Lecture Notes in Computer Science 8262

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

For further volumes:
http://www.springer.com/series/7410

Michael Hutter · Jörn-Marc Schmidt (Eds.)

Radio Frequency Identification

Security and Privacy Issues

9th International Workshop, RFIDsec 2013
Graz, Austria, July 9–11, 2013
Revised Selected Papers

Springer

Editors
Michael Hutter
Jörn-Marc Schmidt
Graz University of Technology
Austria

ISSN 0302-9743 ISSN 1611-3349 (electronic)
ISBN 978-3-642-41331-5 ISBN 978-3-642-41332-2 (eBook)
DOI 10.1007/978-3-642-41332-2
Springer Heidelberg New York Dordrecht London

Library of Congress Control Number: 2013953279

CR Subject Classification K.6.5, E.3, K.4.4, C.2, C.3

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

RFIDsec 2013, the 9th workshop on RFID Security and Privacy, was held in Graz, Austria, during July 9–11, 2013. More than 50 participants from 13 countries attended the workshop. The Program Committee consisting of 24 experts in the field selected 11 papers out of 23 submissions for publication in the workshop proceedings. Each paper was reviewed by at least three and on average four reviewers.

The program included three invited talks given by international experts in the field. The first invited talk entitled "RFID Privacy: From Transportation Payments to Implantable Medical Devices" was given by Wayne Burleson, who introduced the audience to state of the art RFID privacy issues. The second talk was given by Günther Lackner and Karin Greimel, who talked about "20 Years of MIFARE. From CRYPTO1 to Formal Verification." They gave an overview of various industry perspectives in the case of the Mifare product family that celebrates its 20 years anniversary. The third talk was given by Lejla Batina entitled "How Light Is Lightweight Crypto". Her talk focused on RFID identification protocols and hardware-implementation requirements for RFID.

Since 2011, RFIDsec has additionally provided area-relevant tutorials for attendees from academia and industry. In this year's edition, we offered three tutorials that preceded the workshop. The specific topics were "RFID Introduction and the IAIK DemoTag: A Programmable RFID-Tag Emulator" given by Thomas Korak, Raphael Spreitzer, and Hannes Gross, "Side-Channel Attacks and Fault Analysis" given by Johann Heyszl and Thomas Korak, and "Cryptographic Hardware Design and Performance Metrics" given by Frank K. Gürkaynak.

This year's edition of RFIDsec was the first in cooperation with the International Association for Cryptologic Research. We would like to thank Bart Preneel for promoting and supporting us to get the IACR "In Cooperation" status. Furthermore, we would like to thank the sponsorships from the Styrian Business Promotion Agency (SFG), the City of Graz, the State of Styria, and NXP Semiconductors. With their support it was possible to provide student stipends for attending the workshop.

Finally, we would like to thank all authors for their paper submission, the Program Committee and all external reviewers for their support in the review process allowing us to accept a number of high-quality papers, and all the attendees of the workshop for their active participation and contribution to this research area.

August 2013

Michael Hutter
Jörn-Marc Schmidt

RFID: Contactless Identification and Security Technology

Radio-frequency identification (RFID)[1] is a technical system that offers the possibility of reading data through radio waves without the need for contact. This allows the automatic identification and location of objects and makes the collection of data easier.

The most exciting thing about RFID is its diverse application range, which allows both security and comfort for the end user. From passports to logistic processes and patient follow-up, from time recording to bus tickets and engine immobilizers, the application possibilities seem endless and the market potential is huge. And Styria is involved in a big way!

RFID-Hotspot Styria[2]: Styria, the second largest province of Austria, has about 1.2 million inhabitants and is situated central to the emerging markets of south-eastern Europe with about 20 million people. Graz, the capital city of Styria, is an old university town and has a population in the greater area of about 400,000 long-term inhabitants. With seven universities, a broad range of R&D and competence centers, and its own research institution called Joanneum Research, Styria is Austria's top engineering, science, and research province.

The development of the RFID technology has a long tradition in Styria. Styrian RFID companies — and in Styria there are a collection of world-leading companies (NXP, Infineon, ams etc.) — are highly renowned in this field: More than 50% of RFID chips in use worldwide have been developed in Styria. Practically all of these companies are operational at an international and worldwide level and at present employ ca. 2,000 people (primarily in Graz and its surrounding area). The export ratio in the RFID sector in Styria stands at over 90%. Global brands such as Mifare, Hitag, Legic were developed by Styrian companies and have gone on to become world-leading brands. Further data and facts on Styria as an RFID hotspot are as follows:

- Styria offers expertise along the entire value chain (incl. research and education): Chip, Antennas, Reader, Software, System provider.
- More than 50% of RFID chips currently in global use have been developed in Styria.
- Styria is the birthplace of Near Field Communication (NFC).

---

[1] RFID is part of the core competency "Electronics, Instrumentation and Control Technology" of the Economic Strategy Styria 2020 (http://sfg.at/cms/3724/).

[2] The RFID-Hotspot Styria was initiated by the Styrian Business Promotion Agency (SFG). SFG is a service provider, which aims to contribute to the consolidation and growth of the Styrian economy. As a 100% subsidiary of the Styrian Government, SFG operates all business support tasks for its owner. This is the provision of monetary support with a broad range of grant and financing programs, as well as tasks like raising and steering clusters and networks, technology parks, technology transfer, and the consulting of foreign investors. For more information about the RFID-Hotspot Styria, please visit our website (http://sfg.at/rfid) or contact us via e-mail (rfid@sfg.at).

- With a market share of over 95% in the field of RFID and security, chips originating from Styria for application in, e.g., government documents (passports, driver's licences etc.) are in use in over 100 countries.
- The no. 1 innovation used in readers for passport chips comes from Styria.
- In the RFID automotive sector (engine immobilizers, radio controlled keys, tyre pressure sensors etc.), chip innovations from Styria are also no. 1 with a market share of 50%.
- Styria is no. 1 in the area of chip innovation with well-known applications such as access control, electric ticketing, and electronic payments.

What would future technology be without its corresponding research activities? In Styria there are an array of universities and other research and development institutes that are active in the area of RFID. Universities, polytechnics, and non-university research institutes do not just provide us with research results but also with the raw material for future business location development: qualified employees. With its renowned RFID companies and accompanying research and educational activities, Styria is a Mecca for RFID where future RFID developments are forged.

The following research and educational initiatives are examples of the cooperation between economy, science, and education in Styria in the field of RFID:

SeCoS — Secure Contactless Sphere: Representatives from the entire RFID supply chain have come together to form a consortium to work on the K-Project SeCoS (lead partner: Joanneum Research). The aims of the project are to develop a platform that places the highest demands on security and protection of privacy all the way from the chip to the application itself as well as to reduce component size, to enhance carrier frequencies and data transfer rates, and to improve the precision of object tracking. Several application scenarios will be implemented to demonstrate the research results. The focus on security and privacy technology originates from the fact that new applications that involve RFID regularly raise concerns regarding these topics. This is because RFID tags can be read out over a distance without any interaction of the user; the user is not even aware that the tag is/was read out. Within the project, we want to provide a comprehensive methodology for making use of the advance of RFID tags yet ensuring privacy of all parties involved in the product life-cycle.

This K-Project SeCoS is funded in the context of COMET - Competence Centers for Excellent Technologies by BMVIT, BMWFJ, SFG, Province of Styria, Government of Styria. The program COMET is conducted by the Austrian Research Promotion Agency (FFG).

RFID Qualification Network Austria: Based on a study conducted by the SFG, TU Graz and various partners from science and business make up the RFID Qualification Network Austria, which is supported by the Austrian Research Promotion Agency (FFG). The Network has succeeded in establishing a consortium of 24 businesses and educational institutions, covering the entire value-added chain of the RFID area. February 2013 saw the start of a comprehensive continuing education program comprising 48 individual courses offered by TU Graz and FH Campus 02. In terms of content, focuses include state-of-the-art technological developments, the building of

competences in innovation and demand, the integration of RFID into businesses, and know-how on key factors of RFID systems.

Both science and businesses benefit from this cooperation in many ways. The intensive dialogue between participants and instructors influences new innovation and research projects, for example, in the areas of software architecture, Web services, IT security and tool-supported software development. In addition to Graz University of Technology as the applicant and many small and medium-sized businesses, FH Campus 02, Joanneum Research, AVL List, ams, NXP, Infineon, Voest Alpine, and the Evolaris Competence Centre are on board as well.

The goal for the near future is to establish Graz as a leading international educational region for RFID by providing post-graduate university courses, study programs, and courses that go beyond the training currently on offer.

Organization

RFIDsec 2013 was organized by the Institute for Applied Information Processing and Communications (IAIK), Graz University of Technology, Austria.

Executive Committee

Program Co-chairs

Michael Hutter	TU Graz, Austria
Jörn-Marc Schmidt	TU Graz, Austria

General Chair

Jörn-Marc Schmidt	TU Graz, Austria

Program Committee

Gildas Avoine	Université Catholique de Louvain (Belgium)
Lejla Batina	Radboud University Nijmegen (The Netherlands)
Mike Burmester	Florida State University (USA)
Srdjan Capkun	ETH Zurich (Switzerland)
Paolo D'Arco	University of Salerno (Italy)
Thomas Eisenbarth	Worcester Polytechnic Institute (USA)
Martin Feldhofer	NXP Semiconductors (Austria)
Julio Hernandez-Castro	University of Kent (UK)
Jaap-Henk Hoepman	TNO / Radboud University Nijmegen (The Netherlands)
Timo Kasper	Ruhr University Bochum (Germany)
Kerstin Lemke-Rust	Hochschule Bonn-Rhein-Sieg (Germany)
Yingjiu Li	Singapore Management University (Singapore)
Nai-Wei Lo	National Taiwan University of Science and Technology (Taiwan)
Konstantinos Markantonakis	Royal Holloway University of London (UK)
Aikaterini Mitrokotsa	École Polytechnique Fédérale de Lausanne (Switzerland)
Karsten Nohl	Security Research Labs (Germany)
Berna Örs	Istanbul Technical University (Turkey)
Pedro Peris-Lopez	Carlos III University of Madrid (Spain)

Axel Poschmann	Nanyang Technological University (Singapore)
Pankaj Rohatgi	Cryptography Research Inc. (USA)
Kazuo Sakiyama	University of Electro-Communications (Japan)
Nitesh Saxena	University of Alabama at Birmingham (USA)
Marc Witteman	Riscure (The Netherlands)
Avishai Wool	Tel Aviv University (Israel)

External Reviewers

Xavier Carpent	Anna Krasnova	Manar Mohamed
Baris Ege	Yang Li	Phuong Ha Nguyen
Jian Guo	Luka Malisa	David Oswald
Yoshikazu Hanatani	Tania Martin	Babins Shrestha
Gesine Hinterwalder	Ramya Masti	Xin Ye
Divyan Konidala	Shugo Mikami	

Sponsoring Institutions

Styrian Business Promotion Agency (SFG)
City of Graz
State of Styria
NXP Semiconductors

Contents