


Information Security and Cryptography

Series Editors

David Basin , Department of Computer Science F 106, ETH Zürich, Zürich, Switzerland

Kenny Paterson, Information Security Group, Royal Holloway, University of London, Egham, Surrey, UK

Editorial Board

Michael Backes, Department of Computer Science, Saarland University, Saarbrücken, Saarland, Germany

Gilles Barthe, IMDEA Software Institute, Pozuelo de Alarcón, Madrid, Spain

Ronald Cramer, CWI, Amsterdam, The Netherlands

Ivan Damgård, Department of Computer Science, Aarhus University, Aarhus, Denmark

Robert H. Deng , Singapore Management University, Singapore, Singapore

Christopher Kruegel, Department of Computer Science, University of California, Santa Barbara, CA, USA

Tatsuaki Okamoto, Okamoto Research Lab., NTT Secure Platform Laboratories, Musashino-shi, Tokyo, Japan

Adrian Perrig, CAB F 85.1, ETH Zurich, Zürich, Switzerland

Bart Preneel, Department Elektrotechniek-ESAT /COSIC, University of Leuven, Leuven, Belgium

Carmela Troncoso, Security and Privacy Engineering Lab, École Polytechnique Fédérale de Lausa, Lausanne, Switzerland

Moti Yung , Google Inc, New York, NY, USA

Information Security – protecting information in potentially hostile environments – is a crucial factor in the growth of information-based processes in industry, business, and administration. Cryptography is a key technology for achieving information security in communications, computer systems, electronic commerce, and in the emerging information society.

Springer's Information Security & Cryptography (IS&C) book series covers all relevant topics, ranging from theory to advanced applications. The intended audience includes students, researchers and practitioners.

Jörg Schwenk

Guide to Internet Cryptography

Security Protocols and Real-World Attack
Implications



Springer

Jörg Schwenk
Chair for Network and Data Security
Ruhr University Bochum
Bochum, Germany

ISSN 1619-7100 ISSN 2197-845X (electronic)
Information Security and Cryptography
ISBN 978-3-031-19438-2 ISBN 978-3-031-19439-9 (eBook)
<https://doi.org/10.1007/978-3-031-19439-9>

© The Editor(s) (if applicable) and The Author(s), under exclusive license to Springer Nature Switzerland AG 2022

This work is subject to copyright. All rights are solely and exclusively licensed by the Publisher, whether the whole or part of the material is concerned, specifically the rights of 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, 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

To my wife and my children

Preface

In the last two decades, numerous research papers have considerably expanded our knowledge of Internet cryptography, taking into account all details of the different standards and implementations. Some of these papers, especially those on TLS, impacted standardization. This interplay between standardization, implementation, and research is exemplified in TLS 1.3, where numerous research efforts accompanied more than four years of standardization.

This interplay is the topic of this book. Essential Internet standards are described in a language close to applied cryptographic research. Attacks on implementations of these standards are collected from academic and non-academic research because these attacks are our primary source of new insights into real-world cryptography. Summarizing all this information in a single book allows for highlighting cross-influences in standards (e.g., EAP protocols and MIME types) and similarities in cryptographic constructions (e.g., the use of Diffie-Hellman key exchange and challenge-and-response building blocks in numerous protocols).

This book is roughly divided into three parts. Sections 1 to 4 provide an overview and the necessary cryptographic background for the other chapters. At the end of the book, sections 20 and 21 provide additional, helpful background on Internet security, which is, however, not required for the rest of the book.

Important cryptographic standards are described and analyzed in sections 5 to 19. These sections are assigned to TCP/IP network layers, starting from the link layer. Short introductions to these network layers were added to keep the book self-contained. The length of the different chapters differs significantly, which more or less reflects the amount of research done. There are three main focuses: IPsec, TLS, and secure e-mail. IPsec is a hidden champion here: It is a very complex ecosystem of standards, with deployments in non-public networks, which makes research difficult. Since its introduction, TLS has received much attention in the research community. It provided the first real-world example of an adaptive chosen-ciphertext vulnerability. Numerous other attacks have improved our knowledge of TLS; TLS 1.3. is now hardened against all kinds of attacks. This wealth of information made it necessary to devote four chapters to TLS. The last of these chapters summarizes nearly all attacks on TLS published so far and is perhaps the book's most exciting part. Despite

new developments like instant messaging and video conferencing, the security of e-mail communication is still essential in government and business. This topic lends itself to be divided into several chapters: There are OpenPGP, S/MIME, attacks on both standards, and SPAM prevention.

To condense all this knowledge into a single book, omissions are inevitable. Cryptographic primitives are treated as black boxes. We only dive deeper into their internal structure if it is necessary to understand specific attacks. The mathematical formalism is reduced to a minimum and only introduced where it is necessary to explain important cryptographic concepts. For the time being, we omitted post-quantum cryptography because the integration of these new primitives into existing standards is not yet stable. Blockchains are out of the scope of this book, but instant messaging protocols may be included in future editions.

Each chapter has a related work section and Problems. Related work should be regarded as suggestions for further reading, not as an exclusive list of all essential publications. With many excellent researchers worldwide, it can never be complete. Problems are taken from the two-semester undergraduate course in network security at Ruhr University Bochum, both from the weekly exercises and the final exams. They should help to test the reader's knowledge of the subject and may serve as blueprints for other courses.

This book is intended as a guideline for academic courses and a reference guide on Internet security. Chapters 5 to 19 can be taught in any order, only the sections on TLS should be considered a sequence. References to standards should be up-to-date; details omitted here can be found there.

Acknowledgements I want to take the opportunity to thank everyone who helped me to present the many topics of this book in detail. Without the research work at the Chair of Network and Data Security and the intensive discussions about related work, technical details of RFCs, and software implementations that went along with it, many chapters would have been much shorter and less profound. Before going to print, I had the privilege to present the individual chapters to real specialists in the respective field.

For the current edition I would therefore like to thank, in alphabetical order: Fabian Bäumer, Marcus Brinkmann, Nurullah Erinola, Dr. Dennis Felsch, Matthias Gierlings, Dr. Martin Grothe, Dr. Mario Heiderich, Matthias Horst, Prof. Dr. Tibor Jager, Louis Jannett, Lukas Knittel, Dr. Sebastian Lauer, Marcel Maehren, Dr. Christian Mainka, Dr. Robert Merget, Dr. Vladislav Mladenov, Dr. Jens Müller, Dr. Marcus Niemietz, Dominik Noss, Dr. Damian Poddebniak, Simon Rohlmann, Dr. Paul Rösler, Prof. Dr. Sebastian Schinzel, Carsten Schwenk, Prof. Dr. Juraj Somorovsky, Prof. Dr. Douglas Stebila, Tobias Wich and Petra Winkel. The foundations for this book were, of course, laid earlier, and so these thanks naturally also go to all former members of the chair.

Last but not least, I would like to thank my wife, Beate, who helped me with the final editing and made valuable suggestions for revisions, and my children, who gave me the time to work on this book.

Additional material on internet cryptography can be found at internet-cryptography.org.

Contents

1	The Internet	1
1.1	TCP/IP Communication Model	1
1.1.1	Link Layer	3
1.1.2	Internet layer	4
1.1.3	Transport Layer	5
1.1.4	Application Layer	5
1.2	Threats on the Internet	6
1.2.1	Passive Attacks	6
1.2.2	Active Attacks	7
1.3	Cryptography on the Internet	9
	Related Work	10
	Problems	10
	References	10
2	Cryptography: Confidentiality	13
2.1	Notation	13
2.2	Symmetric Encryption	14
2.2.1	Block Ciphers	16
2.2.2	Block Cipher Modes of Operation	17
2.2.3	Stream Ciphers	19
2.2.4	Pseudo-random Sequences	20
2.3	Asymmetric Encryption	21
2.4	RSA Encryption	22
2.4.1	Textbook RSA	22
2.4.2	PKCS#1	23
2.4.3	OAEP	24
2.5	Diffie-Hellman Key Exchange	25
2.5.1	Diffie-Hellman Key Exchange (DHKE)	25
2.5.2	Mathematics: Groups	26
2.5.3	Complexity Assumptions	28
2.6	ElGamal encryption	31

2.6.1	ElGamal encryption	31
2.6.2	Key Encapsulation Mechanism (KEM)	32
2.7	Hybrid Encryption of Messages	33
2.8	Security Goal: Confidentiality	34
	Related Work	36
	Problems	37
	References	39
3	Cryptography: Integrity and Authenticity	43
3.1	Hash Functions	43
3.1.1	Standardized Hash Functions	43
3.1.2	Security of Hash Functions	44
3.2	Message Authentication Codes and Pseudo-random Functions	47
3.3	Authenticated Encryption	49
3.4	Digital Signatures	50
3.5	RSA Signature	51
3.5.1	Textbook RSA	51
3.5.2	RSA-PKCS#1	52
3.6	Discrete Log Based Signature Schemes	52
3.6.1	ElGamal signature	53
3.6.2	DSS and DSA	54
3.7	Security Goal: Integrity and Authenticity	55
3.8	Security Goal: Confidentiality and Integrity	56
	Related Work	57
	Problems	58
	References	59
4	Cryptographic Protocols	63
4.1	Passwords	63
4.1.1	Username/Password Protocol	63
4.1.2	Dictionary Attacks	65
4.1.3	Rainbow Tables	66
4.2	Authentication Protocols	67
4.2.1	One-Time-Password-Protocol (OTP)	68
4.2.2	Challenge-and-Response Protocol	69
4.2.3	Certificate/Verify Protocol	70
4.2.4	Mutual Authentication	71
4.3	Key Agreement	71
4.3.1	Public Key based Key Agreement	71
4.3.2	Symmetric Key Agreement	72
4.4	Authenticated Key Agreement	73
4.5	Attacks and security models	73
4.5.1	Protocol Security Models	74
4.5.2	Generic Attacks on Protocols	75
4.6	Certificates	76

4.6.1	X.509 Certificates	76
4.6.2	Public Key Infrastructure (PKI)	78
4.6.3	Validity of Certificates	79
4.6.4	Attacks on Certificates	80
	Related Work	81
	Problems	81
	References	82
5	Point-to-Point Security	85
5.1	Point-to-Point Protocol	86
5.1.1	PPP Authentication	86
5.1.2	PPP Extensions	87
5.2	Authentication, Authorization and Accounting (AAA)	87
5.3	Point-to-Point Tunneling Protocol (PPTP)	88
5.4	The PPTP attack by Schneier and Mudge	88
5.4.1	Attack on Hashed PAP	89
5.4.2	Attack on MS-CHAP	90
5.5	PPTPv2	92
5.6	EAP Protocols	94
	Related Work	95
	Problems	95
	References	95
6	Wireless LAN (WLAN)	99
6.1	Local Area Network (LAN)	100
6.1.1	Ethernet and other LAN Technologies	100
6.1.2	LAN specific Attacks	100
6.1.3	Non-Cryptographic Security Mechanisms	101
6.2	Wireless LAN	101
6.3	Wired Equivalent Privacy (WEP)	102
6.3.1	WEP Frame Encryption	102
6.3.2	RC4	103
6.3.3	Security Problems of WEP	104
6.3.4	The Attack of Fluhrer, Mantin, and Shamir	105
6.4	Wi-Fi Protected Access (WPA)	108
6.5	IEEE 802.1X	111
6.6	Enterprise WPA/IEEE 802.11i with EAP	111
6.7	Key Reinstallation Attack (KRACK) against WPA2	113
6.8	WPA3	114
	Related Work	115
	Problems	116
	References	117

7	Cellular Networks	121
7.1	Short History	121
7.2	Architecture of Cellular Networks	122
7.3	GSM	123
7.4	UMTS and LTE	127
7.5	Integration with the Internet: EAP	130
	Related Work	130
	Problems	131
	References	131
8	IP Security (IPsec)	135
8.1	Internet Protocol (IP)	136
8.1.1	IP packets	136
8.1.2	IP Address	137
8.1.3	Routing	139
8.1.4	Round-Trip Time (RTT)	140
8.1.5	Private IP Addresses and Network Address Translation (NAT)	141
8.1.6	Virtual Private Network (VPN)	142
8.2	Early Approach: Simple Key Management for Internet Protocols (SKIP)	143
8.3	IPsec: Overview	144
8.3.1	SPI and SA	144
8.3.2	Software Modules	145
8.3.3	Sending an encrypted IP packet	146
8.4	IPsec Data Formats	147
8.4.1	Transport and Tunnel Mode	148
8.4.2	Authentication Header (AH)	149
8.4.3	Encapsulating Security Payload (ESP)	151
8.4.4	ESP and AH in IPv6	152
8.5	IPsec Key Management: Development	152
8.5.1	Station-to-Station Protocol	152
8.5.2	Photuris	153
8.5.3	SKEME	155
8.5.4	OAKLEY	156
8.6	Internet Key Exchange Version 1 (IKEv1)	160
8.6.1	Phases in IKEv1	161
8.6.2	Data Structure: ISAKMP	163
8.6.3	Phase 1 Main Mode	164
8.6.4	Phase 1 Aggressive Mode	167
8.6.5	Phase 2	168
8.7	IKEv2	169
8.7.1	Phases in IKEv2	170
8.7.2	Phase 1	170
8.7.3	Negotiation of further IPsec SAs/Child SAs	174

8.8	NAT Traversal	175
8.9	Attacks on IPsec	176
8.9.1	Attacks on Encryption-Only Modes in ESP	176
8.9.2	Dictionary attacks on PSK modes	176
8.9.3	Bleichenbacher attack on IKEv1 and IKEv2	179
8.10	Alternatives to IPsec	183
8.10.1	OpenVPN	183
8.10.2	New developments	185
	Related Work	185
	Problems	185
	References	187
9	Security of HTTP	191
9.1	TCP and UDP	191
9.1.1	User Datagram Protocol (UDP)	192
9.1.2	Transmission Control Protocol (TCP)	192
9.1.3	UDP and TCP Proxies	194
9.2	Hypertext Transfer Protocol (HTTP)	194
9.3	HTTP Security Mechanisms	195
9.3.1	Basic Authentication for HTTP	196
9.3.2	Digest Access Authentication for HTTP	196
9.3.3	HTML forms with password input	197
9.4	HTTP/2	198
	Related Work	198
	Problems	199
	References	199
10	Transport Layer Security	201
10.1	TLS-Ecosystem	202
10.1.1	Versions	202
10.1.2	Architecture	202
10.1.3	Activation of TLS	204
10.1.4	Other Handshake Components	205
10.2	TLS Record Protocol	205
10.2.1	TLS Record Layer	205
10.3	TLS Handshake Protocol: Overview	208
10.4	TLS Ciphersuites	211
10.5	TLS Handshake: Detailed Walkthrough	215
10.5.1	Negotiation: ClientHello and ServerHello	215
10.5.2	Key Exchange: Certificate and ClientKeyExchange.	216
10.5.3	Key Generation	218
10.5.4	Synchronization: ChangeCipherSpec and Finished	220
10.5.5	Optional authentication of the client: CertificateRequest, Certificate and CertificateVerify	221
10.5.6	TLS-DHE Handshake in Detail	221

10.5.7	TLS-RSA Handshake in Detail	223
10.6	Alert and ChangeCipherSec	224
10.7	TLS Session Resumption	225
10.8	TLS Renegotiation	227
10.9	TLS Extensions	228
10.10	HTTP Headers Affecting TLS	230
10.11	Datagram TLS (DTLS)	231
10.11.1	Problems with TLS over UDP	231
10.11.2	Adjustments made in DTLS	232
	Related Work	233
	Problems	236
	References	238
11	A Short History of TLS	243
11.1	First Attempts: SSL 2.0 and PCT	243
11.1.1	SSL 2.0: Records	243
11.1.2	SSL 2.0: Handshake	244
11.1.3	SSL 2.0: Key Derivation	244
11.1.4	SSL 2.0: Problems	244
11.1.5	Private Communication Technology	246
11.2	SSL 3.0	247
11.2.1	Record Layer	248
11.2.2	Handshake	248
11.2.3	Key Derivation	249
11.2.4	FORTEZZA: Skipjack and KEA	249
11.3	TLS 1.0	250
11.3.1	Use of HMAC	250
11.3.2	Record Layer	250
11.3.3	The PRF function of TLS 1.0 and 1.1	251
11.4	TLS 1.1	251
11.5	TLS 1.3	252
11.5.1	TLS-1.3 Ecosystem	252
11.5.2	Record Layer	253
11.5.3	Regular Handshake: Description	254
11.5.4	TLS 1.3: Key Derivation	256
11.5.5	PSK Handshake and 0-RTT Mode	258
11.6	Important implementations	259
11.7	Conclusion	259
	Related Work	260
	Problems	261
	References	262

12	Attacks on SSL and TLS	267
12.1	Overview	267
12.2	Attacker Models	268
12.2.1	Web Attacker Model	269
12.2.2	Man-in-the-Middle Attack	270
12.3	Record Layer: First Attacks	271
12.3.1	Dictionary of Ciphertext Lengths	271
12.3.2	BEAST	271
12.4	Record Layer: Padding-Oracle Attacks	274
12.4.1	Padding Oracle Attack by Serge Vaudenay	274
12.4.2	Padding Oracles in TLS	278
12.4.3	A First Attack on TLS	279
12.4.4	Padding-Oracle attack on DTLS	280
12.4.5	Lucky 13	281
12.4.6	POODLE	284
12.5	Record Layer: Compression-based Attacks	287
12.5.1	Data Compression in HTTPS	288
12.5.2	CRIME	289
12.5.3	BREACH	290
12.5.4	TIME and HEIST	292
12.6	Attacks on the TLS Handshake	293
12.6.1	Attacks on SSL 2.0	293
12.6.2	Version Rollback Attack on SSL 3.0	294
12.6.3	Bleichenbacher Attack	294
12.6.4	Variants of the Bleichenbacher attack	299
12.6.5	Signature Forgery with Bleichenbacher	300
12.6.6	ROBOT	300
12.6.7	Synchronization Attack on TLS-RSA	301
12.6.8	Triple Handshake Attack	301
12.6.9	Raccoon	303
12.7	Private Key Attacks	307
12.7.1	Timing-based Attacks	307
12.7.2	Heartbleed	307
12.7.3	Small Subgroup Attacks	308
12.8	Cross-Protocol Attacks	310
12.8.1	Cross-Cipher Suite Attacks for TLS	310
12.8.2	TLS and QUIC	311
12.8.3	TLS 1.2 and TLS 1.3	312
12.8.4	TLS and IPsec	313
12.8.5	DROWN	313
12.8.6	ALPACA	316
12.9	Attacks on the Graphical User Interface	317
12.9.1	The PKI for TLS	317
12.9.2	Phishing, Pharming and Visual Spoofing	317
12.9.3	Warnings	317

12.9.4	SSLStrip	318
	Related Work	319
	Problems	321
	References	323
13	Secure Shell (SSH)	329
13.1	Introduction	329
13.1.1	What is a “Shell”?	329
13.1.2	SSH Key Management	331
13.1.3	Short history of SSH	331
13.2	SSH-1	332
13.3	SSH 2.0	334
13.3.1	Handshake	334
13.3.2	Binary Packet Protocol	335
13.4	Attacks on SSH	336
13.4.1	Attack by Albrecht, Paterson, and Watson	336
	Related Work	337
	Problems	338
	References	338
14	Kerberos	341
14.1	Symmetric Crypto: Key Management	341
14.2	The Needham-Schroeder Protocol	343
14.3	Kerberos Protocol	344
14.4	Security of Kerberos v5	347
14.5	Kerberos v5 and Microsoft’s Active Directory	347
	Related Work	348
	Problems	348
	References	349
15	DNS Security	353
15.1	Domain Name System (DNS)	353
15.1.1	Short History of DNS	354
15.1.2	Domain Names and DNS Hierarchy	354
15.1.3	Resource Records	356
15.1.4	Resolution of Domain Names	358
15.1.5	DNS Query and DNS Response	359
15.2	Attacks on the DNS	361
15.2.1	DNS Spoofing	361
15.2.2	DNS Cache Poisoning	361
15.2.3	Name Chaining and In-Bailiwick-RRs	364
15.2.4	Kaminski attack	364
15.3	DNSSEC	366
15.3.1	New RR Data Types	368
15.3.2	Secure Name Resolution with DNSSEC	370

15.4	Securing DNS	370
15.4.1	DNSSEC Deployment	370
15.4.2	Alternatives for DNS	371
	Related Work	372
	Problems	372
	References	373
16	File Encryption: PGP	377
16.1	PGP - The Legend	377
16.1.1	The Beginnings	378
16.1.2	The Prosecution	378
16.1.3	PGP 2.62 and PGP International	379
16.1.4	IETF standard	379
16.2	The PGP Ecosystem	380
16.2.1	Key Management in PGP	380
16.2.2	Encryption	383
16.2.3	Digital Signatures	383
16.3	Open PGP	383
16.3.1	OpenPGP packets	383
16.3.2	Encryption and Signature of a Test Message	385
16.3.3	OpenPGP Packets	387
16.3.4	Radix 64 Conversion	388
16.4	Attacks on PGP	388
16.4.1	Additional Decryption Keys	388
16.4.2	Manipulation of the private key	390
16.5	PGP: Implementations	393
16.5.1	Crypto Libraries with OpenPGP Support	394
16.5.2	OpenPGP GUIs for Different Operating Systems	395
16.5.3	Package Managers with OpenPGP Signatures	395
16.5.4	Software Downloads	396
	Related Work	396
	Problems	397
	References	397
17	Email Security: S/MIME	401
17.1	E-Mail according to RFC 822	401
17.2	Privacy Enhanced Mail (PEM)	404
17.3	Multipurpose Internet Mail Extensions (MIME)	406
17.4	ASN.1, PKCS#7 and CMS	409
17.4.1	Platform independence: ASN.1	409
17.4.2	Public Key Cryptography Standards (PKCS)	410
17.4.3	PKCS#7 and Cryptographic Message Syntax (CMS)	412
17.5	S/MIME	414
17.6	S/MIME: Encryption	416
17.7	S/MIME: Signature	420

17.7.1 Key Management	423
17.8 PGP/MIME	424
Related Work	424
Problems	425
References	426
18 Attacks on S/MIME and OpenPGP	431
18.1 EFAIL 1: Encryption	431
18.1.1 Attacker Model	432
18.1.2 Backchannels	433
18.1.3 Crypto Gadgets	434
18.1.4 Direct Exfiltration	437
18.2 EFAIL 2: Digital Signatures	438
18.2.1 Attacker Model	439
18.2.2 GUI Spoofing	439
18.2.3 FROM Spoofing	440
18.2.4 MIME Wrapping	441
18.2.5 CMS Wrapping	442
18.3 EFAIL 3: Reply Attacks	442
Related Work	443
Problems	444
References	445
19 Email: Protocols and SPAM	447
19.1 POP3 and IMAP	447
19.1.1 POP3	447
19.1.2 IMAP	449
19.2 SMTP-over-TLS	450
19.3 SPAM and SPAM filters	451
19.4 E-Mail Sender	453
19.5 Domain Key Identified Mail (DKIM)	454
19.6 Sender Policy Framework (SPF)	458
19.7 DMARC	460
Related Work	462
Problems	462
References	464
20 Web Security and Single Sign-On Protocols	467
20.1 Web Applications	468
20.1.1 Architecture of Web Applications	468
20.1.2 Hypertext Markup Language (HTML)	469
20.1.3 Uniform Resource Locators (URLs) and Uniform Resource Identifiers (URIs)	470
20.1.4 JavaScript and the Document Object Model (DOM)	470
20.1.5 Same Origin Policy (SOP)	471

20.1.6	Cascading Style Sheets	473
20.1.7	AJAX	474
20.1.8	HTTP Cookies	474
20.1.9	HTTP Redirect and Query Strings	475
20.1.10	HTML Forms	476
20.2	Web Application Security	477
20.2.1	Cross-Site Scripting (XSS)	477
20.2.2	Cross-Site Request Forgery (CSRF)	482
20.2.3	SQL Injection (SQLi)	484
20.2.4	UI Redressing	485
20.3	Single Sign-On Protocols	486
20.3.1	Microsoft Passport	488
20.3.2	Security Assertion Markup Language (SAML)	490
20.3.3	OpenID	492
20.3.4	OAuth	493
20.3.5	OpenID Connect	495
	Related Work	496
	Problems	497
	References	498
21	Cryptographic Data Formats	505
21.1	TLV Encoding and Chracter-Based Encoding	505
21.2	eXtensible Markup Language (XML)	506
21.2.1	XML Namespaces	507
21.2.2	DTD and XML Schema	507
21.2.3	XPath	509
21.2.4	XSLT	510
21.2.5	XML Signature	511
21.2.6	XML Encryption	513
21.2.7	XML Security	515
21.3	JavaScript Object Notation (JSON)	516
21.3.1	Syntax	516
21.3.2	JSON Web Signature	517
21.3.3	JSON Web Encryption	518
21.3.4	Security of JSON Signing and Encryption	519
	Related Work	519
	Problems	519
	References	521
	Index	525