Building the Authorization Server

Justin Boyer

OWNER, GREEN MACHINE SECURITY

https://justinboyerwriter.com

The Role of the Authorization Server

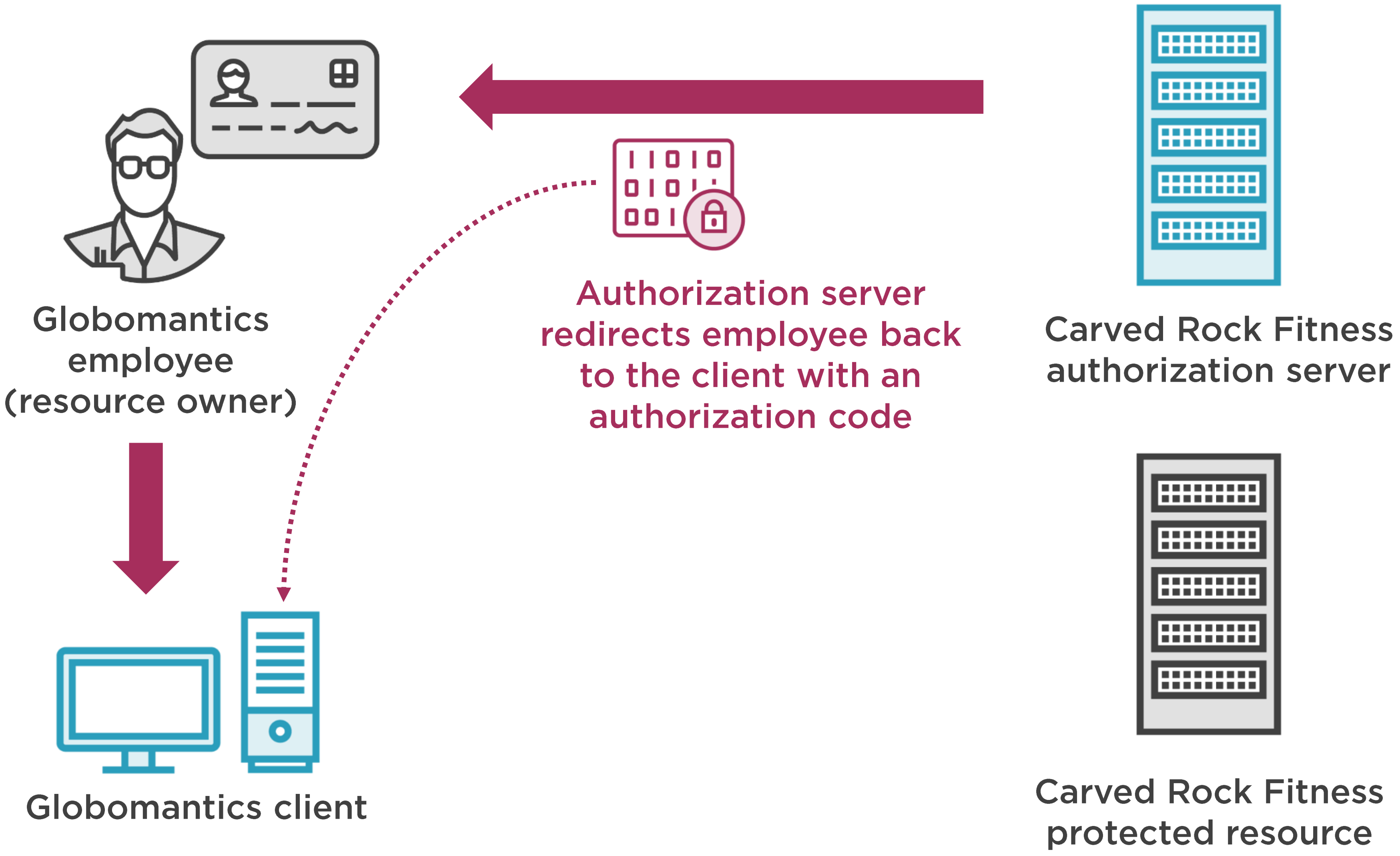
Authenticate

Verify the identity of the resource owner

Create the Authentication Code and Token

Give an authentication code and access token to access the protected resource

How the Application Works



Globomantics employee (resource owner)

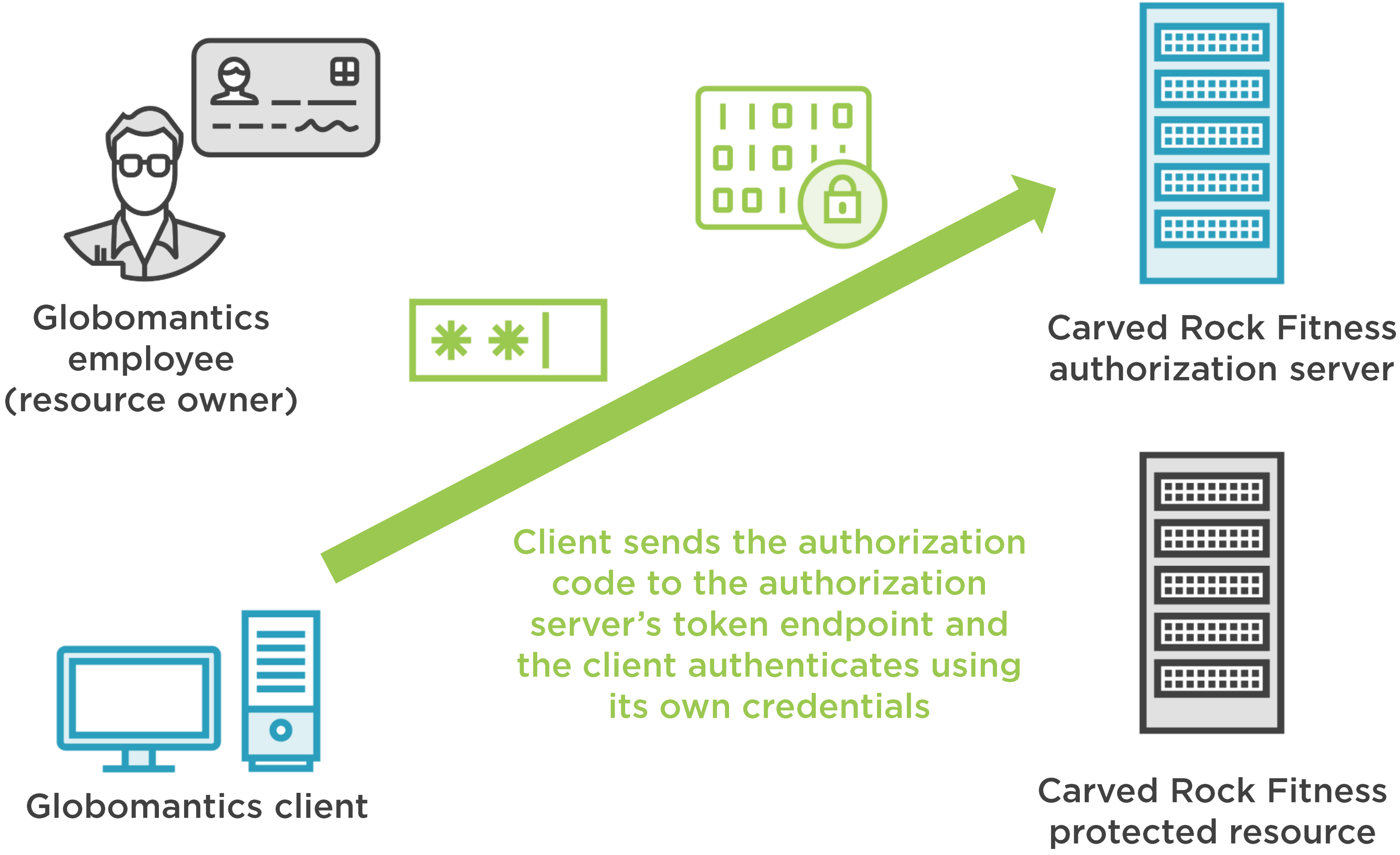
Authorization server redirects employee back to the client with an authorization code

Carved Rock Fitness authorization server

Globomantics client

Carved Rock Fitness protected resource

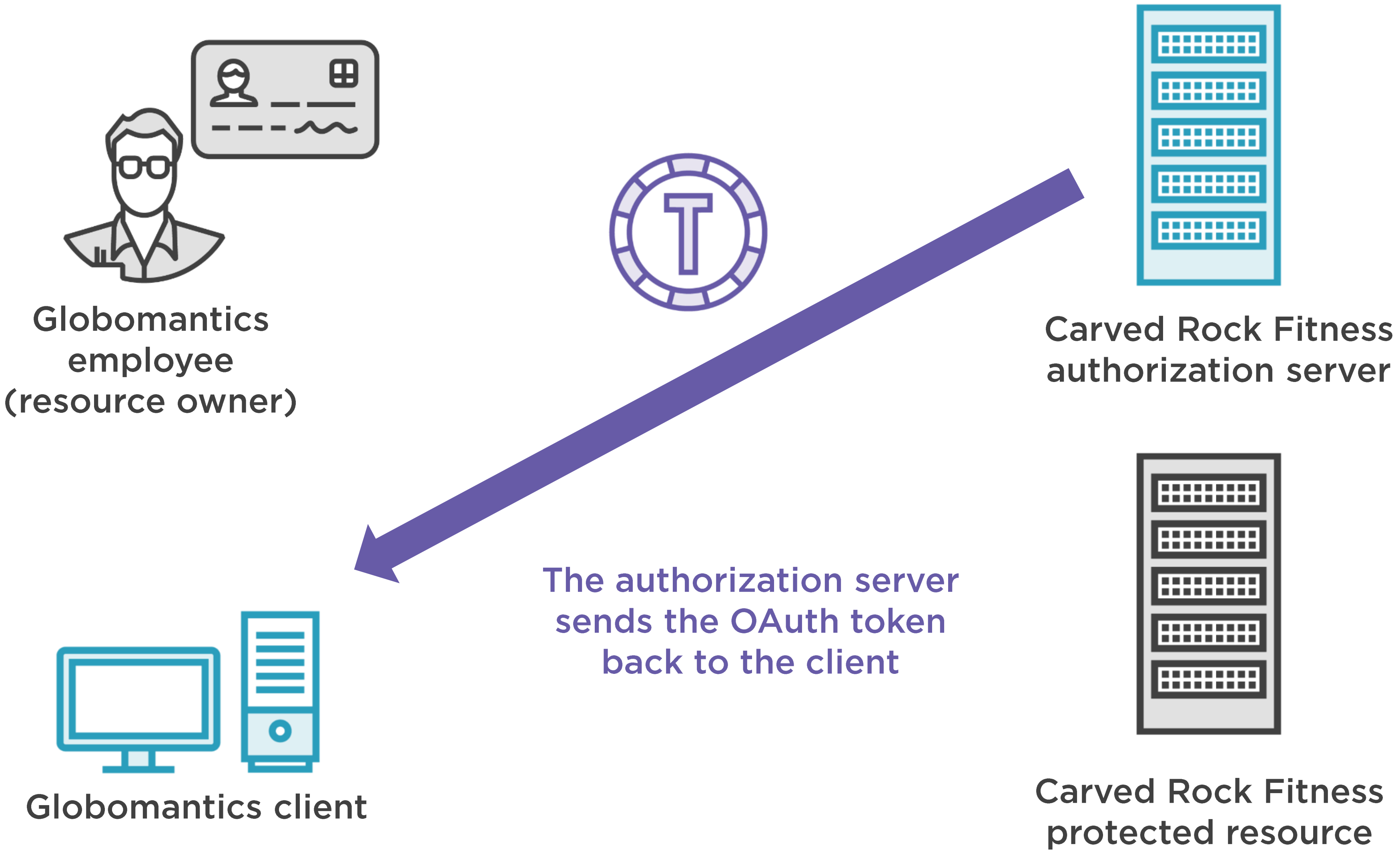
How the Application Works



Globomantics employee (resource owner)
Carved Rock Fitness authorization server
Globomantics client
Carved Rock Fitness protected resource

Client sends the authorization code to the authorization server’s token endpoint and the client authenticates using its own credentials

How the Application Works


Globomantics employee (resource owner)
Carved Rock Fitness authorization server
Globomantics client
Carved Rock Fitness protected resource

The authorization server sends the OAuth token back to the client

Authorization Server Vulnerabilities

Session Hijacking

Authorization code passed through a URL

URL remains in browser history

On a public computer attacker could use authorization code and use it to get an access token

Fix: Authorization codes are single use only

Redirect URI Manipulation

Authorization server validates redirect URIs only using the domain

Allowing subdirectory or allowing subdomain validation opens security holes

Fix: Only use exact matching validation for redirect URIs

Client Impersonation

Attacker steals authorization code

Attacker uses victim's authorization code with his redirect URI

Authorization server doesn't verify redirect URI and gives token to the attacker

Fix: When a redirect URI is in the initial request, the authorization server must validate the redirect URI sent in the access token request

Web API Security Risks

Authorization servers could be vulnerable to any common web API vulnerabilities

Fix: Follow security best practices for web APIs

Pluralsight's Web Application Security Learning Path

- https://app.pluralsight.com/paths/skills/web-application-security

What Have We Learned?

The authorization server is the holder of the “keys” to the OAuth system

Implementing an authorization server in Node.js

Authorization Server Vulnerabilities

- Session hijacking
- Redirect URI manipulation
- Client impersonation
- Web API vulnerabilities

You have the tools, now build your authorization server