

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>

This book is an open access publication.

© The Editor(s) (if applicable) and The Author(s) 2021

Open Access This book is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence and indicate if changes were made.

The images or other third party material in this book are included in the book's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the book's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

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 Kutylowski, 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 Kutylowski, 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 Kutylowski 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 Gérard, 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**.



Funded by the Horizon 2020 Framework Programme of the European Union

Rennes, France
Canterbury, UK

Gildas Avoine
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
Canterbury, UK

Gildas Avoine
Julio Hernandez-Castro

Contents

Part I Introduction

1	Emerging Security Challenges for Ubiquitous Devices	3
	Miroslaw Kutylowski, Piotr Syga, and Moti Yung	
1.1	Introduction	3
1.2	Malicious Devices and Watchdog Concept	4
	1.2.1 Attacks by Malicious Devices	4
	1.2.2 Active Watchdog Concept	5
	1.2.3 Solution Strategy	6
1.3	Privacy	11
	1.3.1 Symmetric Protocols and Deniability	12
	1.3.2 Identity Hiding with Random Key Predistribution	12
	1.3.3 Overloading Identifiers	15
	1.3.4 Pairwise Keys Evolution	15
	1.3.5 Transmission with Errors	16
1.4	Conclusion and Future Directions	17

Part II Lightweight Cryptographic Primitives

2	Catalog and Illustrative Examples of Lightweight Cryptographic Primitives	21
	Aleksandra Mileva, Vesna Dimitrova, Orhun Kara, and Miodrag J. Mihaljević	
2.1	Introduction	21
2.2	Catalog of Lightweight Cryptographic Primitives	23
	2.2.1 Block Ciphers	23
	2.2.2 Stream Ciphers	30
	2.2.3 Hash Functions	31
	2.2.4 Message Authentication Codes	34
	2.2.5 Authenticated Encryption Schemes	38

- 2.3 Illustrative Issues in Security Evaluation of Certain Encryption Schemes..... 38
 - 2.3.1 Reconsidering TMD Tradeoff Attacks for Lightweight Stream Cipher Designs..... 40
 - 2.3.2 Guess-and-Determine Based Cryptanalysis Employing Dedicated TMD-TO 44
- 3 Selected Design and Analysis Techniques for Contemporary Symmetric Encryption 49**

Vasily Mikhalev, Miodrag J. Mihaljević, Orhun Kara, and Frederik Armknecht

 - 3.1 Introduction..... 49
 - 3.2 Keystream Generators with Keyed Update Functions 50
 - 3.2.1 Design Approach 50
 - 3.2.2 On Continuously Accessing the Key 52
 - 3.2.3 The Stream Ciphers Sprout and Plantlet..... 53
 - 3.3 A Generic Attack Against Certain Keystream Generators with Keyed Update Functions 54
 - 3.4 Randomized Encryption Employing Homophonic Coding 58
 - 3.4.1 Background 58
 - 3.4.2 Encryption and Decryption..... 58
 - 3.4.3 Security Evaluation 61
 - 3.5 Conclusion and Future Directions 62
- 4 An Account of the ISO/IEC Standardization of the Simon and Speck Block Cipher Families..... 63**

Tomer Ashur and Atul Luykx

 - 4.1 Introduction..... 63
 - 4.2 Simon and Speck 64
 - 4.2.1 Simon 64
 - 4.2.2 Speck 65
 - 4.3 Simon and Speck’s “Design Rationale”..... 66
 - 4.3.1 Lack of New Information 67
 - 4.3.2 Choice of the Number of Rounds 68
 - 4.3.3 Misquoting Existing Work 71
 - 4.4 The ISO/IEC JTC 1 Standardization Process 72
 - 4.5 The Standardization Process of Simon and Speck in ISO/IEC 29192-2 73
- Part III Authentication Protocols**
- 5 ePassport and eID Technologies 81**

Lucjan Hanzlik and Mirosław Kutylowski

 - 5.1 Application Scenarios..... 81
 - 5.1.1 Remote vs. Local Use 81
 - 5.1.2 Actors and Scenarios 83
 - 5.1.3 Goals of Protocol Execution 84

- 5.2 Threats and Security Requirements 84
 - 5.2.1 Assets 84
 - 5.2.2 Threats 85
- 5.3 Cryptographic Protocols for eIDs 86
 - 5.3.1 Preventing eID Forgeries 86
 - 5.3.2 Enforcing Owner’s Consent 88
 - 5.3.3 EID Authentication and Preventing Cloning 90
 - 5.3.4 Authenticating the Terminal and Its Rights 92
 - 5.3.5 Proof of Interaction 92
 - 5.3.6 Passive Tracing 92
 - 5.3.7 Eavesdropping 93
- 5.4 PKI 94
- 5.5 Challenges for eID Systems 94
- 5.6 Future Directions 96
- 6 Ultra-lightweight Authentication 99**
 Xavier Carpent, Paolo D’Arco, and Roberto De Prisco
 - 6.1 Introduction 99
 - 6.1.1 A Fully Connected World of Small Devices 99
 - 6.1.2 Authentication: Protocol Classification and Physical Constraints 100
 - 6.1.3 Design Challenges 101
 - 6.1.4 Organization of the Chapter 102
 - 6.2 Ultra-lightweight Authentication Protocols 102
 - 6.3 Weaknesses and Pitfalls 106
 - 6.3.1 Poor Diffusion and Linearity 106
 - 6.3.2 Poor Message Composition 107
 - 6.3.3 Biased Output 107
 - 6.3.4 Rotations 108
 - 6.3.5 Vulnerability to Knowledge Accumulation 108
 - 6.3.6 Dubious Proofs of Security: Randomness Tests and Automated Provers 109
 - 6.4 Towards a Sound Approach 110
 - 6.4.1 State of the Literature 110
 - 6.4.2 Promising Avenues 110
 - 6.4.3 The Reductionist Approach 111
 - 6.5 Conclusions 112
- 7 From Relay Attacks to Distance-Bounding Protocols 113**
 Gildas Avoine, Ioana Boureanu, David Gérard, Gerhard P. Hancke, Pascal Lafourcade, and Cristina Onete
 - 7.1 An Introduction to Relay Attacks and Distance Bounding 113
 - 7.1.1 Relay Attacks 114
 - 7.1.2 Distance Bounding 114
 - 7.1.3 Other Relay-Countermeasures 115

7.2	Relay Attacks in Practice	115
7.2.1	Basic Relay Strategies	116
7.2.2	Advanced Relay Strategies	117
7.3	Canonical Distance-Bounding Protocols	119
7.3.1	General Structure	119
7.3.2	The Hancke-Kuhn Protocol	120
7.3.3	The Brands-Chaum Protocol	121
7.4	Distance-Bounding Threat Model and Its Formal Treatments	122
7.4.1	Main Threat-Model	122
7.4.2	Provable Security and Formal Verification	123
7.5	Distance-Bounding Protocols in Practice	125
7.5.1	NXP's Mifare Technology	125
7.5.2	3DB Technology	127
7.5.3	Relay-Resistance in EMV	127
7.6	Current Challenges in Distance Bounding	128
7.6.1	Theory vs. Practice	128
7.6.2	Application-Aware DB	129
7.6.3	Specialist Implementations and Slow Adoption	130

Part IV Hardware Implementation and Systems

8	It Started with Templates: The Future of Profiling in Side-Channel Analysis	133
	Lejla Batina, Milena Djukanovic, Annelie Heuser, and Stjepan Picek	
8.1	Introduction	133
8.2	Profiled Side-Channel Attacks	135
8.2.1	Definition of Profiling Attacks	135
8.2.2	Data Preprocessing	136
8.2.3	Feature Engineering	137
8.3	Template Attacks	138
8.3.1	Context of Template Attack	139
8.3.2	Standard Template Attack	140
8.3.3	Pooled Template Attack	140
8.3.4	Stochastic Attack	140
8.4	Machine Learning-Based Attacks	141
8.4.1	Conducting Sound Machine Learning Analysis	142
8.5	Performance Metrics	144
8.6	Countermeasures Against SCA	144
8.7	Conclusions	145
9	Side Channel Assessment Platforms and Tools for Ubiquitous Systems	147
	Apostolos P. Fournaris, Athanassios Moschos, and Nicolas Sklavos	
9.1	Introduction	147
9.2	Side Channel Attacks, Leakage Assessment Methods and Problems	149

- 9.2.1 Side Channel Attack Categories 150
- 9.2.2 Leakage Assessment Using t-Test 152
- 9.2.3 Practical Considerations in SCA Trace Collection 153
- 9.3 Side Channel Attack Trace Collection Platforms 154
 - 9.3.1 Proposing a Fast Trace Collection Approach
Beyond the Traditional Model 156
- 9.4 A Use Case of a Flexible and Fast Platform for DUT SCA
Evaluation 158
- 9.5 Conclusions 162
- 10 Challenges in Certifying Small-Scale (IoT) Hardware Random
Number Generators 165**
 - Darren Hurley-Smith and Julio Hernandez-Castro
 - 10.1 Introduction 165
 - 10.2 Certification, Standards, and Testing 167
 - 10.3 Challenges in Data Collection 169
 - 10.4 Appropriate Selection of Tests 171
 - 10.4.1 Randomness Testing Under Data Collection
Constraints: Analyzing the DESFire EV1 173
 - 10.4.2 Identifying Issues with Quantum Random Number
Generators 177
 - 10.5 Conclusion 180
- 11 Finding Software Bugs in Embedded Devices 183**
 - Aurélien Francillon, Sam L. Thomas, and Andrei Costin
 - 11.1 The Challenges of Embedded Devices and Software 183
 - 11.1.1 Lack of Transparency 184
 - 11.1.2 Lack of Control 184
 - 11.1.3 Lack of Resistance to Attacks 184
 - 11.1.4 Organization of This Chapter 185
 - 11.1.5 Classification of Embedded Systems 185
 - 11.2 Obtaining Firmware and Its Components 186
 - 11.2.1 Collecting Firmware Packages 186
 - 11.2.2 Extracting Firmware from Devices 187
 - 11.2.3 Unpacking Firmware 188
 - 11.2.4 Firmware Unpacking Frameworks 188
 - 11.2.5 Modifying and Repacking Firmware 189
 - 11.3 Static Firmware Analysis 190
 - 11.3.1 Simple Static Analysis on Firmware Packages 190
 - 11.3.2 Static Code Analysis of Firmware Packages 192
 - 11.4 Dynamic Firmware Analysis 194
 - 11.4.1 Device-Interactive Dynamic Analysis Without
Emulation 195
 - 11.4.2 Device-Interactive Dynamic Analysis with Emulation ... 195
 - 11.4.3 Device-Less Dynamic Analysis and Emulation 196
 - 11.5 Conclusion 197

Part V Privacy and Forensics

12 Privacy-Oriented Analysis of Ubiquitous Computing Systems: A 5-D Approach	201
Agusti Solanas, Edgar Batista, Fran Casino, Achilleas Papageorgiou, and Constantinos Patsakis	
12.1 Introduction.....	201
12.1.1 Goal and Plan of the Chapter	203
12.2 Background and Previous Work on Privacy in UCS.....	203
12.3 5-D Classification and Analysis of Privacy Risks	205
12.3.1 Identity Privacy	206
12.3.2 Query Privacy	207
12.3.3 Location Privacy	208
12.3.4 Footprint Privacy	209
12.3.5 Intelligence Privacy.....	210
12.4 Future Trends and Challenges	210
12.4.1 Privacy by Design	211
12.4.2 Individual-Centred Privacy.....	211
12.4.3 Growing Importance of Legislation	212
12.5 Conclusions.....	213
13 IoT Forensics	215
Sasa Mrdovic	
13.1 Introduction.....	215
13.2 Forensics.....	216
13.2.1 Digital Device Forensics	216
13.2.2 Other Digital Forensics.....	217
13.2.3 The Need for IoT Forensics	218
13.3 Challenges in IoT Forensics	218
13.3.1 General Issues	219
13.3.2 Evidence Identification, Collection and Preservation.....	219
13.3.3 Evidence Analysis and Correlation	220
13.3.4 Presentation	220
13.4 Opportunities of IoT Forensics	221
13.5 An Example of an IoT Forensics Case	221
13.6 Research Overview	225
13.6.1 New Models and Frameworks	225
13.6.2 Preparation Step with Repository	227
13.6.3 Real-World Systems	228
13.7 Conclusion and Future Research Directions	229
References	231

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 Gérard 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 Kutylowski** 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 Picsek** 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