ORY / summit-22

Deniz Onur Duzgun

Cloud security @ Wise Systems

✉ dduzgun@wisesystems.com

Make Auth Great Again With Ory

October 20th 2022

About Me

Deniz Onur Duzgun
Cloud Security @ Wise Systems

- Father of two wonderful 🐶

- Automation and simplicity lover

- Background:
  - Developer
  - Offensive security
  - DevSecOps

Typical Authentication Mistakes

🤔💭
Complicating It

Often not easily reusable and poorly documented

👨‍💼
Writing your own

Often results in bad design or the wrong spec

🎨
Never the same

Everyone implements it in their own way - poorly

👷
Implementation

Challenging to make it fast, reliable and robust

🔍
Vulnerability
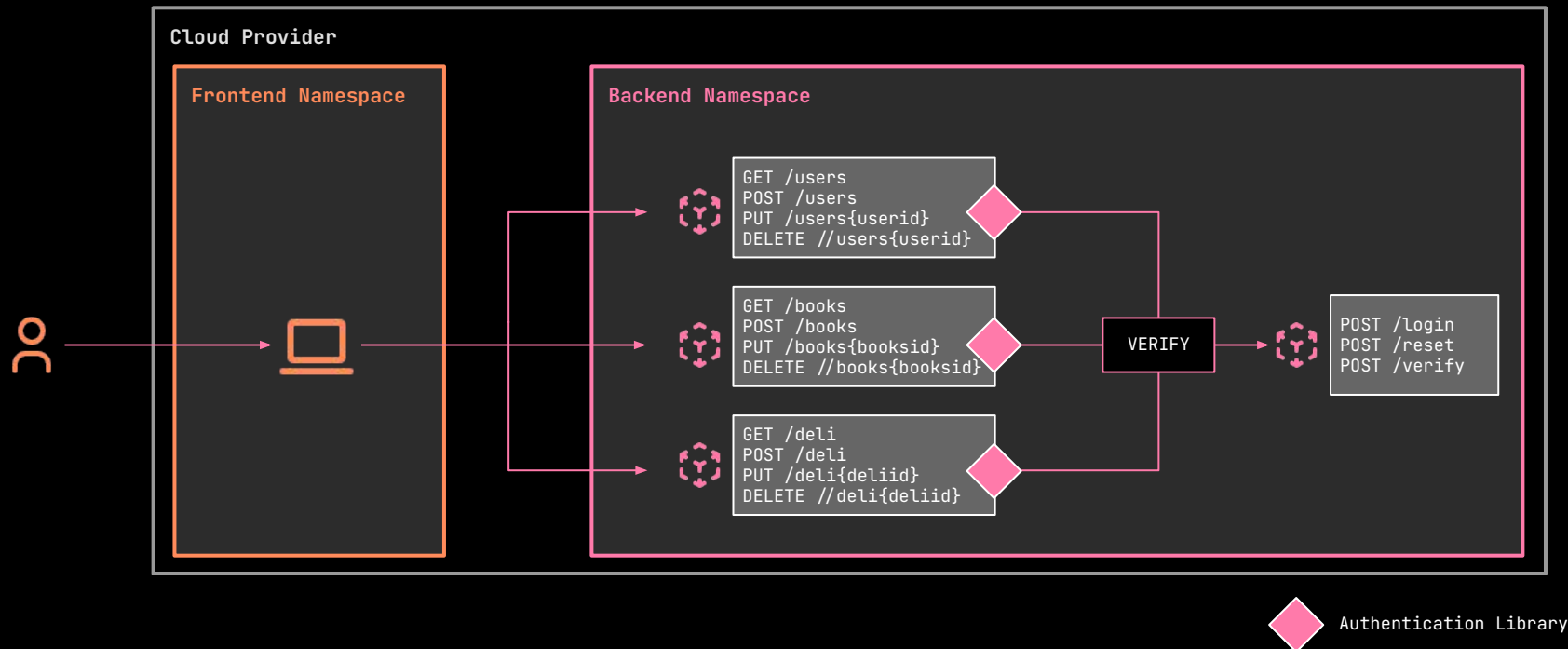
One mistake opens up exploitable security flaws

🚧
Maintenance

Updating, versioning, consuming, deploying - have fun

Agenda

01 **Typical Authentication Mistakes**

02 **Life without modern Authentication**

03 **Why is Ory different for Authentication?**

04 **Demo Time** 👀

05 **Questions Time**
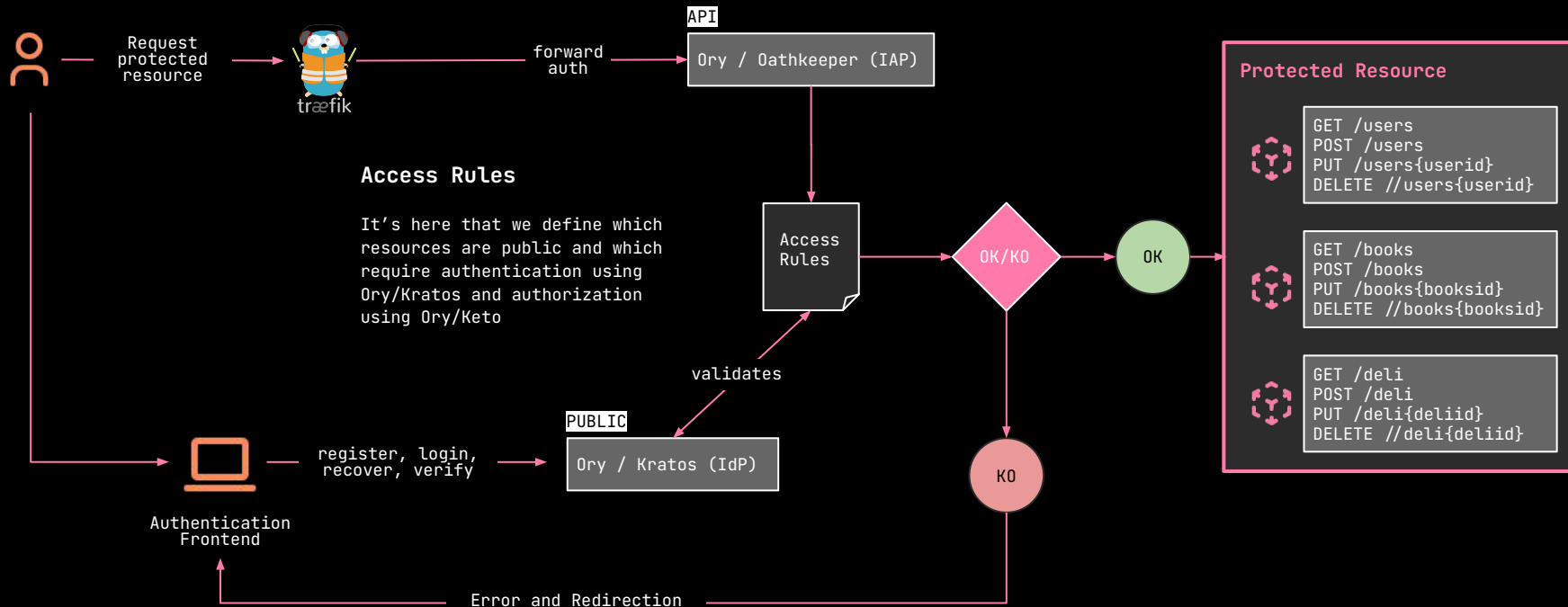
Life without modern Authentication

The Outcome

- Service code gets heavy and complex

- Copy pasting authentication code can result in more mistakes

- Different versions of the authentication libraries are used

- Adds up latency to service calls

- A new version of the authentication services will impact other services

- Really risky, one mistake will result in big security issues

The Security Outcome

Why is Ory different for Authentication?

Access Rules

It's here that we define which resources are public and which require authentication using Ory/Kratos and authorization using Ory/Keto

API
Ory / Oathkeeper (IAP)

Request protected resource

forward auth

Access Rules

OK/KO

OK

KO

validates

PUBLIC
Ory / Kratos (IdP)

register, login, recover, verify

Authentication Frontend

Error and Redirection

Protected Resource

```
GET /users
POST /users
PUT /users{userid}
DELETE //users{userid}
```

```
GET /books
POST /books
PUT /books{booksid}
DELETE //books{booksid}
```

```
GET /deli
POST /deli
PUT /deli{deliid}
DELETE //deli{deliid}
```

How it looks like with Ory

Challenge 1

Find what you need

Ory offers **many projects**, be sure to select the ones that apply to you

Challenge 2

Find where to host

Depending on your business, you can use Ory Cloud or host it internally using the Helm charts.

Challenge 3

Start small

If at first, **you don't need OAuth2 (Ory Hydra)**, Ory Kratos and Oathkeeper are a good starting point.

Demo Time

https://github.com/dduzgun-security/examples
/tree/master/kratos-oathkeeper-traefik

Question Time

Thank you!

Contact me
dduzgun@wisesystems.com