Security of Ubiquitous Computing Systems

Gildas Avoine • Julio Hernandez-Castro
Editors

Security of Ubiquitous Computing Systems

Selected Topics

Springer

Editors

Gildas Avoine
Institut National des Sciences Appliquées
Rennes, France

Julio Hernandez-Castro
University of Kent
Canterbury, UK

ISBN 978-3-030-10590-7 ISBN 978-3-030-10591-4 (eBook)
https://doi.org/10.1007/978-3-030-10591-4

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.
The publisher, the authors, and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG.
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

From the Cryptacus Project to the Cryptacus Book

Dear reader, we thank you for your interest in this book, which we expect will help you gain an understanding of the state of the art in 2020 regarding the challenges and solutions in the security of ubiquitous computing systems.

The definition of the field itself is not without controversy, but in this book we will use the term ‘ubiquitous computing’ or ‘IoT’ to refer to generally small, embedded devices with serious constraints in terms of memory and processing power, typically with no batteries but with good connection capabilities and, frequently, a number of sensors. This definition is, of course, flexible. Electronic passports, contactless transportation cards, personal assistants such as Amazon Echo but also new connected cars and fridges can fall within this definition.

This book is targeted to advanced undergraduate students and master’s and early Ph.D. students who want quick, direct, authoritative, insightful exposure to the topics covered, all generally falling under the umbrella of IoT security. Engineers and other practitioners can also benefit from the book by getting a quick introduction to a variety of practical security topics, their past and present solutions, and some new and promising ideas that may play important roles in its future.

This book would not have been possible without the support of the CRYPTACUS (Cryptanalysis in Ubiquitous Computing Systems) COST Action IC 1403, which started in 2014 and ended in December 2018. We are particularly thankful to the EU COST association, which was extremely positive for the community in Europe and associated countries such as Switzerland, Turkey, and Israel, and we are particularly grateful to the colleagues who were interested in our action.

As Chair (GA) and Vice-Chair (JH-C) we worked hard on the project, but we enjoyed the possibilities offered for collaboration and furthering exchanges between researchers in IoT security and cryptography in Europe. In particular, we are proud that the CRYPTACUS Action achieved a number of successes that can be reflected in the following figures:

- 32 short-term scientific missions
- 5 scientific meetings

- 2 training schools
- 3 workshops and 1 conference

In total, more than 120 researchers took part in related events or activities. We want to thank the Work Package Leaders and Vice-Leaders Prof. Serge Vaudenay, Prof. Frederic Armknecht, Prof. Andrey Bogdanov, Prof. Mirosław Kutyłowski, Prof. Lejla Batina, Prof. Ricardo Chaves, Prof. Flavio Garcia, and Prof. Alex Biryukov. A special thanks as well to Prof. Bart Preneel.

Book Contents

The book is divided into 13 chapters. They can be read independently, but are organised into 5 parts covering topics with some commonalities.

In Part I, the reader can find a very interesting and general introduction by Mirosław Kutyłowski, Piotr Syga, and Moti Yung called **Emerging Security Challenges for Ubiquitous Devices**.

After that, there is a part on Lightweight Cryptographic Primitives where 3 chapters try to offer insightful views of the state of the art on symmetric lightweight cryptographic primitives. The chapter **Catalog and Illustrative Examples of Lightweight Cryptographic Primitives** by Aleksandra Mileva, Vesna Dimitrova, Orhun Kara, and Miodrag Mihaljević nicely exposes the state of the art in the discipline, covering the most important proposals in detail. This is aptly complemented by the next chapter **Selected Design and Analysis Techniques in Contemporary Symmetric Encryption**, where Vasily Mikhalev, Miodrag Mihaljević, Orhun Kara, and Frederik Armknecht offer a splendid review of the techniques and reasoning behind the most successful approaches to designing and attacking these systems. Last, but not least, we conclude this part with an exceptional first-person account of the many issues that surrounded the failed attempts to standardise a couple of NSA's proposed lightweight block ciphers in **An Account of the ISO/IEC Standardization of the Simon and Speck Block Cipher Families** by Atul Luyks and Tomer Ashur.

In the next part of the book, called Authentication Protocols, we focus on lightweight and ultra-lightweight authentication protocols. The section starts with a chapter by Lucjan Hanzlik and Mirosław Kutyłowski titled **ePassport and eID Technologies**, where the authors examine the existing ePassport literature and offer some new solutions and open problems. Xavier Carpent, Paolo DArco, and Roberto De Prisco contributed the chapter **Ultra-lightweight Authentication** where they elaborate on the good and bad practices of previous ultra-lightweight protocols. Finally, Gildas Avoine, Ioana Boureanu, Pascal Lafourcade, David Gérault, Gerhard Hancke, Pascal Lafourcade, and Cristina Onete end this part of the book with their work **From Relay Attacks to Distance-Bounding Protocols**, an area of research that has seen many developments recently and some successful industrial applications that make it more timely and relevant than ever.

The next part is composed of 4 chapters, and can be generally described as Hardware Implementation and Systems. It starts with 2 works devoted to side-channel analysis. The first one is by Lejla Batina, Milena Djukanovic, Annelie Heuser, and Stjepan Picek with the title **It Started with Templates: The Future of Profiling in Side-Channel Analysis**. There the authors present a nice recap on side-channel analysis over the years, with special interest in the use of machine learning to speed it up, and they discuss its future and some open problems. The following chapter is by Apostolos P. Fournaris, Athanassios Moschos, and Nicolas Sklavos and is titled **Side-Channel Attack Assessment Platforms and Tools for Ubiquitous Systems**. These authors also present an insightful perspective on the evolution of this field, and then introduce their latest results and tools in the area.

The next two chapters are in the same area, but cover totally different topics. The first is by Darren Hurley-Smith and Julio Hernandez-Castro and is titled **Challenges in Certifying Small-Scale (IoT) Hardware Random Number Generators**. The authors discuss some of their recent results in analysing hardware random number generators and present some of the limitations of the current approaches used to certify their security, proposing a number of ideas to try and solve these issues. Finally, Aurélien Francillon, Sam L. Thomas, and Andrei Costin propose a study and in-depth description and comparison of the best tools and techniques to detect bugs in firmware in their chapter **Finding Software Bugs in Embedded Devices**.

The last part of the book hosts two works dealing with Privacy and Forensics. Agusti Solanas, Edgar Batista, Fran Casino, Achilleas Papageorgiou, and Constantinos Patsakis present **Privacy-Oriented Analysis of Ubiquitous Computing Systems: A 5-D Approach**, where they show in great detail some of the most pressing issues in privacy on IoT systems and propose a methodology for its improved analysis. Finally, Sasa Mrdovic deals with some of the differences between classical computer forensics and the more challenging forensic analysis of IoT systems, discussing the many open problems in the area but also its relevance in **IoT Forensics**.

cost
EUROPEAN COOPERATION
IN SCIENCE & TECHNOLOGY

Funded by the Horizon 2020 Framework Programme of the European Union

Rennes, France — Gildas Avoine
Canterbury, UK — Julio Hernandez-Castro

Acknowledgements

Finally, we want to offer our thanks to Isabelle Mesguen, from INSA Rennes, whose administrative and organisational skills constituted a major contribution to the successful running of the Action. It was always a joy to work with COST's Science Officer Karina Marcus and Administrative Officer Andrea Tortajada.

This book is the product of our good fortune in convincing so many top researchers to participate and lend their work and their time to it. We sincerely hope you enjoy it and that it is useful for your work as a researcher or practitioner.

One last aspect of the book that we would like to bring to your consideration is the number of ideas it presents, some of which we hope will serve as inspiration on open problems and future research avenues.

Lastly, we want to thank Ronan Nugent from Springer, who with his enthusiasm for the book and infinite patience contributed greatly to its creation.

Rennes, France — Gildas Avoine
Canterbury, UK — Julio Hernandez-Castro

Contents

Part I Introduction

Part II Lightweight Cryptographic Primitives

Part III Authentication Protocols

Part IV Hardware Implementation and Systems

Part V Privacy and Forensics

Contributors

Frederik Armknecht University of Mannheim, Mannheim, Germany

Tomer Ashur imec-COSIC, KU Leuven, Leuven, Belgium

TU Eindhoven, Eindhoven, The Netherlands

Gildas Avoine Univ Rennes, INSA Rennes, CNRS, IRISA, Rennes, France

Lejla Batina Radboud University, Nijmegen, The Netherlands

Edgar Batista SIMPPLE, Tarragona, Catalonia, Spain

Ioana Boureanu University of Surrey, Guildford, UK

Xavier Carpent University of California, Irvine, CA, USA

Fran Casino University of Piraeus, Piraeus, Greece

Andrei Costin University of Jyväskylä – Jyväskylän Yliopisto, Jyväskylä, Finland

Paolo D'Arco University of Salerno Fisciano, Italy

Roberto De Prisco University of Salerno, Fisciano, Italy

Vesna Dimitrova University "Ss Cyril and Methodius" Skopje, Skopje, Republic of Macedonia

Milena Djukanovic University of Montenegro, Podgorica, Montenegro

Apostolos P. Fournaris Industrial Systems Institute/R.C. ATHENA, University of Patras, Patras, Greece

Aurélien Francillon EURECOM, Sophia Antipolis, Chappes, France

David Gérault Université Clermont Auvergne, Clermont-Ferrand, France

Gerhard P. Hancke City University of Hong Kong, Kowloon, PR China

Lucjan Hanzlik Stanford University and CISPA, Stanford, CA, USA

Julio Hernandez-Castro University of Kent, Canterbury, UK

Annelie Heuser Univ Rennes, Inria, CNRS, IRISA, Rennes, France

Darren Hurley-Smith University of Kent, Canterbury, UK

Orhun Kara Department of Mathematics, IZTECH Izmir Institute of Technology, Izmir, Turkey

Mirosław Kutyłowski University of Science and Technology, Wrocław, Poland

Pascal Lafourcade Université Clermont Auvergne, Clermont-Ferrand, France

Atul Luykx imec-COSIC, KU Leuven, Leuven, Belgium

Aleksandra Mileva Universitet "Goce Delcev", Štip, Republic of Macedonia

Miodrag J. Mihaljević Mathematical Institute, Serbian Academy of Sciences and Arts, Belgrade, Serbia

Vasily Mikhalev University of Mannheim, Mannheim, Germany

Athanassios Moschos University of Patras, Patras, Greece

Sasa Mrdovic University of Sarajevo, Sarajevo, Bosnia and Herzegovina

Cristina Onete University of Limoges, XLIM, Limoges, France

Achilleas Papageorgiou University of Piraeus, Piraeus, Greece

Constantinos Patsakis University of Piraeus, Piraeus, Greece

Stjepan Picek Delft University of Technology, Delft, The Netherlands

Nicolas Sklavos University of Patras, Patras, Greece

Agusti Solanas Universitat Rovira i Virgili, Tarragona, Catalonia, Spain

Piotr Syga Wrocław University of Science and Technology, Wrocław, Poland

Sam L. Thomas Univ Rennes, CNRS, IRISA Rennes, France

Moti Yung Columbia University, New York, NY, USA