Information Security and Cryptography

Series Editors

David Basin
Kenny Paterson

Advisory Board

Michael Backes
Gilles Barthe
Ronald Cramer
Ivan Damgård
Andrew D. Gordon
Joshua D. Guttman
Christopher Kruegel
Ueli Maurer
Tatsuaki Okamoto
Adrian Perrig
Bart Preneel

More information about this series at http://www.springer.com/series/4752

Rosario Giustolisi

Modelling and Verification of Secure Exams

Springer

Rosario Giustolisi
Department of Computer Science
IT University of Copenhagen
Copenhagen, Denmark

ISSN 1619-7100 ISSN 2197-845X (electronic)
Information Security and Cryptography
ISBN 978-3-319-67106-2 ISBN 978-3-319-67107-9 (eBook)
https://doi.org/10.1007/978-3-319-67107-9

Library of Congress Control Number: 2018933583

© Springer International Publishing AG 2018
This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.
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, express 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.

Printed on acid-free paper

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

Foreword

We are endeavouring in the relocation of traditional human activities and facilities to the digital world: for example, electronic voting and its diverse security challenges still make researchers and developers alike tingle all over; electronic cash and its intricacies are there for the miners' rapture and, for just a little longer, the layman's bewilderment. If by *exams* we refer to all sorts of activities to verify and mark people's skills towards a degree, a post or a promotion, then this book convinces us that exams are following the same fate as voting or cash, getting an increasing level of computer support.

I was driven by love and respect for my job as an academic when, during 2004, I felt that the final exams of my Computer Security modules deserved the robustness and rigour of a security protocol. Hence, I designed WATA, the first version of the Written Authenticated Though Anonymous secure exam protocol, and soon started using a prototype profitably. Giustolisi chose the dawning challenges of that protocol and its variants as his main research and proficiently elaborated them out as the full-fledged research area and growing business value that secure electronic exams are today.

Although more and more universities are leafing through ways to modernise their exam systems, possibly with some use of computers, I still feel that electronic exams have various dimensions of uncertainty, such as whether they are to be taken on site or from home via the Internet, and then whether they are to be carried out over personal or institutional devices. The first contribution of this book is the design of a taxonomy that serves as a practical play board on which every exam type can be meaningfully positioned, hence understood with respect to its neighbours.

The security requirements of the various exam flavours are far from simple. While anonymous marking is intuitive because any honest candidate would like her test to be marked irrespectively of her identity, privacy steps in somewhat originally. For example, the mark of a candidate is meant to stay private in certain exams, and the candidate herself may be required to stay anonymous; however, the candidate will eventually need to prove her qualification, namely to confirm to someone, such as a lecturer or a boss, that she received a certain mark in a specific exam. Privacy therefore intertwines with universal verifiability, so that exam marks can be verified a posteriori.

The details of many exam protocols that are currently in use are easily accessible through the web. Surprisingly many can be found to insist on threat models that baffle a security protocol analyst, for example with their strong reliance on some bureaucrats' office to exercise the association between codes and candidates, or between codes and tests. Pseudo-anonymization cannot work without a real Chinese wall to confine the candidates' identities, while news scandals shout out that in practice those bureaucrats and the examiners might collude fraudulently or simply be members of the same family. By contrast, the protocols that follow below make a systematic effort to reduce the trust assumptions and rest on a realistic threat model.

I am very proud to be writing this foreword for a variety of reasons. The main one is the significance of the overarching topic that this book stands on. Exams are ubiquitous and required by qualifications at all levels; they are run virtually every minute somewhere in the world, perhaps more frequently than elections; they involve principals, such as candidates and examiners, who pose potentially contrasting security requirements that are not immutable over time. And finally, if democracy is strictly related to secure electronic voting, then meritocracy, which is one of the biggest attributes of democracy, proceeds from secure electronic exams.

Giampaolo Bella

Contents

1 Introduction 1

1.1 Objectives and Results 2

1.2 Outline 4

2 Preliminaries and Definitions 7

2.1 Tasks 7

2.2 Roles and Principals 8

2.3 Phases 9

2.4 Threats 10

2.5 Taxonomy 12

2.5.1 Exam Types 12

2.5.2 Exam Categories 14

2.6 Exams as Security Protocols 15

2.7 The Applied π-calculus 16

2.8 Modelling Exams Formally 20

3 Security Requirements 23

3.1 Formal Approaches 24

3.2 Authentication 26

3.3 Privacy 30

3.4 Verifiability 34

3.4.1 Individual Verifiability 37

3.4.2 Universal Verifiability 39

3.5 Conclusion 40

4 The Huszti-Pethő Protocol 43

4.1 Reusable Anonymous Return Channel 45

4.2 Protocol Description 47

4.3 Security of Reusable Anonymous Return Channel 50

4.4 Security of the Huszti-Pethő Protocol 54

4.5 Fixing Authentication 61

4.6 Conclusion 63

5 The Remark! Internet-Based Exam 65

5.1 Internet-Based Exams 66

5.2 Exponentiation Mixnet 67

5.3 Protocol Description 68

5.4 Security of Remark! 71

5.5 Conclusion 93

6 The WATA Family 95

6.1 Computer-Assisted and Computer-Based Exams 96

6.2 WATA I & II 97

6.3 WATA III 101

6.4 WATA IV 105

6.5 WATA Without TTP 111

6.5.1 Dispute Resolution 117

6.5.2 Security of WATA Without TTP 118

6.6 Conclusion 122

7 Conclusions 125

Bibliography 129

List of Figures

2.1 A set-theory representation of exams 14
2.2 The grammar for plain processes in the applied π-calculus 17
2.3 The grammar for extended processes in the applied π-calculus . . 18

3.1 A graphical representation of the authentication requirements for exams 29

4.1 Reusable anonymous return channel in the Alice-Bob notation . 47
4.2 The Huszti-Pethő e-exam protocol in the Alice-Bob notation . . 48
4.3 The processes of sender, receivers, and mixer 51
4.4 The instance of sender, receiver, and mixer processes 52
4.5 The instance of sender to analyse message secrecy 52
4.6 The instance of sender to analyse anonymity 52
4.7 Attack trace on sender anonymity 52
4.8 The process of the exam authority that concerns preparation . . 56
4.9 The process of the exam authority that concerns testing, marking, and notification 57
4.10 The process of the candidate 58
4.11 The process of the examiner 59
4.12 The process of the NET 60
4.13 The exam process 60

5.1 The exponentiation mixnet scheme 67
5.2 The Remark! Internet-based exam protocol 69
5.3 The process of the exam authority 73
5.4 The process of the candidate 74
5.5 The process of the mixnet 74
5.6 The process of the examiner 75
5.7 The exam process 75
5.8 The Question Validity individual verifiability-test 79
5.9 The Marking Correctness individual verifiability-test 79
5.10 The Test Integrity individual verifiability-test 80
5.11 The Test Markedness individual verifiability-test 81
5.12 The Mark Integrity individual verifiability-test 82
5.13 The Mark Notification Integrity individual verifiability-test . . . 83
5.14 The Registration universal verifiability-test 86
5.15 The Marking Correctness universal verifiability-test 88
5.16 The Test Integrity universal verifiability-test 90
5.17 The Mark Integrity universal verifiability-test 92

6.1 The WATA II exam protocol 98
6.2 Fragment of a test in WATA II 99
6.3 The WATA III exam protocol 102
6.4 Representation of bits 0 and 1 using visual cryptography 105
6.5 The WATA IV exam protocol 107
6.6 The candidate paper sheet in WATA IV 108
6.7 Preparation phase 113
6.8 Testing phase 114
6.9 Marking phase 114
6.10 Notification phase 114

List of Tables

2.1 Acronyms for exam types 13
2.2 Sets of exam types 14

3.1 Individual and universal verifiability 36

4.1 Comparison of Huszti and Pethő's requirements with ones proposed in this book 44
4.2 Equational theory to model reusable anonymous return channel . 53
4.3 Equational theory to model the Huszti-Pethő protocol 54
4.4 Summary of the analysis of the Huszti-Pethő protocol 55
4.5 Summary of the analysis of authentication of the modified Huszti-Pethő protocol 62

5.1 Equational theory to model Remark! 72
5.2 Summary of authentication and privacy analysis of Remark! . . . 76
5.3 Summary of the analysis of Remark! for I.V. requirements . . . 83
5.4 Summary of the analysis of Remark! for U.V. requirements . . . 93

6.1 Equational theory to model the enhanced protocol 118
6.2 Summary of the analysis of the enhanced protocol 123