

---

# Contents

<b>1 Introduction</b>	<b>13</b>
1.1 Security vs. Usability: The Need for Design Patterns . . . . .	14
1.2 Computer Security at the Crossroads . . . . .	18
1.3 Why Have Security Specialists Failed to Address Usability? . . . . .	22
1.4 Why Have Usability Specialists Failed to Address Security Issues? . . . . .	26
1.5 Security Principles . . . . .	29
1.6 Original Contributions . . . . .	30
1.7 Thesis Roadmap . . . . .	34
<b>2 Prior Work</b>	<b>37</b>
2.1 Early Work in HCI-SEC . . . . .	37
2.2 Rules and Principles for Designing Usable Systems . . . . .	43
2.3 Properties, Models and Principles for Usable Security . . . . .	48
2.4 Specific Techniques for Aligning Security and Usability . . . . .	59
2.5 Prior and Related Work on Sanitization. . . . .	66
2.6 A Brief Survey of Regulatory and Other Non-Technical Approaches . . . . .	79
2.7 Conclusion . . . . .	100
<b>3 Sanitization and Visibility 1: Operating Systems</b>	<b>101</b>
3.1 Background . . . . .	102
3.2 The Problem of Discarded Data . . . . .	105
3.3 Case Study: <i>Remembrance of Data Passed</i> . . . . .	117
3.4 The Traceback Study . . . . .	127
3.5 Future Work: Cross-Drive Forensics . . . . .	132
3.6 Proposals for Addressing the Sanitization Problem . . . . .	133
3.7 Patterns for User Visibility and Sanitization . . . . .	138
3.8 The Policy Implications of “Complete Delete” . . . . .	140
<b>4 Sanitization and Visibility 2: Applications</b>	<b>143</b>
4.1 Case Study: Sanitizing Web Browser History . . . . .	143
4.2 Case Study: Failed Document Sanitization in Word and Acrobat . . . . .	155

4.3	Conclusion . . . . .	158
<b>5</b>	<b>Solving Secure Email’s “Grand Challenge” with Signature-Only Email</b>	<b>161</b>
5.1	Background: Three Decades in Pursuit of Secure Messaging . . . . .	162
5.2	A Survey of Secure Email Capabilities and Attitudes. . . . .	170
5.3	Signatures Without Sealing . . . . .	182
5.4	Hidden Signatures . . . . .	195
5.5	Conclusions and Recommendations . . . . .	196
<b>6</b>	<b>The Key Certification Problem: Rethinking PKI</b>	<b>201</b>
6.1	A Tale of Two Protocols . . . . .	201
6.2	Reinterpreting the History of PKI . . . . .	203
6.3	Alternatives to X.509 . . . . .	216
6.4	Fundamental Problems with PKI . . . . .	222
6.5	Making PKI Usable . . . . .	236
<b>7</b>	<b>Key Continuity Management</b>	<b>241</b>
7.1	Key Continuity Management . . . . .	241
7.2	Patterns for Improving Message Security . . . . .	249
7.3	Testing KCM with <i>Johnny 2</i> . . . . .	250
7.4	Walk-Through. . . . .	267
7.5	Results and Discussion . . . . .	272
7.6	Conclusion . . . . .	281
<b>8</b>	<b>Regulatory Approaches</b>	<b>283</b>
8.1	Patterns for Regulation . . . . .	284
8.2	The Security Lexicon . . . . .	285
8.3	Spyware and the “Pure Software” Proposal . . . . .	291
8.4	RFID on Consumer Items: The “RFID Bill of Rights”. . . . .	298
8.5	Conclusion . . . . .	301
<b>9</b>	<b>Additional Techniques for Aligning Security and Usability</b>	<b>303</b>
9.1	Additional Patterns for Enhancing Secure Operations . . . . .	303
9.2	Other Applications of User Auditing . . . . .	304
9.3	Operating System Improvements . . . . .	310
9.4	Eliminating the Security Policy “Construction Kit”. . . . .	311
<b>10</b>	<b>Design Principles and Patterns for Aligning Security and Usability</b>	<b>317</b>
10.1	User Visibility and Sanitization Patterns . . . . .	324
10.2	Identification and Key Management Patterns. . . . .	330
10.3	Patterns for Promoting Overall Secure Operation . . . . .	340

<i>CONTENTS</i>	11
<b>11 Future Work: an HCI-SEC Research Agenda</b>	<b>349</b>
11.1 Short Term . . . . .	349
11.2 Long Term . . . . .	356
11.3 A Call for New Patterns . . . . .	365
11.4 In Conclusion . . . . .	370
<b>A Hard Drive Study Details</b>	<b>371</b>
<b>B Mail Security Survey Details</b>	<b>375</b>
B.1 Commercially Oriented Email . . . . .	375
B.2 Financial Communications. . . . .	378
B.3 Personal Email At Home and At Work . . . . .	378
B.4 Communication with Politicians. . . . .	379
<b>C Johnny 2 User Test Details</b>	<b>381</b>
C.1 Description of Test Participants . . . . .	381
C.2 Description of the Testing Process . . . . .	384
C.3 Summaries of Test Sessions . . . . .	402
C.4 OpenSSL Configuration . . . . .	406
<b>D Two Email Proxies</b>	<b>413</b>
D.1 Proxy Philosophy . . . . .	414
D.2 Stream: A PGP Proxy . . . . .	416
D.3 CoPilot: A Proxy or Plug-In that Implements KCM . . . . .	420
<b>E Specific Recommendations to Vendors</b>	<b>425</b>
E.1 Recommendations for Desktop Software . . . . .	425
E.2 Recommendations for Organizations that Send Bulk Email . . . . .	426
E.3 Recommendations for Webmail Providers . . . . .	427
<b>Colophon</b>	<b>471</b>