Advanced API Security

Securing APIs with OAuth 2.0, OpenID Connect, JWS, and JWE

Prabath Siriwardena
This book is dedicated to two great ladies: my mother and my wife.
Contents at a Glance

About the Author .................................................................................................................. xiii
About the Technical Reviewer ............................................................................................. xv
Acknowledgments ................................................................................................................ xvii
Introduction ........................................................................................................................... xix

■ Chapter 1: Managed APIs ............................................................................................... 1
■ Chapter 2: Security by Design ....................................................................................... 11
■ Chapter 3: HTTP Basic/Digest Authentication ............................................................. 33
■ Chapter 4: Mutual Authentication with TLS ................................................................. 47
■ Chapter 5: Identity Delegation ....................................................................................... 59
■ Chapter 6: OAuth 1.0 ...................................................................................................... 75
■ Chapter 7: OAuth 2.0 ...................................................................................................... 91
■ Chapter 8: OAuth 2.0 MAC Token Profile .................................................................. 133
■ Chapter 9: OAuth 2.0 Profiles ...................................................................................... 143
■ Chapter 10: User Managed Access (UMA) ................................................................. 155
■ Chapter 11: Federation ................................................................................................... 171
■ Chapter 12: OpenID Connect ....................................................................................... 181
■ Chapter 13: JWT, JWS, and JWE ................................................................................ 201
■ Chapter 14: Patterns and Practices ............................................................................. 221

Index ................................................................................................................................... 231
Contents

About the Author .......................................................................................................................... xiii
About the Technical Reviewer ..................................................................................................... xv
Acknowledgments ....................................................................................................................... xvii
Introduction .................................................................................................................................. xix

■ Chapter 1: Managed APIs ......................................................................................................... 1
  The API Evolution ....................................................................................................................... 1
  API vs. Managed API .................................................................................................................. 3
  API vs. Service ............................................................................................................................ 4
  Discovering and Describing APIs ............................................................................................. 5
  Managed APIs in Practice ........................................................................................................... 6
    Twitter API ................................................................................................................................ 6
    Salesforce API .......................................................................................................................... 8
  Summary ..................................................................................................................................... 10

■ Chapter 2: Security by Design .................................................................................................... 11
  Design Challenges ....................................................................................................................... 11
    User Comfort ............................................................................................................................ 11
  Design Principles ....................................................................................................................... 13
    Least Privilege ......................................................................................................................... 13
    Fail-Safe Defaults .................................................................................................................... 13
    Economy of Mechanism .......................................................................................................... 13
    Complete Mediation ............................................................................................................... 14
    Open Design ........................................................................................................................... 14
    Separation of Privilege ............................................................................................................ 14
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Least Common Mechanism</td>
<td>14</td>
</tr>
<tr>
<td>Psychological Acceptability</td>
<td>14</td>
</tr>
<tr>
<td><strong>Confidentiality, Integrity, Availability (CIA)</strong></td>
<td>14</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>14</td>
</tr>
<tr>
<td>Integrity</td>
<td>16</td>
</tr>
<tr>
<td>Availability</td>
<td>16</td>
</tr>
<tr>
<td>Security Controls</td>
<td>17</td>
</tr>
<tr>
<td>Authentication</td>
<td>18</td>
</tr>
<tr>
<td>Authorization</td>
<td>19</td>
</tr>
<tr>
<td>Nonrepudiation</td>
<td>21</td>
</tr>
<tr>
<td>Auditing</td>
<td>21</td>
</tr>
<tr>
<td>Security Patterns</td>
<td>22</td>
</tr>
<tr>
<td>Direct Authentication Pattern</td>
<td>22</td>
</tr>
<tr>
<td>Sealed Green Zone Pattern</td>
<td>25</td>
</tr>
<tr>
<td>Least Common Mechanism Pattern</td>
<td>26</td>
</tr>
<tr>
<td>Brokered Authentication Pattern</td>
<td>26</td>
</tr>
<tr>
<td>Policy-Based Access Control Pattern</td>
<td>27</td>
</tr>
<tr>
<td>Threat Modeling</td>
<td>29</td>
</tr>
<tr>
<td>Summary</td>
<td>31</td>
</tr>
<tr>
<td><strong>Chapter 3: HTTP Basic/Digest Authentication</strong></td>
<td>33</td>
</tr>
<tr>
<td>HTTP Basic Authentication</td>
<td>33</td>
</tr>
<tr>
<td>HTTP Digest Authentication</td>
<td>34</td>
</tr>
<tr>
<td>Summary</td>
<td>46</td>
</tr>
<tr>
<td><strong>Chapter 4: Mutual Authentication with TLS</strong></td>
<td>47</td>
</tr>
<tr>
<td>Evolution of TLS</td>
<td>47</td>
</tr>
<tr>
<td>How TLS Works</td>
<td>48</td>
</tr>
<tr>
<td>TLS Handshake</td>
<td>48</td>
</tr>
<tr>
<td>Application Data Transfer</td>
<td>51</td>
</tr>
<tr>
<td>Summary</td>
<td>58</td>
</tr>
</tbody>
</table>
Chapter 5: Identity Delegation

Direct Delegation vs. Brokered Delegation

Evolution of Identity Delegation

Google ClientLogin

Google AuthSub

Flickr Authentication API

Yahoo! Browser-Based Authentication (BBAuth)

Summary

Chapter 6: OAuth 1.0

The Token Dance

Temporary-Credential Request Phase

Resource-Owner Authorization Phase

Token-Credential Request Phase

Invoking a Secured Business API with OAuth 1.0

Demystifying oauth_signature

Three-Legged OAuth vs. Two-Legged OAuth

OAuth WRAP

Summary

Chapter 7: OAuth 2.0

OAuth WRAP

Client Account and Password Profile

Assertion Profile

Username and Password Profile

Web App Profile

Rich App Profile

Accessing a WRAP-Protected API

WRAP to OAuth 2.0

OAuth 2.0 Grant Types

Authorization Code Grant Type

Implicit Grant Type
Resource Owner Password Credentials Grant Type ................................................................. 100
Client Credentials Grant Type ................................................................................................. 101
OAuth 2.0 Token Types ........................................................................................................... 102
OAuth 2.0 Bearer Token Profile .............................................................................................. 102
OAuth 2.0 Client Types ........................................................................................................... 103
OAuth 2.0 and Facebook ......................................................................................................... 109
OAuth 2.0 and LinkedIn .......................................................................................................... 116
OAuth 2.0 and Salesforce ........................................................................................................ 119
OAuth 2.0 and Google ............................................................................................................ 124
Authentication vs. Authorization ............................................................................................. 131
Summary ................................................................................................................................. 132

Chapter 8: OAuth 2.0 MAC Token Profile ............................................................................. 133
Bearer Token vs. MAC Token .................................................................................................. 134
Obtaining a MAC Token .......................................................................................................... 135
Invoking an API Protected with the OAuth 2.0 MAC Token Profile ...................................... 138
Calculating the MAC ............................................................................................................... 138
MAC Validation by the Resource Server .................................................................................. 140
OAuth Grant Types and the MAC Token Profile ................................................................. 141
OAuth 1.0 vs. OAuth 2.0 MAC Token Profile ......................................................................... 141
Summary ................................................................................................................................. 142

Chapter 9: OAuth 2.0 Profiles .................................................................................................. 143
Token Introspection Profile ...................................................................................................... 143
  XACML and OAuth Token Introspection ............................................................................... 146
Chain Grant Type Profile ........................................................................................................ 149
Dynamic Client Registration Profile ...................................................................................... 150
Token Revocation Profile ....................................................................................................... 152
Summary ................................................................................................................................. 153
## Chapter 10: User Managed Access (UMA)

- **ProtectServe** ................................................................. 155
- **UMA and OAuth** .......................................................... 160
- **UMA Architecture** .......................................................... 161
- **UMA Phases** ................................................................. 161
  - UMA Phase 1: Protecting a Resource ................................. 161
  - UMA Phase 2: Getting Authorization .................................. 164
  - UMA Phase 3: Accessing the Protected Resource ................. 168
- **UMA APIs** ............................................................... 168
  - Protection API ............................................................. 169
  - Authorization API ....................................................... 170
- **The Role of UMA in API Security** ................................ 170
- **Summary** ................................................................. 170

## Chapter 11: Federation

- **Enabling Federation** ...................................................... 171
- **Brokered Authentication** ............................................... 171
- **SAML 2.0 Profile for OAuth: Client Authentication** .......... 173
- **SAML 2.0 Profile for OAuth: Grant Type** ......................... 176
- **JWT Profile for OAuth 2.0 Client Authentication and Authorization Grants** .................. 180
- **Summary** ................................................................. 180

## Chapter 12: OpenID Connect

- **A Brief History of OpenID Connect** ............................... 181
- **Understanding OpenID Connect** .................................. 184
  - Anatomy of the ID Token ............................................... 184
  - OpenID Connect Request .............................................. 187
  - Requesting User Attributes .......................................... 189
  - Grant Types for OpenID Connect .................................... 191
  - Requesting Custom User Attributes ................................ 191
  - OpenID Connect Discovery .......................................... 194
<table>
<thead>
<tr>
<th>Chapter 13: JWT, JWS, and JWE</th>
<th>201</th>
</tr>
</thead>
<tbody>
<tr>
<td>JSON Web Token</td>
<td>201</td>
</tr>
<tr>
<td>JOSE Working Group</td>
<td>205</td>
</tr>
<tr>
<td>JSON Web Signature</td>
<td>206</td>
</tr>
<tr>
<td>Signature Algorithms</td>
<td>207</td>
</tr>
<tr>
<td>Serialization</td>
<td>208</td>
</tr>
<tr>
<td>JSON Web Encryption</td>
<td>213</td>
</tr>
<tr>
<td>Content Encryption vs. Key Wrapping</td>
<td>215</td>
</tr>
<tr>
<td>Serialization</td>
<td>215</td>
</tr>
<tr>
<td>Summary</td>
<td>220</td>
</tr>
<tr>
<td>Chapter 14: Patterns and Practices</td>
<td>221</td>
</tr>
<tr>
<td>Direct Authentication with the Trusted Subsystem Pattern</td>
<td>221</td>
</tr>
<tr>
<td>Single Sign-On with the Delegated Access Control Pattern</td>
<td>222</td>
</tr>
<tr>
<td>Single Sign-On with the Integrated Windows Authentication Pattern</td>
<td>223</td>
</tr>
<tr>
<td>Identity Proxy with the Delegated Access Control Pattern</td>
<td>223</td>
</tr>
<tr>
<td>Delegated Access Control with the JSON Web Token Pattern</td>
<td>224</td>
</tr>
<tr>
<td>Nonrepudiation with the JSON Web Signature Pattern</td>
<td>225</td>
</tr>
<tr>
<td>Chained Access Delegation Pattern</td>
<td>226</td>
</tr>
<tr>
<td>Trusted Master Access Delegation Pattern</td>
<td>227</td>
</tr>
<tr>
<td>Resource Security Token Service (STS) with the Delegated Access Control Pattern</td>
<td>228</td>
</tr>
<tr>
<td>Delegated Access Control with the Hidden Credentials Pattern</td>
<td>229</td>
</tr>
<tr>
<td>Summary</td>
<td>230</td>
</tr>
</tbody>
</table>

Index .................................................................................................................. 231
Prabath Siriwardena is the Director of Security Architecture at WSO2 Inc., a company that produces a wide variety of open source software from data to screen. He is a member of the OASIS Identity Metasystem Interoperability (IMI) TC, OASIS eXtensible Access Control Markup Language (XACML) TC, OASIS Security Services (SAML) TC, OASIS Identity in the Cloud TC, and OASIS Cloud Authorization (CloudAuthZ) TC. Prabath is also a member of Apache Axis PMC and has spoken at numerous international conferences including OSCON, ApacheCon, WSO2Con, the European Identity Conference (EIC), IDentity Next, the API Strategy Conference, and OSDC. He has more than ten years of industry experience and has worked with many Fortune 100 companies. Advanced API Security is his second book. His first book was Enterprise Integration with WSO2 ESB (Packt Publishing, 2013).
Michael Peacock is an experienced software developer and team lead from Newcastle, UK. Michael holds a degree in software engineering from the University of Durham.

After spending a number of years running his own web agency and subsequently working directly for a number of software startups, Michael now serves as a technical consultant for a range of companies, helping with application development, software processes, and technical direction.

He is the author of Creating Development Environments with Vagrant, PHP 5 Social Networking, PHP 5 E-Commerce Development, Drupal 7 Social Networking, Selling online with Drupal e-Commerce, and Building Websites with TYPO3. Michael has been involved with other publications including Mobile Web Development, Jenkins Continuous Integration Cookbook, and Drupal for Education and E-Learning, on which he served as a technical reviewer.

Michael has presented at a number of user groups and technical conferences including the PHP UK Conference, the Dutch PHP Conference, ConFoo, PHPNE, PHPNW, and Could Connect Santa Clara.

You can follow Michael on Twitter (@michaelpeacock) or find out more about him through his web site (www.michaelpeacock.co.uk).
I would first like to thank Jonathan Hassel, senior editor at Apress, for evaluating and accepting my proposal for this book. Then, of course, I must thank Rita Fernando, coordinating editor at Apress, who was extremely patient and tolerant of me throughout the publishing process. Thank you very much Rita for your excellent support—I really appreciate it. Also, Gary Schwartz and Tiffany Taylor did an amazing job reviewing the manuscript—many thanks, Gary and Tiffany! Michael Peacock served as technical reviewer—thanks, Michael, for your quality review comments, which were extremely useful. Thilina Buddhika from Colorado State University also helped in reviewing the first two chapters of the book—many thanks, again, Thilina!

Dr. Sanjiva Weerawarana, the CEO of WSO2, and Paul Fremantle, the CTO of WSO2, are two constant mentors for me. I am truly grateful to both Dr. Sanjiva and Paul for everything they have done for me. I also must express my gratitude to Asanka Abeysinghe, the Vice President of Solutions Architecture at WSO2 and a good friend of mine—we have done designs for many Fortune 500 companies together, and those were extremely useful in writing this book. Thanks, Asanka!

Of course, my beloved wife, Pavithra, and my little daughter, Dinadi, supported me throughout this process. Pavithra wanted me to write this book even more than I wanted to write it. If I say she is the driving force behind this book, it's no exaggeration. She simply went beyond just feeding me with encouragement—she also helped immensely in reviewing the book and developing samples. She was always the first reader. Thank you very much, Pavithra.

My parents and my sister have been the driving force behind me since my birth. If not for them, I wouldn't be who I am today. I am grateful to them for everything they have done for me. Last but not least, my wife's parents—they were amazingly helpful in making sure that the only thing I had to do was to write this book, taking care of almost all the other things that I was supposed to do.

The point is that although writing a book may sound like a one-man effort, it's the entire team behind it who makes it a reality. Thank you to everyone who supported me in many different ways.
Introduction

APIs are becoming increasingly popular for exposing business functionalities to the rest of the world. According to an infographic published by Layer 7, 86.5% of organizations will have an API program in place in the next five years. Of those, 43.2% already have one. APIs are also the foundation of building communication channels in the Internet of Things (IoT). From motor vehicles to kitchen appliances, countless items are beginning to communicate with each other via APIs. Cisco estimates that as many as 50 billion devices could be connected to the Internet by 2020.

This book is about securing your most important APIs. As is the case with any software system design, people tend to ignore the security element during the API design phase. Only at deployment or at the time of integration do they start to address security.

Security should never be an afterthought—it’s an integral part of any software system design, and it should be well thought out from the design’s inception. One objective of this book is to educate you about the need for security and the available options for securing an API.

The book also guides you through the process and shares best practices for designing APIs for rock-solid security. API security has evolved a lot in the last five years. The growth of standards has been exponential. OAuth 2.0 is the most widely adopted standard. But it’s more than just a standard—it’s a framework that lets people build standards on top of it. The book explains in depth how to secure APIs, from traditional HTTP Basic Authentication to OAuth 2.0 and the standards built around it, such as OpenID Connect, User Managed Access (UMA), and many more.

JSON plays a major role in API communication. Most of the APIs developed today support only JSON, not XML. This book also focuses on JSON security. JSON Web Encryption (JWE) and JSON Web Signature (JWS) are two increasingly popular standards for securing JSON messages. The latter part of this book covers JWE and JWS in detail.

Another major objective of this book is to not just present concepts and theories, but also explain each of them with concrete examples. The book presents a comprehensive set of examples that work with APIs from Google, Twitter, Facebook, Yahoo!, Salesforce, Flickr, and GitHub.

The evolution of API security is another topic covered in the book. It’s extremely useful to understand how security protocols were designed in the past and how the drawbacks discovered in them pushed us to where we are today. The book covers some older security protocols such as Flickr Authentication, Yahoo! BBAuth, Google AuthSub, Google ClientLogin, and ProtectServe in detail.

I hope this book effectively covers this much-needed subject matter for API developers, and I hope you enjoy reading it.