Pragmatic Web Security

Security training for developers

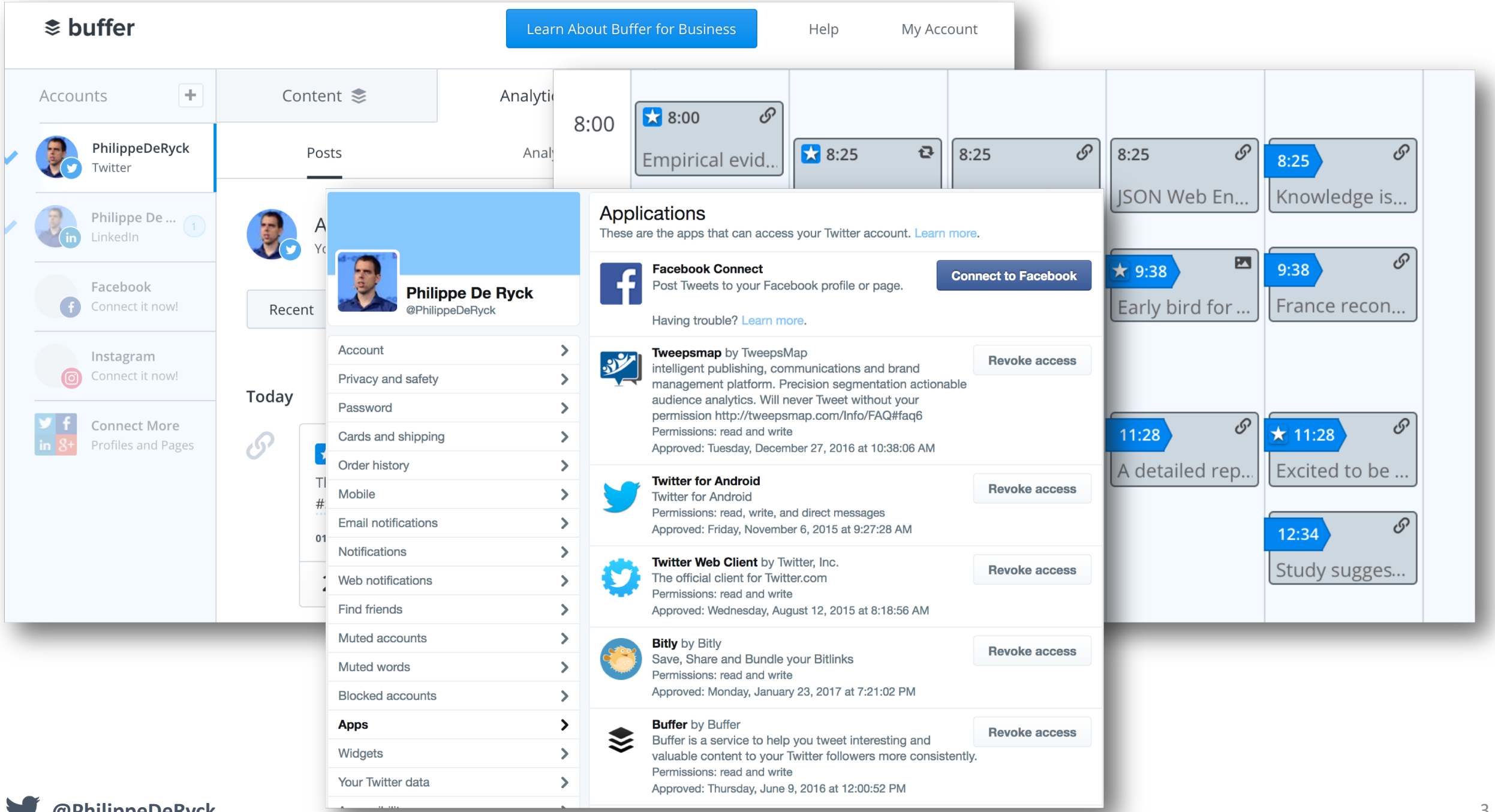
Passwords and pixie dust

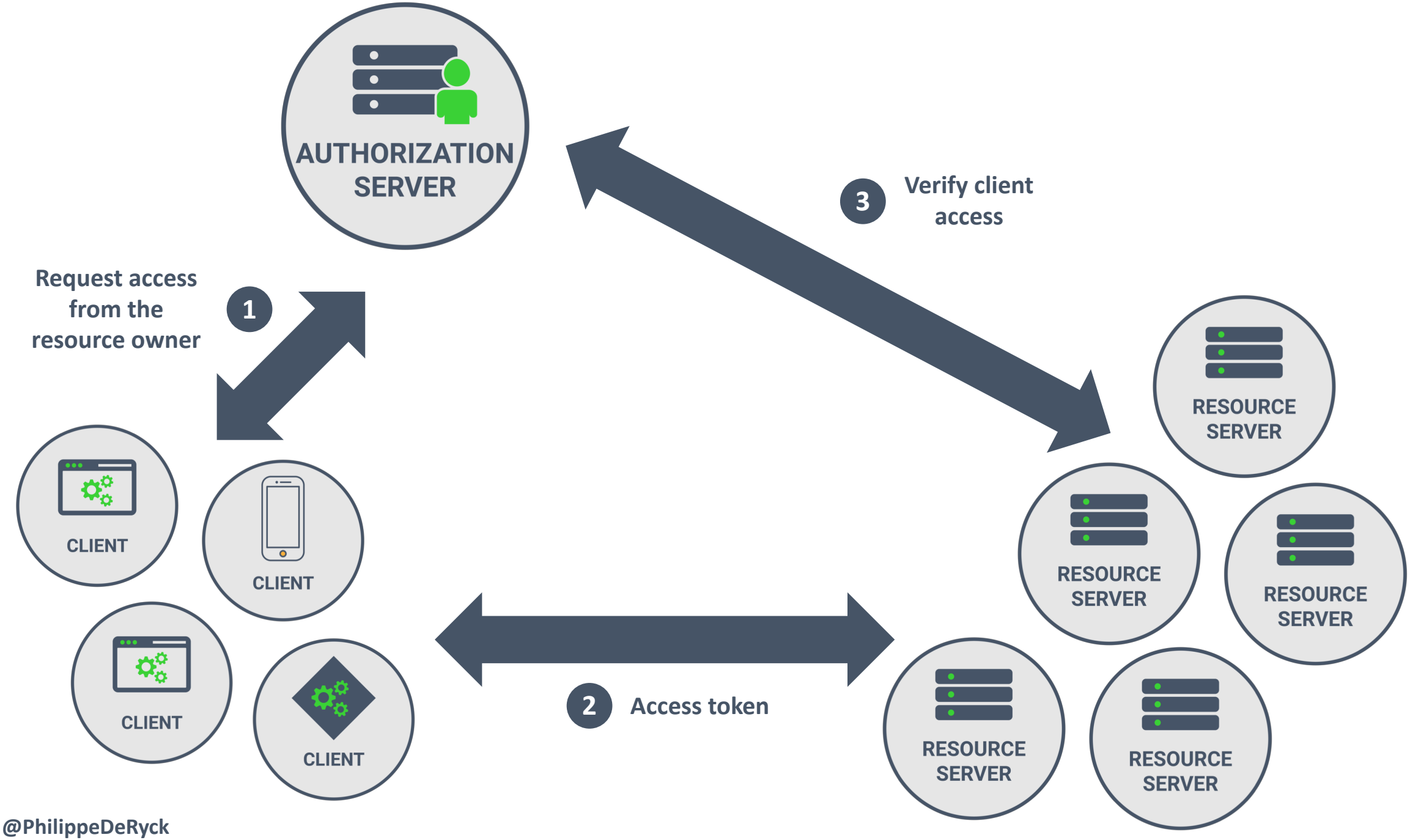
A look at OAuth 2.0 security in Angular

Philippe De Ryck

@PhilippeDeRyck – philippe@PragmaticWebSecurity.com

WHAT IS THE CORE ASPECT OF OAUTH 2.0?


buffer
Learn About Buffer for Business
Help
My Account
Accounts
Content
Posts
PhilippeDeRyck
Twitter
Philippe De ...
LinkedIn
Facebook
Connect it now!
Instagram
Connect it now!
Connect More
Profiles and Pages
Recent
Today
8:00
8:00
Empirical evid...
8:25
8:25
8:25
JSON Web En...
8:25
Knowledge is...
9:38
Early bird for ...
9:38
France recon...
11:28
A detailed rep...
11:28
Excited to be ...
12:34
Study sugges...
Philippe De Ryck
@PhilippeDeRyck
Account
Privacy and safety
Password
Cards and shipping
Order history
Mobile
Email notifications
Notifications
Web notifications
Find friends
Muted accounts
Muted words
Blocked accounts
Apps
Widgets
Your Twitter data
Applications
These are the apps that can access your Twitter account. Learn more.
Facebook Connect
Post Tweets to your Facebook profile or page.
Connect to Facebook
Having trouble? Learn more.
Tweepsmap by TweepsMap
intelligent publishing, communications and brand management platform. Precision segmentation actionable audience analytics. Will never Tweet without your permission http://tweepsmap.com/Info/FAQ#faq6
Permissions: read and write
Approved: Tuesday, December 27, 2016 at 10:38:06 AM
Revoke access
Twitter for Android
Twitter for Android
Permissions: read, write, and direct messages
Approved: Friday, November 6, 2015 at 9:27:28 AM
Revoke access
Twitter Web Client by Twitter, Inc.
The official client for Twitter.com
Permissions: read and write
Approved: Wednesday, August 12, 2015 at 8:18:56 AM
Revoke access
Bitly by Bitly
Save, Share and Bundle your Bitlinks
Permissions: read and write
Approved: Monday, January 23, 2017 at 7:21:02 PM
Revoke access
Buffer by Buffer
Buffer is a service to help you tweet interesting and valuable content to your Twitter followers more consistently.
Permissions: read and write
Approved: Thursday, June 9, 2016 at 12:00:52 PM
Revoke access


AUTHORIZATION SERVER
3
Verify client access
Request access from the resource owner
1
CLIENT
CLIENT
CLIENT
CLIENT
2
Access token
RESOURCE SERVER
RESOURCE SERVER
RESOURCE SERVER
RESOURCE SERVER
RESOURCE SERVER

- Founder of **Pragmatic Web Security**
  - In-depth web security training for developers
  - Covering web security, API security & Angular security
- 15+ years of security experience
  - Web security instructor and conference speaker
  - Author of ***Primer on client-side web security***
  - Creator of ***Web Security Fundamentals*** on edX
- Course curator of the **SecAppDev course**
  - Yearly security course targeted towards developers
  - More information on ***https://secappdev.org***
- Foodie and professional chef

Dr. Philippe De Ryck

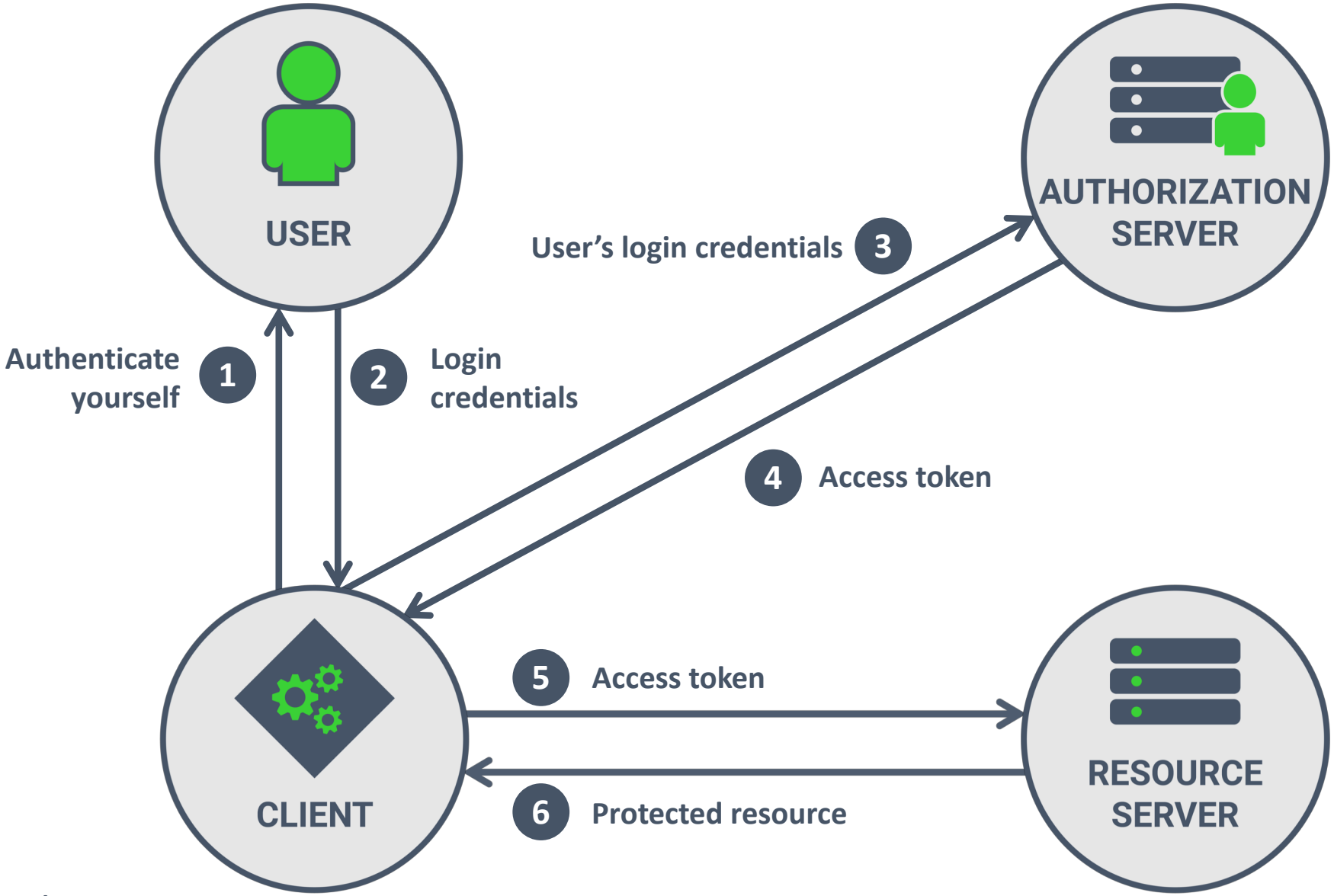
Ph.D. in web security

Google developer expert

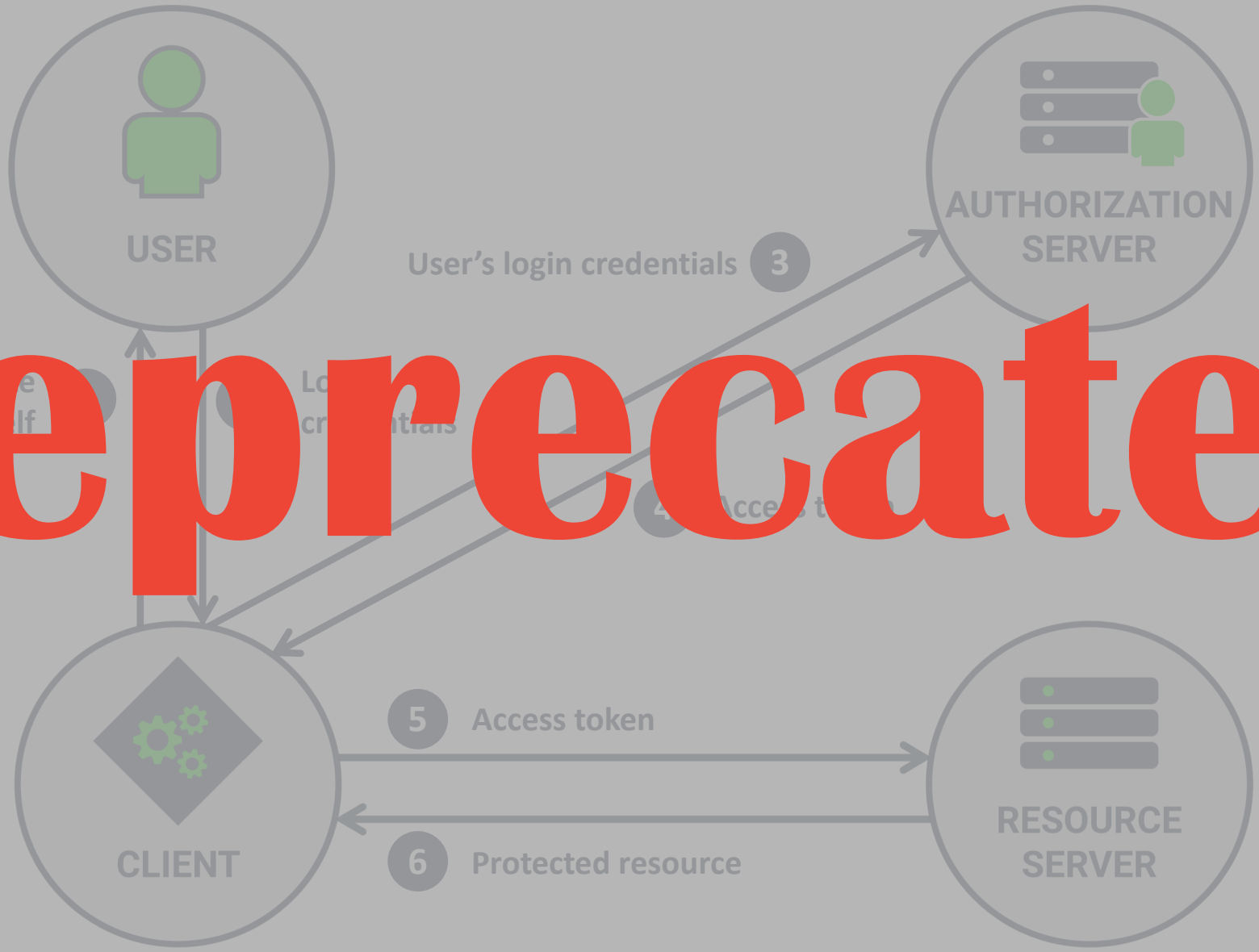
@PhilippeDeRyck

https://PragmaticWebSecurity.com

The Resource Owner Password Credentials Grant flow



The Resource Owner Password Credentials Grant flow



Deprecated

Challenges with *password-based* flows

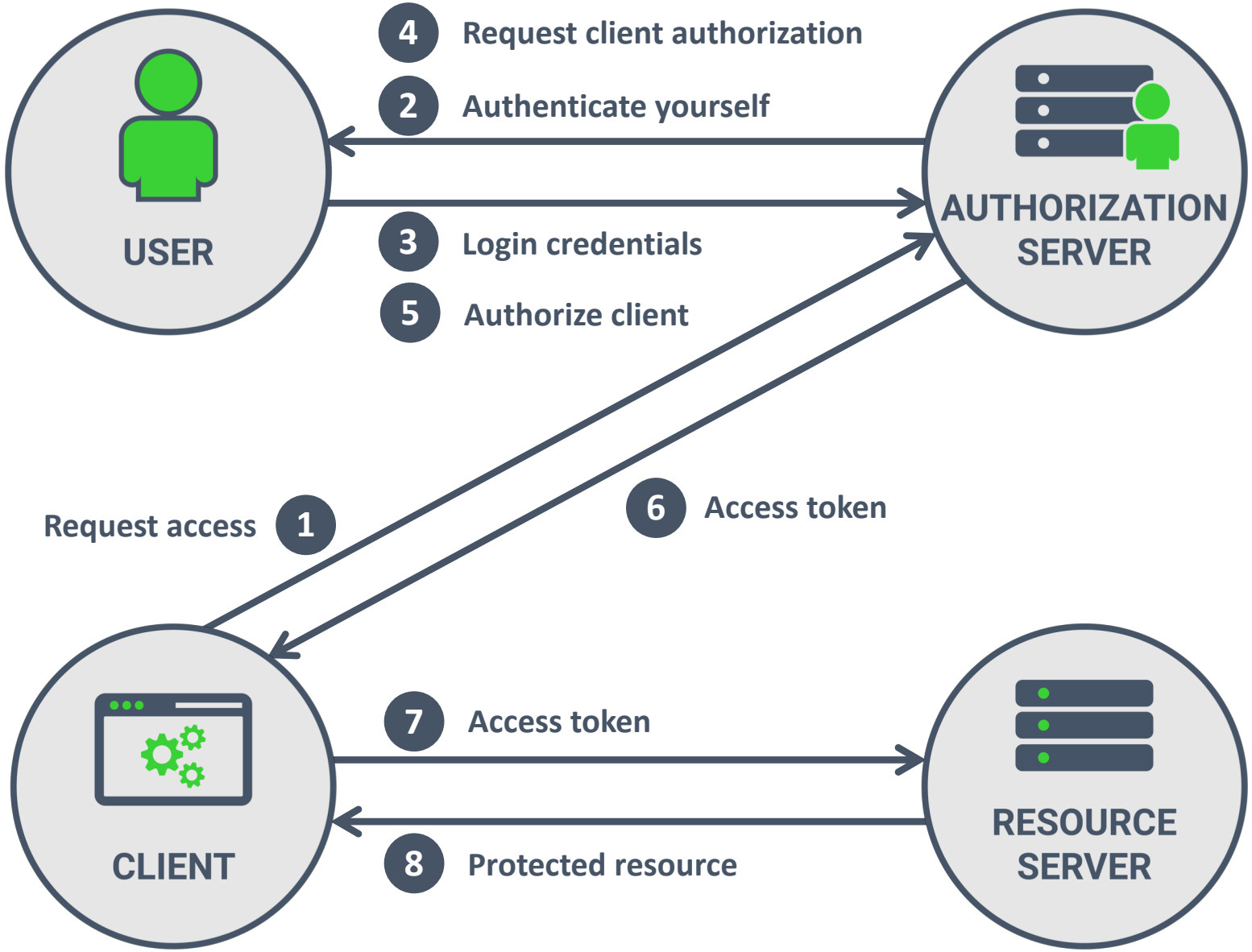
Giving client applications access to raw credentials

Teaching users to fill out passwords everywhere

Frontend applications cannot use client credentials in the flow

Refresh tokens should not be used without client credentials

THE IMPLICIT GRANT FLOW



Challenges with Implicit Grant flows

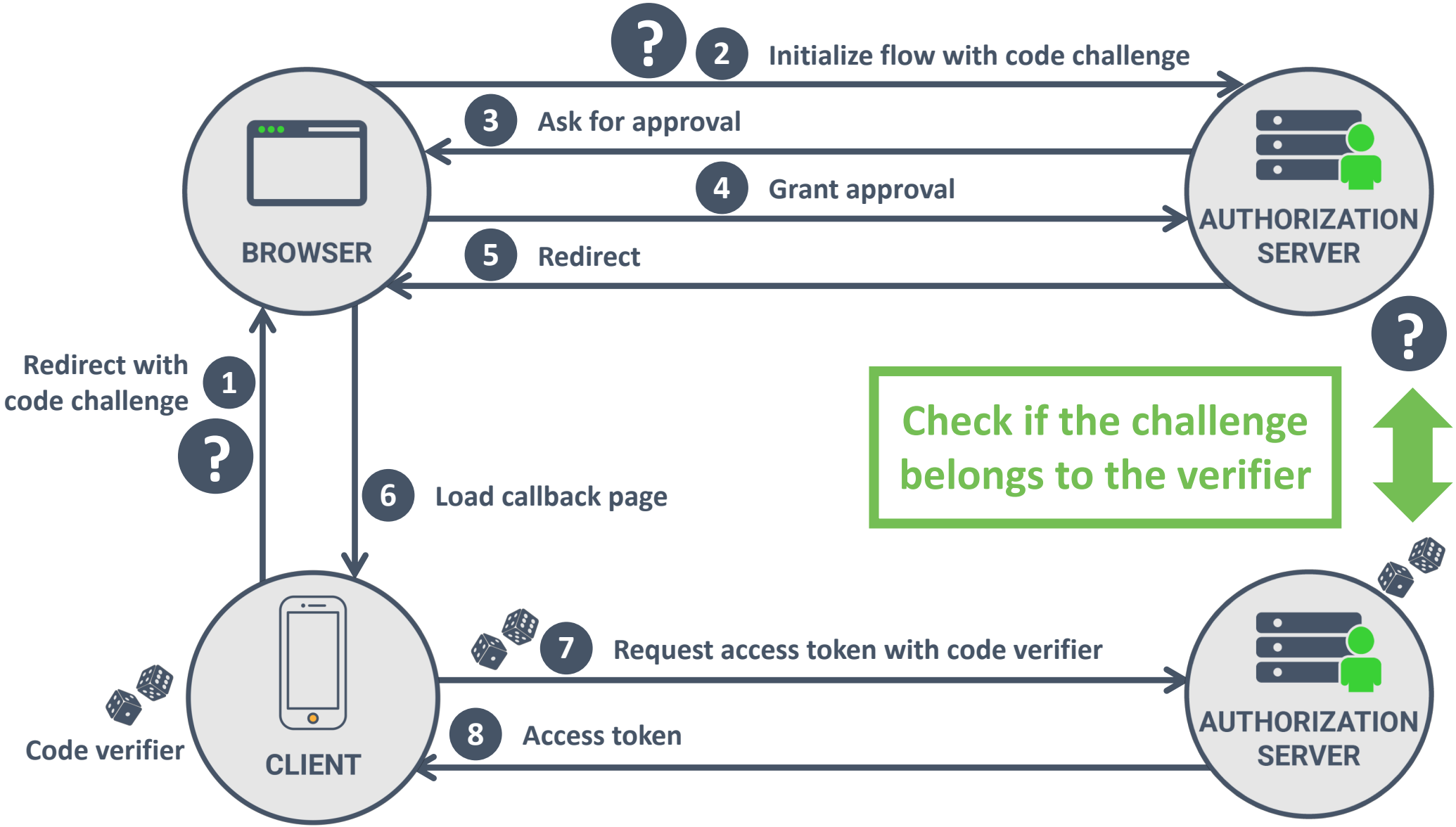
Tokens are part of the browser history

Mobile applications suffer from callback interception attacks

Refresh tokens are not available in this flow

Silent refresh of expired access tokens is not always available

The PKCE-based Authorization Code Grant flow



Revisiting earlier challenges

Tokens are part of the browser history

Mobile applications suffer from callback interception attacks

Refresh tokens are not available in this flow

Silent refresh of expired access tokens is not always available

Revisiting earlier challenges

~~Tokens are part of the browser history~~

~~Mobile applications suffer from callback interception attacks~~

~~Refresh tokens are not available in this flow~~

~~Silent refresh of expired access tokens is not always available~~

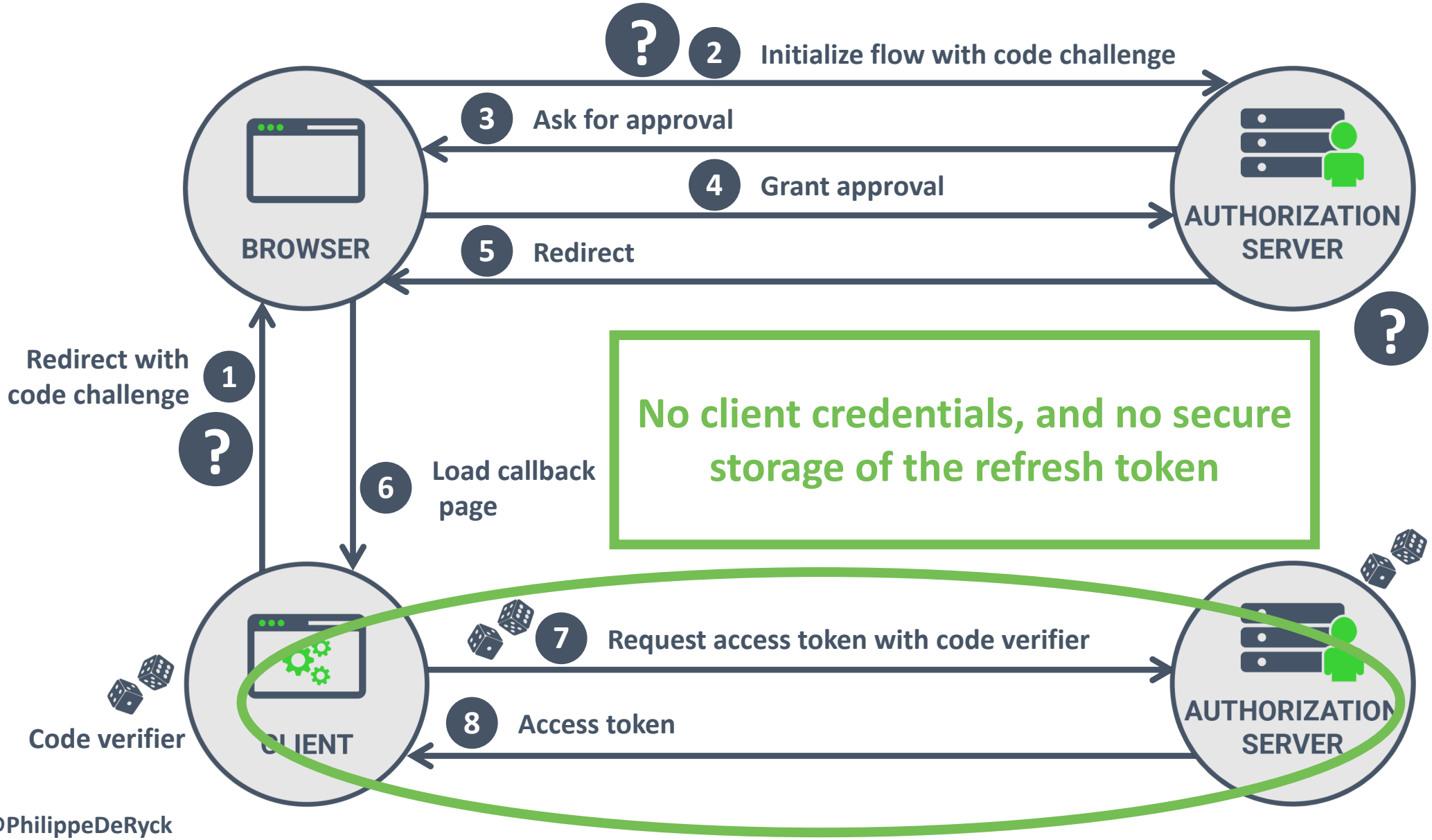
NO CLIENT CREDENTIALS TO EXCHANGE REFRESH TOKEN

NO SECURE STORAGE FOR THE REFRESH TOKEN

NO CLIENT CREDENTIALS TO EXCHANGE REFRESH TOKEN

NO SECURE STORAGE FOR THE REFRESH TOKEN

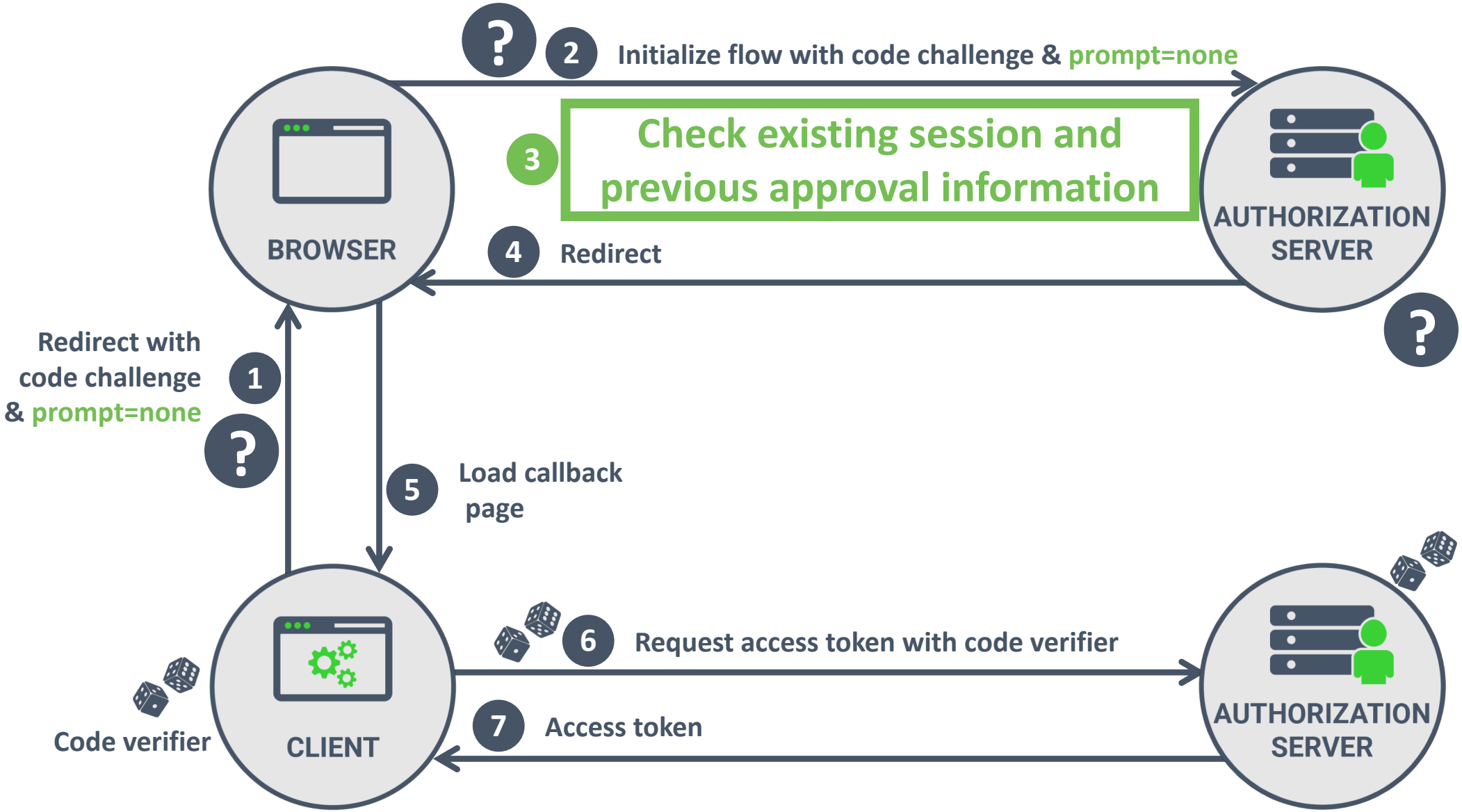
THE PKCE-BASED AUTHORIZATION CODE GRANT FLOW



How can you SOLVE this problem gracefully?

prompt=none

SILENTLY REQUESTING A NEW ACCESS TOKEN



Silently requesting a new access token

The user maintains a session with the authorization server

As long as the session is active, access tokens can be requested

The client only needs to handle short-lived access tokens

Requires support for the PKCE-based Authorization Code Flow

Oct. 15th – 16th 2018

Leuven, Belgium

Oct. 18th – 19th 2018

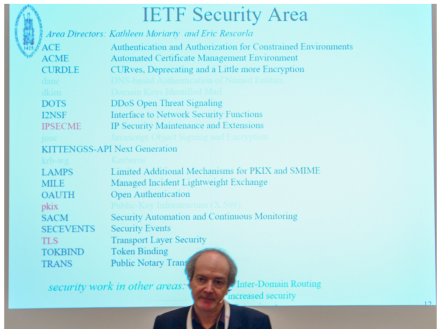
Web Security Essentials

Angular Security Masterclass

https://pragmaticwebsecurity.com/#courses

SecAppDev 2019

February 18 - 22, Leuven, Belgium



1-day workshops

Building secure web & web service applications
Jim Manico

Whiteboard hacking (aka hands-on Threat Modeling)
Sebastien Deleersnyder

Securing Kubernetes the hard way
Jimmy Mesta

5-day dual-track program

Crypto, AppSec Processes, web security, access control, mobile security, ...

Pragmatic Web Security

Security training for developers

/in/PhilippeDeRyck

@PhilippeDeRyck

philippe@pragmaticwebsecurity.com