, Marek Klonowski, Piotr Syga, and Szymon Wilczek. Obfuscated counting in single-hop radio network. In *ICPADS*, pages 692–693. IEEE Computer Society, 2012.

[8] Marek Klonowski, Miroslaw Kutylowski, and Piotr Syga. Chameleon rfid and tracking prevention. In *Radio Frequency Identification System Security*, pages 17–29, 2013.