



River Publishers Series in Communications

CYBERSECURITY AND PRIVACY BRIDGING THE GAP

Samant Khajuria, Lene Sørensen and Knud Erik Skouby (Editors)

WIRELESS WORLD
RESEARCH FORUM


River Publishers

Cybersecurity and Privacy – Bridging the Gap

WIRELESS WORLD
RESEARCH FORUM®

RIVER PUBLISHERS SERIES IN COMMUNICATIONS

Series Editors

ABBAS JAMALIPOUR

*The University of Sydney
Australia*

MARINA RUGGIERI

*University of Rome Tor Vergata
Italy*

Indexing: All books published in this series are submitted to Thomson Reuters Book Citation Index (BkCI), CrossRef and to Google Scholar.

The “River Publishers Series in Communications” is a series of comprehensive academic and professional books which focus on communication and network systems. The series focuses on topics ranging from the theory and use of systems involving all terminals, computers, and information processors; wired and wireless networks; and network layouts, protocols, architectures, and implementations. Furthermore, developments toward new market demands in systems, products, and technologies such as personal communications services, multimedia systems, enterprise networks, and optical communications systems are also covered.

Books published in the series include research monographs, edited volumes, handbooks and textbooks. The books provide professionals, researchers, educators, and advanced students in the field with an invaluable insight into the latest research and developments.

Topics covered in the series include, but are by no means restricted to the following:

- Wireless Communications
- Networks
- Security
- Antennas & Propagation
- Microwaves
- Software Defined Radio

For a list of other books in this series, visit www.riverpublishers.com

Cybersecurity and Privacy – Bridging the Gap

Editors

Samant Khajuria
Lene Tolstrup Sørensen
Knud Erik Skouby

CMI/Aalborg University
Denmark


River Publishers

 **Routledge**
Taylor & Francis Group
LONDON AND NEW YORK

Published 2017 by River Publishers
River Publishers
Alsbjergvej 10, 9260 Gistrup, Denmark
www.riverpublishers.com

Distributed exclusively by Routledge
4 Park Square, Milton Park, Abingdon, Oxon OX14 4RN
605 Third Avenue, New York, NY 10017, USA

Cybersecurity and Privacy – Bridging the Gap/by Samant Khajuria, Lene Tolstrup Sørensen, Knud Erik Skouby.

© 2017 River Publishers. All rights reserved. No part of this publication may be reproduced, stored in a retrieval systems, or transmitted in any form or by any means, mechanical, photocopying, recording or otherwise, without prior written permission of the publishers.

Routledge is an imprint of the Taylor & Francis Group, an informa business

ISBN 978-87-93519-66-4 (print)

While every effort is made to provide dependable information, the publisher, authors, and editors cannot be held responsible for any errors or omissions.

DOI: 10.1201/9781003337812

Contents

Foreword	xi
Preface	xiii
List of Figures	xv
List of Tables	xix
List of Abbreviations	xxi
Introduction	1
1 An Introduction to Security Challenges in User-Facing Cryptographic Software	15
Greig Paul and James Irvine	
1.1 Usability and Security	15
1.2 Background	16
1.3 Practical Cryptographic Implementation	17
1.4 Analysis of a Selection of Android Encryption Apps	20
1.4.1 Main Findings	21
1.5 Priorities to Improve upon Existing Applications	23
1.6 Implementation Considerations	24
1.6.1 Key Derivation Stage	24
1.6.2 Master Key Generation and Use	25
1.6.3 Cipher Use and Initialisation	26
1.6.4 Indistinguishability and Resistance to Malleability	27
1.6.5 Authentication of Ciphertexts	29
1.6.6 Padding Attacks	32
1.7 Discussion	34
1.8 Conclusions	35
References	36

2	“Take It or Leave It”: Effective Visualization of Privacy Policies	39
	Prashant S. Dhotre, Anurag Bihani, Samant Khajuria and Henning Olesen	
2.1	Introduction	39
2.2	Related Work	42
2.2.1	Survey and Machine Learning-based Methodologies	43
2.2.2	Privacy Enhancing Tools	44
2.3	Privacy Policy Elucidator Tool (PPET)	45
2.3.1	Privacy Categories Definition (Core Contents of a Privacy Policy)	45
2.3.2	General Description of the Tool	46
2.3.3	Corpus Design	47
2.3.4	Preprocessing	49
2.3.5	Privacy Policy Detector	50
2.3.6	Database Description	50
2.4	PPET Architecture and Modelling	50
2.4.1	Classification	53
2.4.2	Summarization and Ranking	54
2.5	Results	55
2.6	Recommendations	60
2.7	Conclusion and Future Work	61
	References	62
3	A Secure Channel Using Social Messaging for Distributed Low-Entropy Steganography	65
	Eckhard Pfluegel, Charles A. Clarke, Joakim G. Randulff, Dimitris Tsaptsinos and James Orwell	
3.1	Introduction	65
3.1.1	Outline of Proposed Method	67
3.1.2	Research Contributions	68
3.1.3	Chapter Organisation	68
3.2	Previous Work	68
3.2.1	UP Anonymity	70
3.2.2	UGC Confidentiality	71
3.2.3	Distributed High-Entropy Steganography Approach	72
3.3	Proposed Architecture	74

3.4	Implementation	76
3.5	Conclusion	78
	References	79
4	Computational Trust	83
	Birger Andersen, Bipjeet Kaur and Henrik Tange	
4.1	Introduction	83
4.2	Trust	84
4.3	Security and Trust	87
4.4	Trust Models	87
	4.4.1 Fuzzy Trust Model Description	89
	4.4.2 Reputation Evaluation	90
	4.4.3 Eigen Trust Algorithm	91
	4.4.4 Notion of Trust	92
4.5	Example: PGP Web of Trust	92
4.6	Example: X.509 Certificates	94
4.7	Summary	95
	References	95
5	Security in Internet of Things	99
	Egon Kidmose and Jens Myrup Pedersen	
5.1	Introduction	99
5.2	Examples of Problematic IoT Devices	101
	5.2.1 IP Camera	101
	5.2.2 Internet Gateways	102
	5.2.3 Smart Energy Meters	103
	5.2.4 Automotive IoT	105
	5.2.5 IoT and Health	107
	5.2.6 The Smart Home and Appliances	109
5.3	Security Challenges in IoT	111
5.4	Security Recommendations	113
5.5	Conclusion	115
	References	115
6	Security in the Industrial Internet of Things	119
	Aske Hornbæk Knudsen, Jens Myrup Pedersen, Mikki Alexander, Mousing Sørensen and Theis Dahl Villumsen	
6.1	Introduction	119
6.2	Background	120

6.3	Introducing Penetration Testing	122
6.4	Methods	123
6.5	Tools	124
6.6	Findings	125
6.7	Results	126
6.8	Recommendations	127
6.9	Conclusion	133
	References	134
7	Modern & Resilient Cybersecurity <i>The Need for Principles, Collaboration, Innovation, Education & the Occasional Application of Power</i>	135
	Ole Kjeldsen	
7.1	Introduction	135
7.2	Trends	137
7.2.1	Trends in Summary	141
7.3	Protect, Detect & Respond	141
7.3.1	Protect	141
7.3.2	Detect	142
7.3.3	Respond	142
7.4	Beyond Protect, Detect and Respond	142
7.4.1	Cyber-Offense	142
7.4.2	Deterrence & Disruption	144
7.4.2.1	Resilience	144
7.4.3	Importance of Culture to a Resilient Cybersecurity Strategy	147
7.5	Global Security Intelligence Graph	148
7.5.1	The Use of Big Data	148
7.6	Emerging Innovative Technologies	150
7.6.1	Cloud Computing	150
7.6.2	Internet of Things	151
7.6.3	Artificial Intelligence	152
7.7	Partnerships	155
7.8	Conclusion	156
8	Building Secure Data Centers for Cloud Based Services – <i>A Case Study</i>	161
	Lars Kierkegaard	
8.1	The Emergence of a New Industrial Era	161

8.2	Cloud Based Services and Data Centers	163
8.3	Types of Data Centers	163
8.4	Security Considerations	164
8.5	Case: Teracom A/S	164
8.6	Future Perspectives	168
	References	168

9 Pervasive Governance – Understand and Secure Your Transaction Data & Content 169

Kristoffer Rohde

9.1	Introduction	169
9.2	The Challenges and Risks of Unmanaged Data & Content . .	171
9.2.1	The Fragmented Approach	172
9.2.2	The Classic Records Management Approach	173
9.2.3	Keeping Legacy Systems Alive – Just In Case	174
9.2.4	The Ideal Scenario	175
9.2.4.1	Enterprise content management	175
9.2.4.2	Core retention capability	176
9.2.4.3	Formal records management capability . .	176
9.2.4.4	Archiving & decommissioning – privacy by design	176
9.3	The Need for a Pervasive Governance Strategy	177
9.4	Understanding Your Unstructured Content	178
9.4.1	Automated Intelligence	179
9.4.2	Content Classification	179
9.4.3	Actionable Intelligence through Reporting	180
9.4.4	Automating Policy	180
9.5	An Application Decommissioning Program	181
9.5.1	The Decommissioning Factory	182
9.5.2	Developing a Roadmap	182
9.5.3	Phase 1: Program Governance	182
9.5.4	Phase 2: Application Decommissioning Factory Bootstrap	183
9.5.4.1	Train IT staff	183
9.5.4.2	Coordinate with other business services . .	183
9.5.4.3	Automate technology selection	184
9.5.4.4	Use proof of concept to reduce risk	184
9.5.5	Phase 3: Application Decommissioning Projects . .	184
9.5.5.1	Business and data analysis	185

9.5.5.2	Design and build	185
9.6	Conclusion – Solving the Challenges of Unmanaged Data & Content	186
	References	188
10	Challenges of Cyber Security and a Fundamental Way to Address Cyber Security	189
	Fei Liu and Marcus Wong	
10.1	Introduction	190
10.2	Security by Design	192
10.2.1	Functional Design over Security Design	194
10.2.2	Proliferation of Internet	195
10.2.3	Being a Big Target	195
10.2.4	Quick to Market	196
10.2.5	Design Aspect	197
10.3	Cyber Security Paradigm Shift	198
10.3.1	Security Assurance	199
10.3.2	Security Assurance Challenges	199
10.3.3	Market Place Challenges	201
10.3.4	Regulatory Challenges	202
10.3.5	Requirements of Security Assurance	202
10.4	Security Assurance Process	203
10.4.1	Goals of Security Assurance	203
10.4.2	Challenges of Security Assurance	204
10.4.3	3GPP Security Assurance	205
10.4.4	3GPP Security Assurance Approach	207
10.4.5	Security Assurance around the Globe	209
10.5	Conclusion	210
	References	211
	Index	213
	About the Editors	215

Foreword

The WWRF Series in Mobile Telecommunications

The Wireless World Research Forum (WWRF) is a global organization bringing together researchers into a wide range of aspects of mobile and wireless communications, from industry and academia, to identify the key research challenges and opportunities. Members and meeting participants work together to present their research and develop white papers and other publications on the way to the Wireless World. Much more information on the Forum, and details of its publication programme, are available on the WWRF website www.wwrf.ch. The scope of WWRF includes not just the study of novel radio technologies and the development of the core network, but also the way in which applications and services are developed, and the investigation of how to meet user needs and requirements.

WWRF's publication programme includes use of social media, online publication via our website and special issues of well-respected journals. In addition, where we have identified significant deserving subjects, WWRF is keen to support the publication of extended expositions of our material in book form, either singly-authored or bringing together contributions from a number of authors. This series, published by River Publications, is focused on treating important concepts in some depth and bringing them to a wide readership in a timely way. Some will be based on extending existing white papers, while others are based on the output from WWRF-sponsored events or from proposals from individual members.

We believe that each volume of this series will be useful and informative to its readership, and will also contribute to further debate and contributions to WWRF and more widely.

Dr. Nigel Jefferies
WWRF Chairman

Professor Klaus David
WWRF Publications Chair



Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>

Preface

This book is motivated by activities and collaborations within World Research Wireless Forum (WWRF) especially Working Group A/B. Cybersecurity and privacy are issues that in a connected world are raising concerns of wide groups including the scientific community; industry; governments and politicians; and civic groups. There are daily reports on major security breaches with huge economic and social impact and on inappropriate use of private data. This result in loss of trust in the digital platforms companies loose revenue and public institutions are discredited.

Global trends in cybersecurity and privacy are discussed and possible remedies to counter unwarranted developments are analyzed from both academic and industry point of views.

The book is addressing security professionals and university audiences.

Sincerely thanks to authors Anurag Bihani, STES's Sinhgad Institute of Technology and Science, Pune, India; Aske Hornbæk Knudsen, Electronic Systems, Aalborg University, Denmark; Bipjeet Kaur, Technical University of Denmark, Ballerup Campus (DTU); BirgerAndersen, Technical University of Denmark, Ballerup Campus (DTU); Charles A. Clarke, School of Computer Science and Mathematics, Kingston University, Kingston upon Thames, London, United Kingdom; DimitrisTsaptsinos, School of Computer Science and Mathematics, Kingston University, Kingston upon Thames, London, United Kingdom; Eckhard Pfluegel, School of Computer Science and Mathematics, Kingston University, Kingston upon Thames, London, United Kingdom; Egon Kidmose, Electronic Systems, Aalborg University, Denmark; Fei Liu, 2012 Shield Laboratories, Huawei Technologies, Singapore; Greig Paul, Department of Electronic & Electrical Engineering, University of Strathclyde, Glasgow, United Kingdom; Henning Olesen, Center for Communication, Media and Information Technologies (CMI), Aalborg University Copenhagen, Copenhagen, Denmark; Henrik Tange, Technical University of Denmark, Ballerup Campus (DTU); James Irvine, Department of Electronic & Electrical Engineering, University of Strathclyde, Glasgow,

United Kingdom; James Orwell, School of Computer Science and Mathematics, Kingston; University, Kingston upon Thames, London, United Kingdom; Jens Myrup Pedersen, Electronic Systems, Aalborg University, Denmark; Joakim G. Randulff, School of Computer Science and Mathematics, Kingston University, Kingston upon Thames, London, United Kingdom; Kristoffer Rohde, Principal Sales Engineer, Opentext/EMC/Dell; Lars Kierkegaard, Founder of InnoPaze; Marcus Wong, Wireless Security Research and Standardization, Huawei Technologies, USA; Mikki Alexander, Electronic Systems, Aalborg University, Denmark; Mousing Sørensen, Electronic Systems, Aalborg University, Denmark; Ole Kjeldsen, Microsoft Corporation, Kongens Lyngby, Denmark; Prashant S. Dhotre, Center for Communication, Media and Information Technologies (CMI), Aalborg University Copenhagen, Denmark; Samant Khajuria, Center for Communication, Media and Information Technologies (CMI), Aalborg University Copenhagen, Denmark; Theis Dahl Villumsen, Electronic Systems, Aalborg University, Denmark

We are grateful for inspiration and support from the publishers and WWRF.

Finally, but not least thanks to Samant Khajuria Lene Tolstrup Sørensen for getting the idea of the book and for tireless effort in collecting the contributions and editing.

Knud Erik Skouby
Copenhagen, March 2017

List of Figures

Figure 1.1	Flow chart indicating the operation of a key derivation function, to derive a cryptographic key from a user-supplied password or passphrase.	18
Figure 1.2	Flow chart indicating the operation of a simple encryption utility, using a password-derived key to encrypt data with a cipher.	18
Figure 1.3	Flow chart indicating the operation of a more complex encryption utility, using a password-derived key to protect a master key, which is then used to encrypt data with a cipher.	19
Figure 1.4	Flow chart indicating the operation of a more complex encryption utility, using a password-derived key to protect a master key, which is then used to encrypt a per-file metadata block, itself incorporating a file encryption key and IV, which are used to protect the file itself.	20
Figure 1.5	Demonstration of the risk of an uninitialised cipher producing identifiable ciphertext output blocks, revealing information about repetition patterns within the plaintext.	27
Figure 1.6	Illustration of cipher block chaining being used to encrypt a second ciphertext block based upon the previous block output, and an initialisation vector used for the first block.	27
Figure 1.7	Illustration of cipher block chaining being used to decrypt two ciphertext blocks. Note that the output of the second cipher block (i.e. the plaintext) is derived from the cipher block output XOR'd with the previous ciphertext block, showing that arbitrary modifications can be made to the underlying plaintext block by manipulating the ciphertext.	30
Figure 1.8	Illustration of the Encrypt-then-MAC (ETM) construct, where the plaintext is first encrypted, resulting in a ciphertext. This ciphertext then acts as the input to the MAC function, producing an authenticator output for the ciphertext itself.	31

Figure 1.9	Illustration of the MAC-then-Encrypt (MTE) construct, where the incoming plaintext is passed through the MAC authenticator function initially. The output of this function, the authenticator, is then appended to the plaintext, and the result is then encrypted by the cipher, producing a ciphertext containing both the plaintext and MAC of the plaintext.	31
Figure 1.10	Illustration of the Encrypt-and-MAC (EAM) construct, where the encryption and authentication processes are carried out independently. The resulting MAC encompasses the plaintext, such that the ciphertext must first be decrypted, and then the computed plaintext authenticated against the authenticator function.	32
Figure 2.1	Privacy Policy Elucidator Tool (PPET) dashboard (Add-on in action: Privacy policy distribution).	48
Figure 2.2	Privacy policy analysis and visualization workflow.	51
Figure 2.3	The training and testing module of the proposed system.	52
Figure 2.4	Mapping of feature to class using Naïve network.	53
Figure 2.5	Add-on in action: Panel showing the ratings of www.google.co.in	56
Figure 2.6	Add-on in action: Panel showing the ratings of www.snapdeal.com	56
Figure 2.7	Add-on in action: Panel showing the list of attributes (personal and non-personal).	57
Figure 2.8	Add-on in action: Panel showing the use of cookies among the analyzed privacy policies in this study.	58
Figure 2.9	Add-on in action: Panel showing the user interested section of the privacy policy (Information sharing from flipkart.com).	58
Figure 2.10	Add-on in action: Panel showing the summary of a section of privacy policy (Cookies policy of Amazon.in).	59
Figure 3.1	Distributed architecture for undetectable communication.	75
Figure 3.2	Sending and receiving a message.	77
Figure 4.1	Concept of Internet of Everything (IoE).	84
Figure 4.2	High level computational trust engine.	88
Figure 4.3	Trust level.	88
Figure 6.1	A graphical display of the production line.	121
Figure 6.2	The existing network setup. It should be noted that the bridged connection at the control system PC, which bridges the internal network to the Internet, is not shown.	122

Figure 6.3	The proposed network infrastructure.	129
Figure 7.1	Malware and unwanted software encounter rates for domain-based and non-domain computers.	139
Figure 7.2	Malware encounter rates by country/region in 2Q2016. . .	140
Figure 7.3	Encounter rates for ransomware families by country/region in 2Q2016.	140
Figure 7.4	BotNet takedowns in collaboration between Microsoft and law Enforcement Agencies.	145
Figure 7.5	Resilience through system architecture – networked versus hierarchical flow.	147
Figure 7.6	The explosion of digital data.	149
Figure 7.7	The use of AI in cybersecurity.	154
Figure 8.1	The modern society heavily relies on ICT.	162
Figure 8.2	Typical 200-meter tower used for TV- and radio purposes.	165
Figure 8.3	Teracom A/S data center located in Hove, Denmark. . . .	166
Figure 8.4	The Network Operation Centre (NOC) is the focal point of any state-of-the-art data center.	167
Figure 10.1	Vulnerability by year.	196
Figure 10.2	Threat and attack model.	201
Figure 10.3	3GPP security assurance process.	206
Figure 10.4	International security assurance collaboration.	208



Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>

List of Tables

Table 2.1	Comparison between the difference privacy tools	45
Table 7.1	Data breach statistics	136
Table 7.2	Actions for the ‘over-national entities’ such as the UN or the EU	157
Table 7.3	Actions for nation states	157
Table 7.4	Actions for state agencies at both national, regional and municipal level	158
Table 7.5	Actions for businesses of all sizes	158
Table 7.6	Actions for international SW, HW and services vendors . .	158
Table 7.7	Actions for individuals	159



Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>

List of Abbreviations

AM	Amplitude Modulation
ANSI	American National Standards Institute
DAB	Digital Audio Broadcast
DECT	Digital Enhanced Cordless Telecommunications
DTT	Digital Terrestrial Television
DVB-T	Digital Video Broadcast-Terrestrial
FM	Frequency Modulation
GDPR	General Data Protection Regulation
GSM	Global System for Mobile communication
ICT	Information and Communication Technology
ISO	International Standards Organisation
LTE	Long Term Evolution
NOC	Network Operation Centre
UMTS	Universal Mobile Telecommunication System
UPS	Uninterruptable Power Supply
WAN	Wide Area Network



Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>

Introduction

Cybersecurity and privacy are global issues with a local impact. When any security or privacy breach occurs, it impacts our society at all levels. Trust in the digital platforms is lost; companies lose revenue and even public institutions are discredited. These two issues have become major concerns of wide groups of today's globally connected society; the scientific community; industry; governments and politicians; and civic groups.

Our every-day life is very much dependent on the connected devices we are surrounded by – mobile phones, computer in homes and offices, sensors and machines in factories, hospitals etc. Cybersecurity and privacy concerns are fueled by the collection of huge amount of data exchanged by the connected devices and increasingly collected by Internet of Things (IoT). The IoT technology integrates the Internet as we know it today into a multitude of things, and hence commonly known objects such as clothes, food packing toothbrushes, etc. In this integration a huge amount of data is created. It will be stored in data centers and accessible as via cloud services in cross referenced selections. This vision of IoT incorporates new forms of communication between people and things and between things themselves. A multiplicity of devices/sensors acts outside the reach of the humans: sensors and devices communicate via Internet, analyze and act upon the data they select to provide services for the user. This automated communication and action is a key-feature in the potential of Information and Communication Technologies (ICTs). The interconnected physical devices, vehicles; buildings, and other items embedded with electronics collect and exchange data as basis for new services effectuated on predefined conditions that, however, may be modified in the provision process. The current view is that there will be more than 30 billion interacting devices by the year 2020 (e.g., Forbes, 2016) and the IoT vision foresees use cases in ever more sensitive areas such as e-health, Intelligent Transport System, Smart Grids, smart homes (Patel et al., 2016). It is estimated that around 70% of these will have vulnerability against cybersecurity (Security Intelligence, 2016) as the sharing of data