Advanced API Security

OAuth 2.0 and Beyond

—

Second Edition

—

Prabath Siriwardena

Apress®

Advanced API Security

OAuth 2.0 and Beyond

Second Edition

Prabath Siriwardena

Apress®

Advanced API Security: OAuth 2.0 and Beyond

Prabath Siriwardena
San Jose, CA, USA

ISBN-13 (pbk): 978-1-4842-2049-8 ISBN-13 (electronic): 978-1-4842-2050-4
https://doi.org/10.1007/978-1-4842-2050-4

Copyright © 2020 by Prabath Siriwardena

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.

Trademarked names, logos, and images may appear in this book. Rather than use a trademark symbol with every occurrence of a trademarked name, logo, or image we use the names, logos, and images only in an editorial fashion and to the benefit of the trademark owner, with no intention of infringement of the trademark.

The use in this publication of trade names, trademarks, service marks, and similar terms, even if they are not identified as such, is not to be taken as an expression of opinion as to whether or not they are subject to proprietary rights.

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.

Managing Director, Apress Media LLC: Welmoed Spahr
Acquisitions Editor: Jonathan Gennick
Development Editor: Laura Berendson
Coordinating Editor: Jill Balzano

Cover image designed by Freepik (www.freepik.com)

Distributed to the book trade worldwide by Springer Science+Business Media New York, 233 Spring Street, 6th Floor, New York, NY 10013. Phone 1-800-SPRINGER, fax (201) 348-4505, e-mail orders-ny@springer-sbm.com, or visit www.springeronline.com. Apress Media, LLC is a California LLC and the sole member (owner) is Springer Science + Business Media Finance Inc (SSBM Finance Inc). SSBM Finance Inc is a **Delaware** corporation.

For information on translations, please e-mail rights@apress.com, or visit http://www.apress.com/rights-permissions.

Apress titles may be purchased in bulk for academic, corporate, or promotional use. eBook versions and licenses are also available for most titles. For more information, reference our Print and eBook Bulk Sales web page at http://www.apress.com/bulk-sales.

Any source code or other supplementary material referenced by the author in this book is available to readers on GitHub via the book's product page, located at www.apress.com/9781484220498. For more detailed information, please visit http://www.apress.com/source-code.

Printed on acid-free paper

This book is dedicated to my sister Deepani,
who backed me all the time!

Table of Contents

About the Author xv

Acknowledgments xvii

Introduction xix

Chapter 1: APIs Rule! 1

API Economy 1

Amazon 3

Salesforce 5

Uber 5

Facebook 6

Netflix 7

Walgreens 8

Governments 9

IBM Watson 9

Open Banking 10

Healthcare 10

Wearables 11

Business Models 12

The API Evolution 13

API Management 20

The Role of APIs in Microservices 25

Summary 32

Chapter 2: Designing Security for APIs 33

Trinity of Trouble 34

Design Challenges 37

User Experience 38
Performance 39
Weakest Link 40
Defense in Depth 41
Insider Attacks 42
Security by Obscurity 44
Design Principles 45
Least Privilege 45
Fail-Safe Defaults 46
Economy of Mechanism 48
Complete Mediation 49
Open Design 49
Separation of Privilege 51
Least Common Mechanism 52
Psychological Acceptability 53
Security Triad 54
Confidentiality 54
Integrity 56
Availability 57
Security Control 59
Authentication 59
Authorization 62
Nonrepudiation 64
Auditing 65
Summary 65

Chapter 3: Securing APIs with Transport Layer Security (TLS) 69

Setting Up the Environment 69
Deploying Order API 71
Securing Order API with Transport Layer Security (TLS) 74
Protecting Order API with Mutual TLS 76

Running OpenSSL on Docker 78
Summary 79

Chapter 4: OAuth 2.0 Fundamentals 81

Understanding OAuth 2.0 81
OAuth 2.0 Actors 83
Grant Types 84
Authorization Code Grant Type 85
Implicit Grant Type 88
Resource Owner Password Credentials Grant Type 90
Client Credentials Grant Type 91
Refresh Grant Type 92
How to Pick the Right Grant Type? 93
OAuth 2.0 Token Types 94
OAuth 2.0 Bearer Token Profile 94
OAuth 2.0 Client Types 96
JWT Secured Authorization Request (JAR) 97
Pushed Authorization Requests (PAR) 99
Summary 101

Chapter 5: Edge Security with an API Gateway 103

Setting Up Zuul API Gateway 103
Running the Order API 104
Running the Zuul API Gateway 105
What Happens Underneath? 107
Enabling TLS for the Zuul API Gateway 107
Enforcing OAuth 2.0 Token Validation at the Zuul API Gateway 109
Setting Up an OAuth 2.0 Security Token Service (STS) 110
Testing OAuth 2.0 Security Token Service (STS) 112
Setting Up Zuul API Gateway for OAuth 2.0 Token Validation 114
Enabling Mutual TLS Between Zuul API Gateway and Order Service 117
Securing Order API with Self-Contained Access Tokens 121

Setting Up an Authorization Server to Issue JWT 121
Protecting Zuul API Gateway with JWT 124
The Role of a Web Application Firewall (WAF) 125
Summary 126

Chapter 6: OpenID Connect (OIDC) 129
From OpenID to OIDC 129
Amazon Still Uses OpenID 2.0 132
Understanding OpenID Connect 133
Anatomy of the ID Token 134
OpenID Connect Request 139
Requesting User Attributes 142
OpenID Connect Flows 144
Requesting Custom User Attributes 145
OpenID Connect Discovery 146
OpenID Connect Identity Provider Metadata 149
Dynamic Client Registration 151
OpenID Connect for Securing APIs 153
Summary 155

Chapter 7: Message-Level Security with JSON Web Signature 157
Understanding JSON Web Token (JWT) 157
JOSE Header 158
JWT Claims Set 160
JWT Signature 163
JSON Web Signature (JWS) 167
JWS Compact Serialization 167
The Process of Signing (Compact Serialization) 172
JWS JSON Serialization 174
The Process of Signing (JSON Serialization) 176
Summary 184

Chapter 8: Message-Level Security with JSON Web Encryption 185

JWE Compact Serialization 185

JOSE Header 186

JWE Encrypted Key 191

JWE Initialization Vector 194

JWE Ciphertext 194

JWE Authentication Tag 194

The Process of Encryption (Compact Serialization) 195

JWE JSON Serialization 196

JWE Protected Header 197

JWE Shared Unprotected Header 197

JWE Per-Recipient Unprotected Header 198

JWE Initialization Vector 198

JWE Ciphertext 198

JWE Authentication Tag 199

The Process of Encryption (JSON Serialization) 199

Nested JWTs 201

Summary 210

Chapter 9: OAuth 2.0 Profiles 211

Token Introspection 211

Chain Grant Type 215

Token Exchange 217

Dynamic Client Registration Profile 220

Token Revocation Profile 225

Summary 226

Chapter 10: Accessing APIs via Native Mobile Apps 227

Mobile Single Sign-On (SSO) 227

Login with Direct Credentials 228

Login with WebView 229

Login with a System Browser 230

Using OAuth 2.0 in Native Mobile Apps 231
Inter-app Communication 233
Proof Key for Code Exchange (PKCE) 235
Browser-less Apps 237
OAuth 2.0 Device Authorization Grant 237
Summary 241

Chapter 11: OAuth 2.0 Token Binding 243

Understanding Token Binding 244
Token Binding Negotiation 244
TLS Extension for Token Binding Protocol Negotiation 246
Key Generation 247
Proof of Possession 247
Token Binding for OAuth 2.0 Refresh Token 249
Token Binding for OAuth 2.0 Authorization Code/Access Token 251
TLS Termination 254
Summary 255

Chapter 12: Federating Access to APIs 257

Enabling Federation 257
Brokered Authentication 258
Security Assertion Markup Language (SAML) 261
SAML 2.0 Client Authentication 261
SAML Grant Type for OAuth 2.0 264
JWT Grant Type for OAuth 2.0 267
Applications of JWT Grant Type 269
JWT Client Authentication 270
Applications of JWT Client Authentication 271
Parsing and Validating JWT 274
Summary 276