Securing Microservices

Mark Heath
CLOUD ARCHITECT

@mark_heath www.markheath.net

Overview

Encryption

- In transit and at rest

Authentication

Authorization

OAuth 2.0 and OpenID Connect

Network security

- Virtual networks, IP whitelisting and firewalls

Defense in depth

- Penetration testing, alerts, auditing

Sensitive Data

Catalog Service

Non-sensitive data

Ordering Service

Highly sensitive data

Needs encryption

Encrypting Data

Encryption in transit

Use standard algorithms

Transport Layer Security (TLS)

SSL certificates

Certificate management

Encryption at rest

Disk encryption

Key management

Encrypt backups

Authentication

We need to know who is calling our service

HTTP Authorization Options

Username & password

“Basic authentication”

Client login

Requires password storage

API key

Key per client

Key management

Client certificate

Public-key cryptography

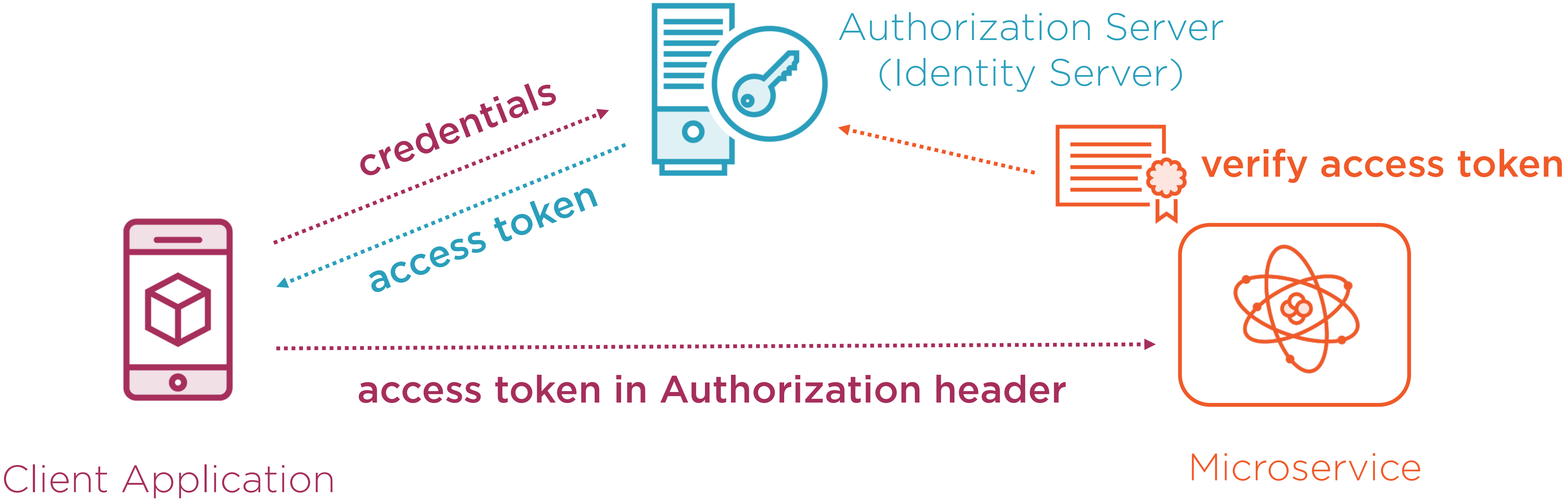
Complex management

Using an Identity Server

Use industry-standard protocols:

OAuth 2.0 & OpenID Connect

IdentityServer4



Authorization Server
(Identity Server)

credentials

access token

verify access token

access token in Authorization header

Client Application

Microservice

Learn More About OAuth 2.0 and OpenID Connect

Getting Started with OAuth 2.0 (Scott Brady)

https://www.pluralsight.com/courses/oauth-2-getting-started

ASP.NET Authentication: The Big Picture (Scott Brady)

https://www.pluralsight.com/courses/aspdotnet-authentication-big-picture

Securing ASP.NET Core 2 with OAuth2 and OpenID Connect (Kevin Dockx)

https://www.pluralsight.com/courses/securing-aspdotnet-core2-oauth2-openid-connect

Authorization

Authentication: who is calling?

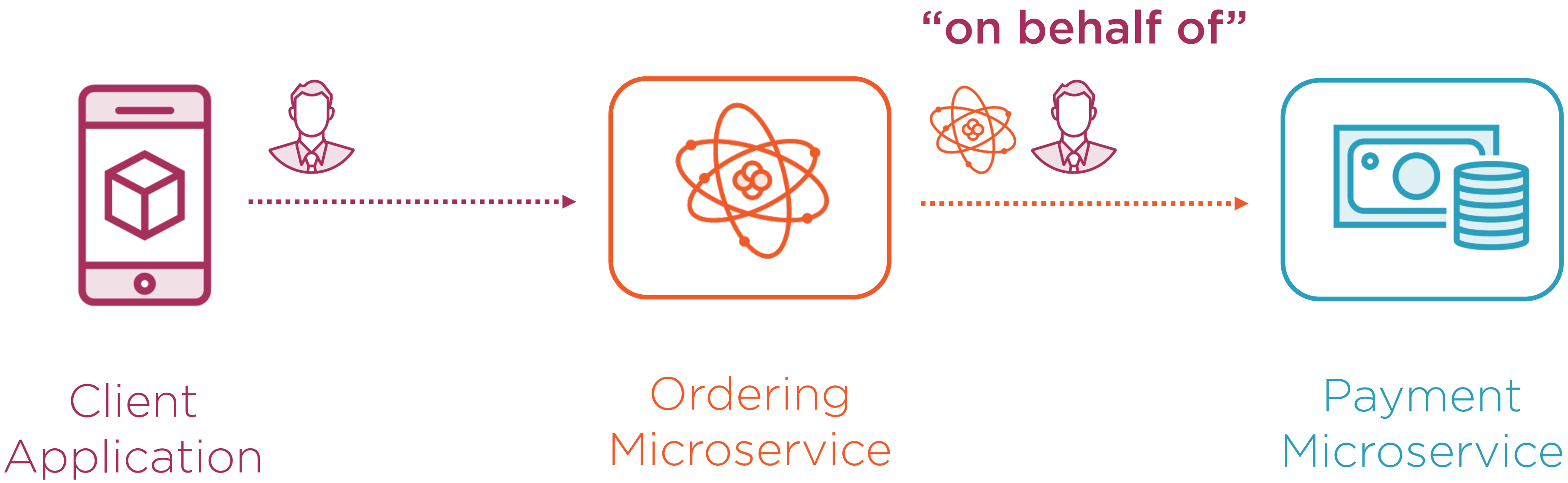
Authorization: what can they do?

- e.g. I can see **my** orders
- I should not be allowed to see **your** orders

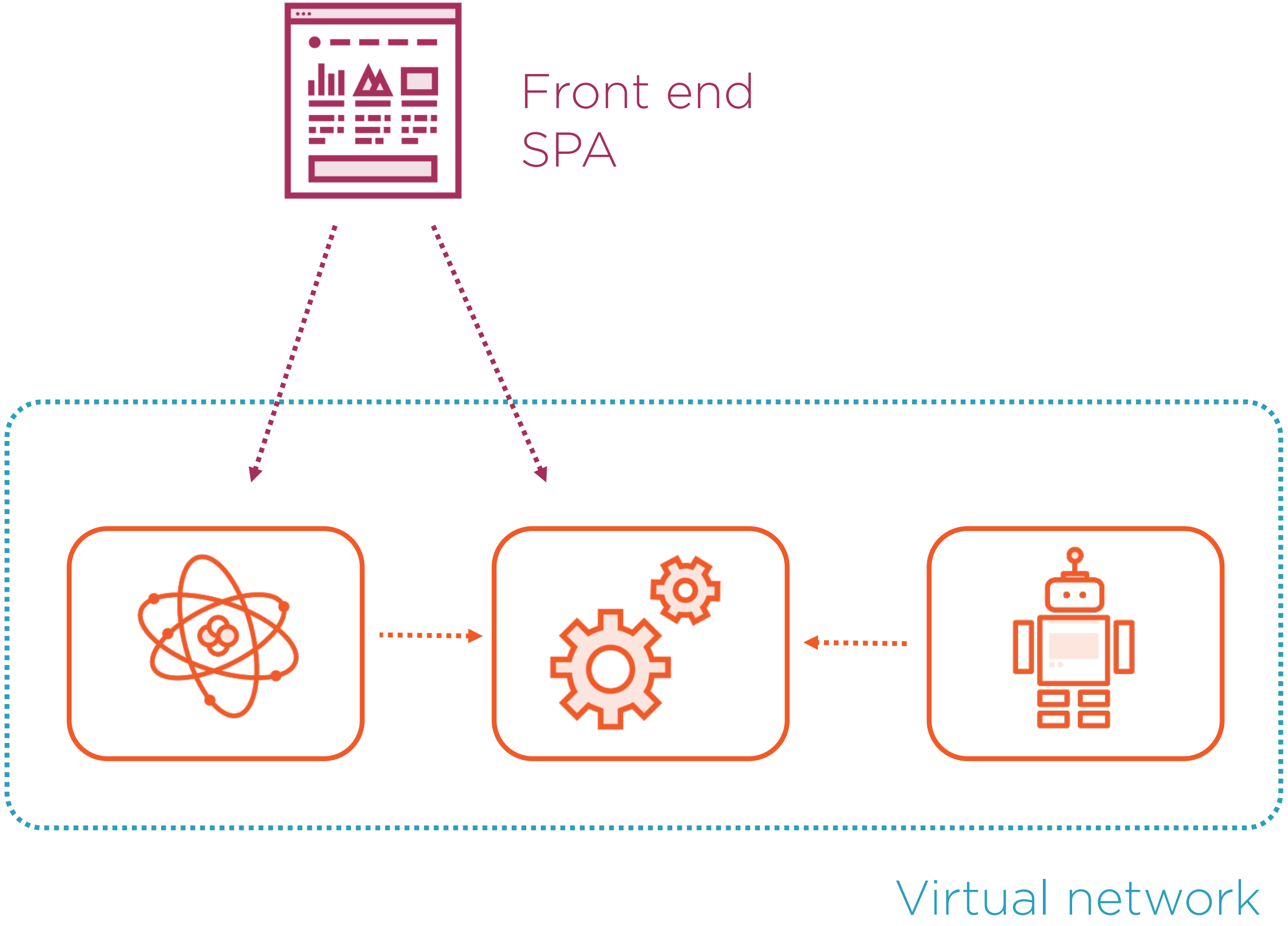
Authorization frameworks

- Can make decisions based on “roles”
- Consider carefully what callers should be allowed to do

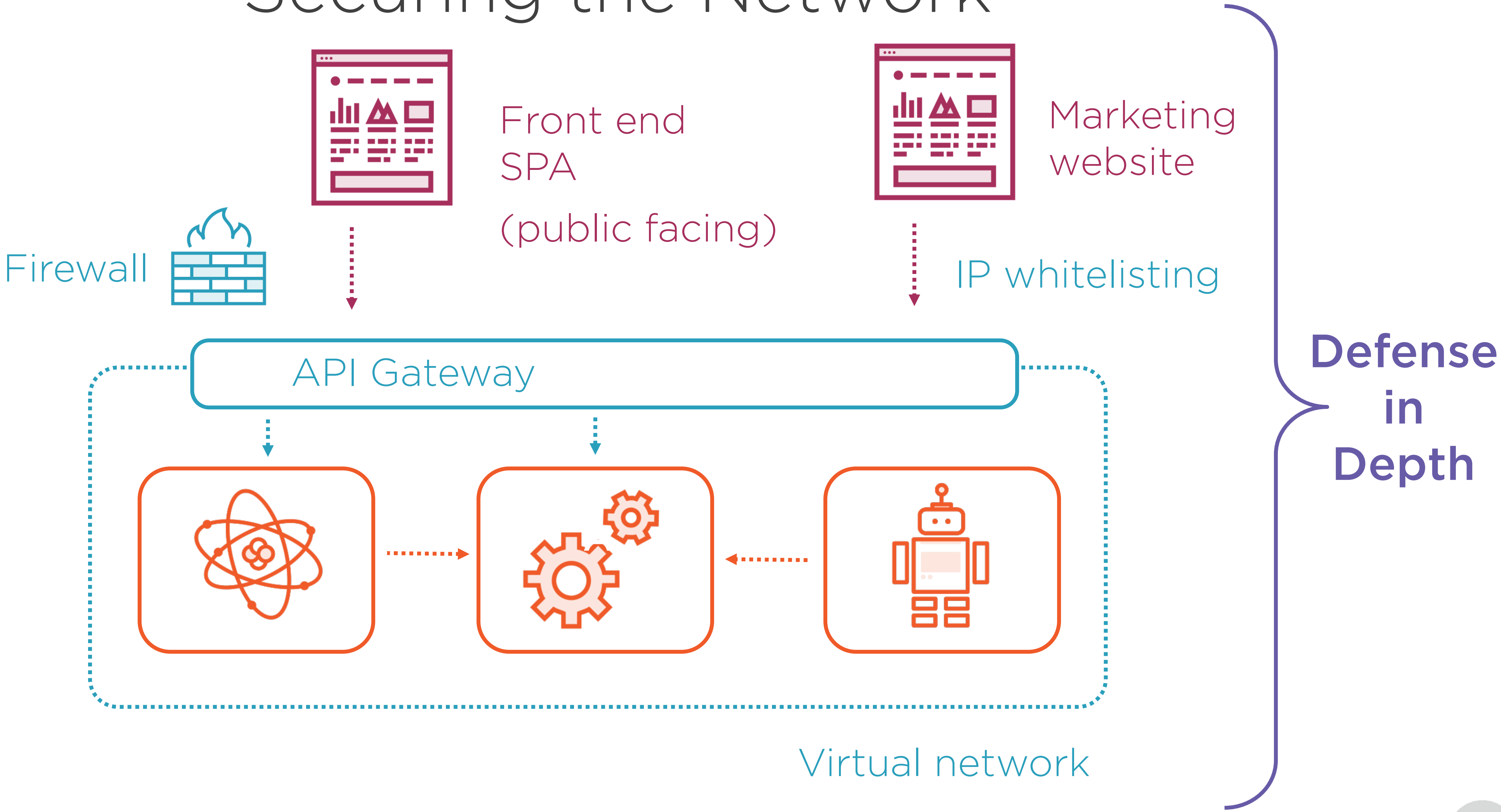
Confused Deputy



Securing the Network



Securing the Network



Defense in Depth

Encryption in transit

Access tokens

Network security

Don’t rely on a single technique

Apply multiple layers of protection

Additional Defensive Measures

Penetration testing … get help from the experts

Automated security testing … prove your APIs reject unauthorized callers

Attack detection … react quickly when you’re under attack

Auditing … know exactly who did what and when

Summary

Security matters!

Defense in depth

- Encryption in transit (TLS)
- Encryption at rest
- Authentication
- OAuth 2.0 and OpenID Connect
- Authorization
- Virtual networks
- IP whitelisting
- Firewalls
- API gateways
- Penetration testing
- Attack detection

Up next…

Delivering microservices