Authentication in Insecure Environments

Sebastian Pape

Authentication in Insecure Environments

Using Visual Cryptography and Non-Transferable Credentials in Practise

Springer Vieweg

Dr. Sebastian Pape
Dortmund, Germany

Doctoral thesis at the University of Kassel, Department Electrical Engineering and Computer Science, defended on September 2nd, 2013, submitted with the title "The Challenge of Authentication in Insecure Environments" by Sebastian Pape

ISBN 978-3-658-07115-8 ISBN 978-3-658-07116-5 (eBook)
DOI 10.1007/978-3-658-07116-5

The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available in the Internet at http://dnb.d-nb.de.

Library of Congress Control Number: 2014948456

Springer Vieweg
© Springer Fachmedien Wiesbaden 2014
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. Exempted from this legal reservation are brief excerpts in connection with reviews or scholarly analysis or material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the work. Duplication of this publication or parts thereof is permitted only under the provisions of the Copyright Law of the Publisher's location, in its current version, and permission for use must always be obtained from Springer. Permissions for use may be obtained through RightsLink at the Copyright Clearance Center. Violations are liable to prosecution under the respective Copyright Law.
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.
While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

Printed on acid-free paper

Springer Vieweg is a brand of Springer DE.
Springer DE is part of Springer Science+Business Media.
www.springer-vieweg.de

For my parents

Preface

For scientific research it is essential to have interested conversational partners who come up with helpful suggestions, references and especially criticism. At this point, I like to thank them for their kind support when writing this thesis.

I particularly owe thanks to my supervisor Prof. Dr. Lutz Wegner, who in the first place made this work possible, supported me at any time with thematically and scientific advice and also untiringly encouraged me regarding all other aspects.

I thank Prof. Dr. Jan Jürjens for enabling me to finish my work at his chair, for his active support and for appraising this work.

Furthermore, I appreciate very constructive and helpful discussions about the application of anonymous credentials with Prof. Dr. Andreas Pfitzmann. I am also very thankful to Dipl.-Inf. Marit Hansen for her valuable advice, which facilitated entering the topic of privacy-enhancing technologies.

I also like to thank Dr. Sebastian Gajek and M.Sc. Denise Doberitz for fruitful discussions on visual cryptography which had a large influence that this subject was examined to this extent.

I extend my thanks to all to my former colleagues at Kassel University as well as to my current colleagues at Dortmund Technical University and the Fraunhofer Institute for Software and Systems Engineering. In particular, my thanks go to Dipl.-Ing. Michael Möller for his active support and to Dipl.-Inf. Christian Wessel for numerous helpful comments and suggestions.

I am grateful to Bruce Schneier and Kim Cameron for the permission to include photographs from their blogs in this work. I also like to thank the anonymous reviewers whose comments helped to improve the papers which were published previously and which this work is based on.

I express my sincere gratitude to all the persons mentioned here. Nevertheless, without saying all possible errors and inaccuracies go completely to my account. I am grateful for further suggestions or comments on this work.

Dortmund Sebastian Pape

Contents

List of Figures XIII

List of Tables XV

1 Introduction 1
1.1 Authentication in Insecure Environments 1
1.2 Overview 4

I Preliminaries 7

2 Mathematical and Cryptographic Foundation 9
2.1 Preliminaries and Notation 9
2.1.1 Functions and Algorithms 9
2.1.2 Basic Group Theory 18
2.2 Encryption Schemes 22
2.2.1 Notions of Security 27
2.2.2 Passive Attacks 28
2.2.3 Security Models 35
2.2.4 Active Attacks 45
2.2.5 Practical Security 53
2.3 Cryptographic Hardness Assumptions 58
2.3.1 The Factoring and RSA Assumption 58
2.3.2 The Discrete Logarithm and Diffie-Hellman Assumptions 61
2.4 Hash Functions and Digital Signature Schemes 67
2.4.1 Hash Functions 67
2.4.2 Digital Signature Schemes 68
2.4.3 Blind Signatures 72

II Human Decipherable Encryption Schemes 79

3 Introduction, Scenario, and Related Work 81
3.1 Background and Purpose 81
3.2 Overview 84
3.3 Scenarios 85
3.4 Related Work 85

4 Human Decipherable Encryption Scheme 87
4.1 Notation and Terminology 87
4.1.1 Messages, Codings, Ciphertexts and Keys 87
4.1.2 Unicity Distance 89
4.1.3 Encodings and Decodings 95
4.1.4 Human Decipherable Encryption Scheme 103
4.1.5 XOR, EQV and Hamming Functions 117
4.2 Visual Cryptography 119
4.2.1 Pixel-based Visual Cryptography 120
4.2.2 Segment-based Visual Cryptography 124
4.2.3 Applications of Visual Cryptography 127
4.2.4 Using Key-Transparencies Multiple Times 130

5 Human Decipherable Encryption Schemes Based on Dice Codings 135
5.1 Dice Codings 135
5.1.1 Underlying Spaces and Parameters 135
5.1.2 Coding Scheme 137
5.2 Basic Version 139
5.2.1 EQV Encryption Scheme 139
5.2.2 Basic Human Decipherable Encryption Scheme 141
5.3 Security Analysis of the Basic Version 145
5.3.1 Ciphertext-Only Attacks Without Side Information 146
5.3.2 Ciphertext-Only Attacks With Side Information 149
5.3.3 Security Models 167
5.4 Dice Codings with Noise 174
5.4.1 Changes in Underlying Spaces and Parameters 174
5.4.2 EQV Encryption Scheme with Noise 175
5.4.3 Human Decipherable Encryption Scheme with Noise . . . 178
5.5 Security Analysis of Dice Codings with Noise 183
5.5.1 Ciphertext-Only Attacks Without Side Information 184
5.5.2 Ciphertext-Only Attacks With Side Information 185
5.5.3 Security Models 192

6 Conclusion and Future Work 197
6.1 Summary and Conclusion 197
6.2 Future Work 198
6.2.1 Addressing Other Senses than Sight 198
6.2.2 Security Assumptions and Models 201
6.2.3 Methods to Improve Reusing the Key-Transparencies . . 202

III Non-Transferable Anonymous Credentials 207

7 Introduction, Scenario, and Related Work 209
7.1 Background and Purpose 209
7.2 Overview 210
7.3 Scenarios 210
7.4 Related Work 211

8 Privacy and Data Security 213
8.1 Notions and Terms of Privacy 213
8.1.1 Anonymity, Pseudonymity, Unlinkability, Untraceability . 213
8.1.2 Trust Levels Regarding Privacy 214
8.2 Anonymous Credentials 215
8.2.1 Properties of Anonymous Credentials 216
8.2.2 Zero-Knowledge Proofs 217
8.2.3 Wallet-With-Observer Architecture 219
8.3 Smartcards and Biometrics 220
8.3.1 Smartcards 220
8.3.2 Biometrics 221

9 Analysis of Non-Transferable Anonymous Credentials 229
9.1 Approaches Aiming at Non-Transferability 229
9.1.1 Embedding Valuable Secrets 229
9.1.2 Biometrically Enforced Non-Transferability 230
9.1.3 Consideration of Other Approaches 231
9.1.4 Security Issues 232
9.1.5 Limiting the Consequences of Security Breaches 242
9.2 Templateless Biometric-Enforced Non-Transferability 244
9.2.1 Adapting Schemes to Work without Templates 246
9.2.2 Comparison of Approaches' Security 249

10 Conclusion and Future Work **253**

10.1 Summary and Conclusion 253

10.2 Future Work 254

IV Outlook and Appendix **257**

11 Summary, Conclusion and Outlook **259**

11.1 Summary 259

11.2 Conclusion 260

11.3 Outlook 261

Example of Pixel-based Visual Cryptography in Detail **265**

Auxiliary Tables and Proofs **271**

Source Code Listings **281**

Bibliography **307**

List of Symbols and Abberviations **349**

Index of Keywords **353**

Index of Names **359**

List of Figures

2.1 Relations between Security Models for Asymmetric Encryption . 38
2.2 Visualisation of Game-Based IND-atk Security Models 39
2.3 Relations between Securitymodels for Symmetric Encryption . . 45
2.4 Setup of Active Attacks on the Communication Channel 45
2.5 Protocol Flow of a Man-in-the-Middle Attack 51
2.6 Keypads 56
2.7 Diffie-Hellman Key Exchange Protocol 64
2.8 Blind Signature Scheme 75
2.9 Chaum's Blind Signature Protocol 77

3.1 Example for Visual Cryptography 83
3.2 Transparencies for Visual Cryptography 84

4.1 Relations of Encoding and Encryption Functions' (Co-)Domains . 87
4.2 Representation of Cipher 91
4.3 Seven-Segment Display: Digits 101
4.4 Seven-Segment Display: Notation of Segments 101
4.5 Example of Pixel-Based Visual Cryptography 120
4.6 Visual Forms of Shares with 4 Subpixels 121
4.7 Visual Forms of Shares Represented by Rotated Half Circles . . . 122
4.8 Shares of a 4 out of 4 Visual Secret Sharing Problem 124
4.9 Shares Usable for Steganography in Visual Cryptography 125
4.10 Principle of Visual Cryptography applied to a 7-Segment Display 126
4.11 Application of Visual Cryptography 129
4.12 Reusing Transparencies in Pixel-Based Visual Cryptography . . . 131
4.13 Segment-Based Visual Cryptography: Sample Encryptions 132
4.14 Segment-Based Visual Cryptography: Possible Keys 133
4.15 Closed Subgroup in Segment-Based Visual Cryptography 134

5.1 Dice Codings: Sample Encodings 136
5.2 Sample Visualisations of $\mathcal{HE}_{\mathsf{DICE}}$ 143
5.3 Representation of Possible Keys with a Binary Tree 166

5.4 Sample Visualisation of the Ext Function 176
5.5 Sample Visualisations of the Noise Function 177
5.6 Sample Visualisations of the Noise^{-1} Function 179
5.7 Sample Visualisation of $\mathcal{HE}^{\star}_{\mathsf{DICE}}$ 181

6.1 'University of Kassel' Written in Grade 2 Braille 199
6.2 Refreshable Braille Display 200
6.3 Rotating $\mathcal{HE}_{\mathsf{DICE}}$-keys 203

8.1 FEIGE-FIAT-SHAMIR Identification Scheme 219
8.2 Fingerprint Charade 223

9.1 Points of Attacking a Biometric System 233
9.2 Sharing a Credential via Radio Transmission 238
9.3 Combining Biometrics with Anonymous Credentials 245
9.4 Modified FEIGE-FIAT-SHAMIR Identification Scheme 248

1 Example of Pixel-based Visual Cryptography: Original Picture . . 266
2 Example of Pixel-based Visual Cryptography: Transparency 1 . . 267
3 Example of Pixel-based Visual Cryptography: Transparency 2 . . 268
4 Example of Pixel-based Visual Cryptography: Overlay 269

List of Tables

2.1 Syverson's Taxonomy of Replay Attacks 53

4.1 International Morse Code (letters) 97
4.2 Example of Hexadecimal Encodings for a 7-Segment Display . . 101
4.3 XOR and Identity Truth Tables 118
4.4 Contingency and Evaluation Table for the Overlay of Two Pixel-Based Transparencies in Visual Cryptography 121
4.5 Contingency and Evaluation Table for the Overlay of Two Segment-Based Transparencies in Visual Cryptography 127
4.6 7-Segment-Display XOR Contingency Table 134

5.1 Dice Codings: Numbers of possible Encodings 136
5.2 Contingency Table for the Encryption with EQV 140
5.3 Contingency and Evaluation Table for the Decryption with EQV . 141
5.4 Possible Numbers of Different Dots for Dice Codings' Ciphertexts 148
5.5 Probabilities of Uniformly Distributed Characters' Dice Codings . 150
5.6 Evaluation of $\mathsf{P}(\#0{*} = 2;3|\mathsf{N})$'s summands for selected N, N_{1*} . 156
5.7 Evaluation of $\mathsf{P}(\#0{*} = 2;2|\mathsf{N})$'s summands for selected N, N_{1*} . 158
5.8 Probabilities to Attack Single Characters Encrypted with $\mathcal{HE}_{\mathsf{DICE}}$ 159
5.9 Expected Value and Standard Deviation of Distributions 160
5.10 Probabilities of Binomial Distributed Characters' Dice Codings . 161
5.11 Number of Needed Ciphertexts to Attack Pairs of Ciphertexts . . 163
5.12 Number of Needed Ciphertexts to Attack Complete Keypads . . . 167
5.13 Contingency and Evaluation Table for the Decryption with EQV^* 180
5.14 Probabilities of Hamming Differences of $\mathcal{HE}^{\star}_{\mathsf{DICE}}$ Encrypted Uniformly Distributed Characters 188
5.15 Conditional Probabilities of Hamming Differences of $\mathcal{HE}^{\star}_{\mathsf{DICE}}$ Encrypted Uniformly Distributed Characters 190
5.16 Probabilities of Determining the Positions of Noise 193

6.1 Contingency Table for Audible Encryption with EQV 201
6.2 Composition of Keys for $\mathcal{HE}^{\star}_{\mathsf{DICE}}$ 204

9.1 Attributes of Different Non-Transferability Approaches 241
9.2 Relevant Risks Enforcing Biometric Authentication 252

1 Pairs of Dice Codings for a Given Number of Different Dots . . . 274
2 Upper Bounds of Probabilities for k Matching Ciphertexts 275
3 Probabilities that N_{i^*} Ciphertexts of i^* Occur 276
4 Probabilities that N_{1^*} Ciphertexts of 1^* Occur with $N_{0^*} = 2$ . . . 277
5 Probabilities that N_{1^*} Ciphertexts of 1^* Occur with $N_{0^*} = 3$ . . . 278
6 Evaluation of $P(\#0* = 3; 3|N)$'s summands for selected N, N_{1^*} . 279
7 Needed CPU Time to Attack Complete Keypads 280