

# Internet Applications Design and Implementation

## 2020 - 2021

**MIEI - Integrated Master in Computer Science and Informatics  
Specialization block**

**João Costa Seco ([joao.seco@fct.unl.pt](mailto:joao.seco@fct.unl.pt))**

(with previous participations of Jácome Cunha ([jacome@fct.unl.pt](mailto:jacome@fct.unl.pt)) and João Leitão ([jc.leitao@fct.unl.pt](mailto:jc.leitao@fct.unl.pt)))



**FACULDADE DE  
CIÊNCIAS E TECNOLOGIA  
UNIVERSIDADE NOVA DE LISBOA**

# Internet Applications Design and Implementation

## 2020 - 2021

### (Introductory Video and Logistics)

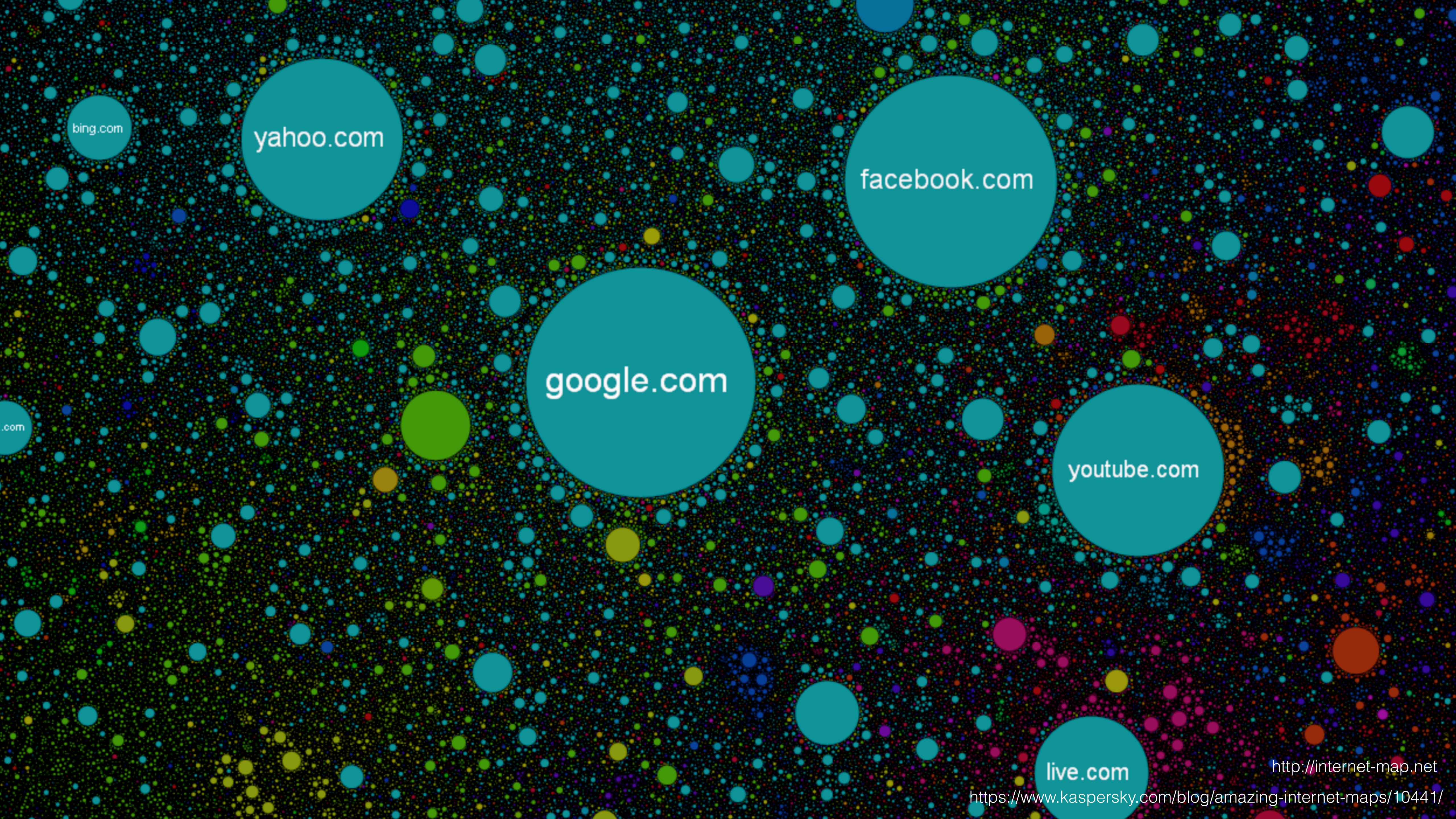
**MIEI - Integrated Master in Computer Science and Informatics  
Specialization block**

**João Costa Seco ([joao.seco@fct.unl.pt](mailto:joao.seco@fct.unl.pt))**

(with previous participations of Jácome Cunha ([jacome@fct.unl.pt](mailto:jacome@fct.unl.pt)) and João Leitão ([jc.leitao@fct.unl.pt](mailto:jc.leitao@fct.unl.pt)))



FACULDADE DE  
CIÊNCIAS E TECNOLOGIA  
UNIVERSIDADE NOVA DE LISBOA



live.com

<http://internet-map.net>

<https://www.kaspersky.com/blog/amazing-internet-maps/10441/>

# Internet Applications Design and Implementation

---

**Internet application | 'ɪntənet aplɪ'keɪʃ(ə)n |, noun**

1. Any application that uses the internet to consume and/or provide services and data.

# Internet Applications Design and Implementation

---

**Web application | wɛb aplɪ'keɪʃ(ə)n |, noun**

1. An internet application that runs on a browser and obtains HTML and data pages from a web server.

**Mobile application | 'məʊbʌɪl aplɪ'keɪʃ(ə)n |, noun**

2. An application installed and running in a mobile device, usually dependent on web services as data sources.

**Web service | wɛb 'sə:vɪs |, noun**

3. A computational procedure available on the Internet to provide services and data to other apps and services. Usually associated to binding technologies like SOAP or REST.

# Internet Applications Design and Implementation

---

**Cloud application | klaʊd aplɪ'keɪʃ(ə)n |, noun**

1. An internet application deployed on an independent hosting service, providing computation and additional resources and features like replication and storage.

**Service-based architecture | 'sə:vɪs bə:s 'a:kɪtɛktʃə |, noun**

2. A conceptual structure and logical organisation of web services, usually implemented using orchestration languages and tools.

**Data-Centric Applications | Data'deɪtə-'sentrɪk ,æplɪ'keɪʃ(ə)nz |, noun**

3. Applications that are developed primarily based on resource-based rules, making their data available to others through well defined interfaces

# Internet Applications Design and Implementation

---

The challenge is to **design, specify, and implement**

modular,  
loosely-coupled,  
large-scale applications,

so that the software development process is more efficient and the longevity of the applications is longer.

# Internet Applications Design and Implementation

---

- Goals:
  - Faster development cycles,
  - functionally correct applications,
  - applications that can easily be used by other systems,
  - heterogeneous development and execution environments,
  - applications are easily maintainable (corrections and extensions)
  - secure systems
  - reliable and available systems
  - performant applications

# Internet Applications Design and Implementation

---

- Goals:
  - Faster development cycles,
  - functionally correct applications
  - Many of these goals are specific of Internet Applications and should be attained using specific methods, tools and techniques.
  - secure systems
  - reliable and available systems
  - performant applications

What about Internet Applications?

# Features of Internet Applications

---

- Everything is (inter)connected and developing software for interconnection requires special skills and methods
- Internet Apps can be:
  - Standalone / Desktop with native interfaces (RPC) or http connections
  - Web, via http, accessible through browsers
  - Mobile native or PWAs (connected via http or native, w/ offline capabilities)
  - Compound and orchestrated services
  - Mash-up interfaces  
(e.g. google maps + rentals, friends, ...<http://mashable.com/2009/10/08/top-mashups/>)

# Skills for Internet Applications

- Special skills because
  - software evolves fast, we need to develop extensible and maintainable software.
  - data and code have different wills, we need to develop software in sync with data.
- software is “open” and connected (the world changes), we need to develop software that is loosely coupled, robust and follows standard API conventions.
- Internet Apps may grow to have a huge user base (millions of requests)...
- It also needs to be scalable, secure, replicated, reliable, concurrent, safe...

## Introduction To Continuous Delivery

#1 in the **Continuous Delivery** webinar series

This talk will introduce the principles and practices of Continuous Delivery, an approach pioneered by companies like Facebook, Flickr and ThoughtWorks, that aims to make it possible for an organization to deliver frequently (weekly, daily or even hourly) and confidently. It uses idea -> live (the time from idea being conceived until the feature is live) as a key metric, minimizing that metric across the whole path to production.



By Rolf Russell

DEC 11, 2012 @ 11:48 PM 8,338 VIEWS

## Gmail Outage Embarrasses Internet Giant -- Cause Was a Software Update

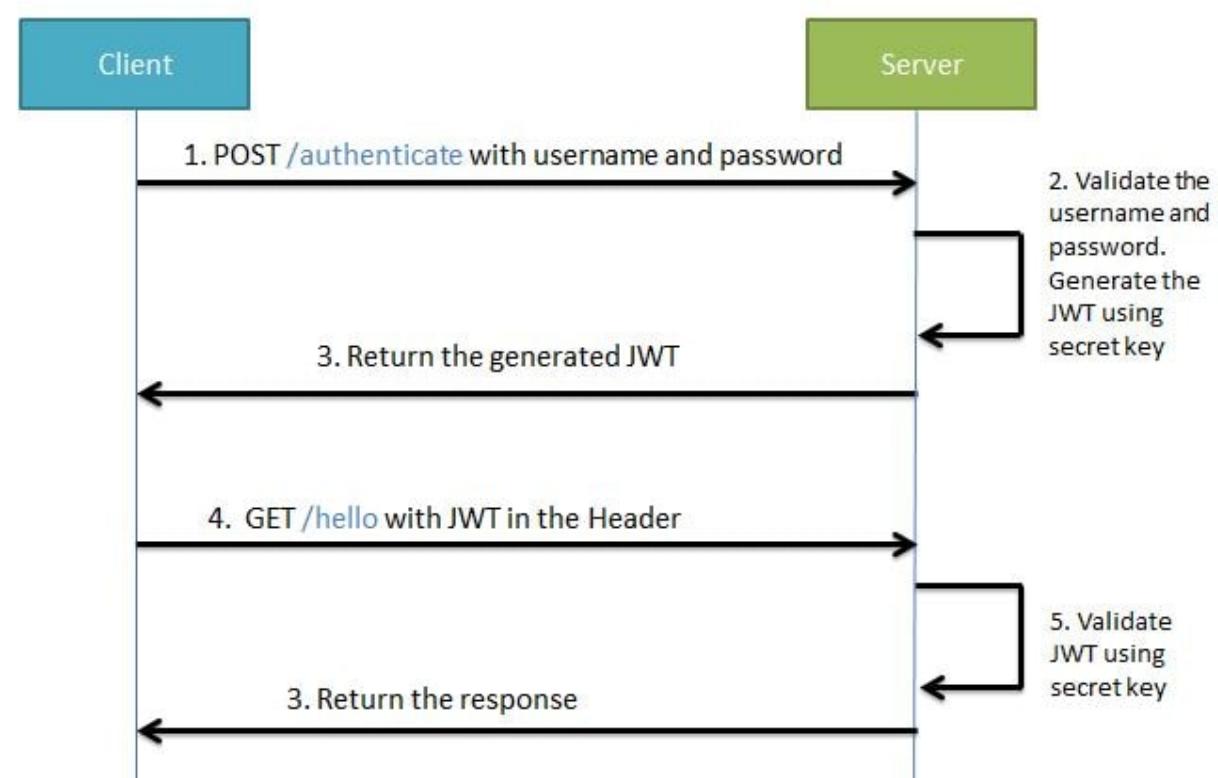
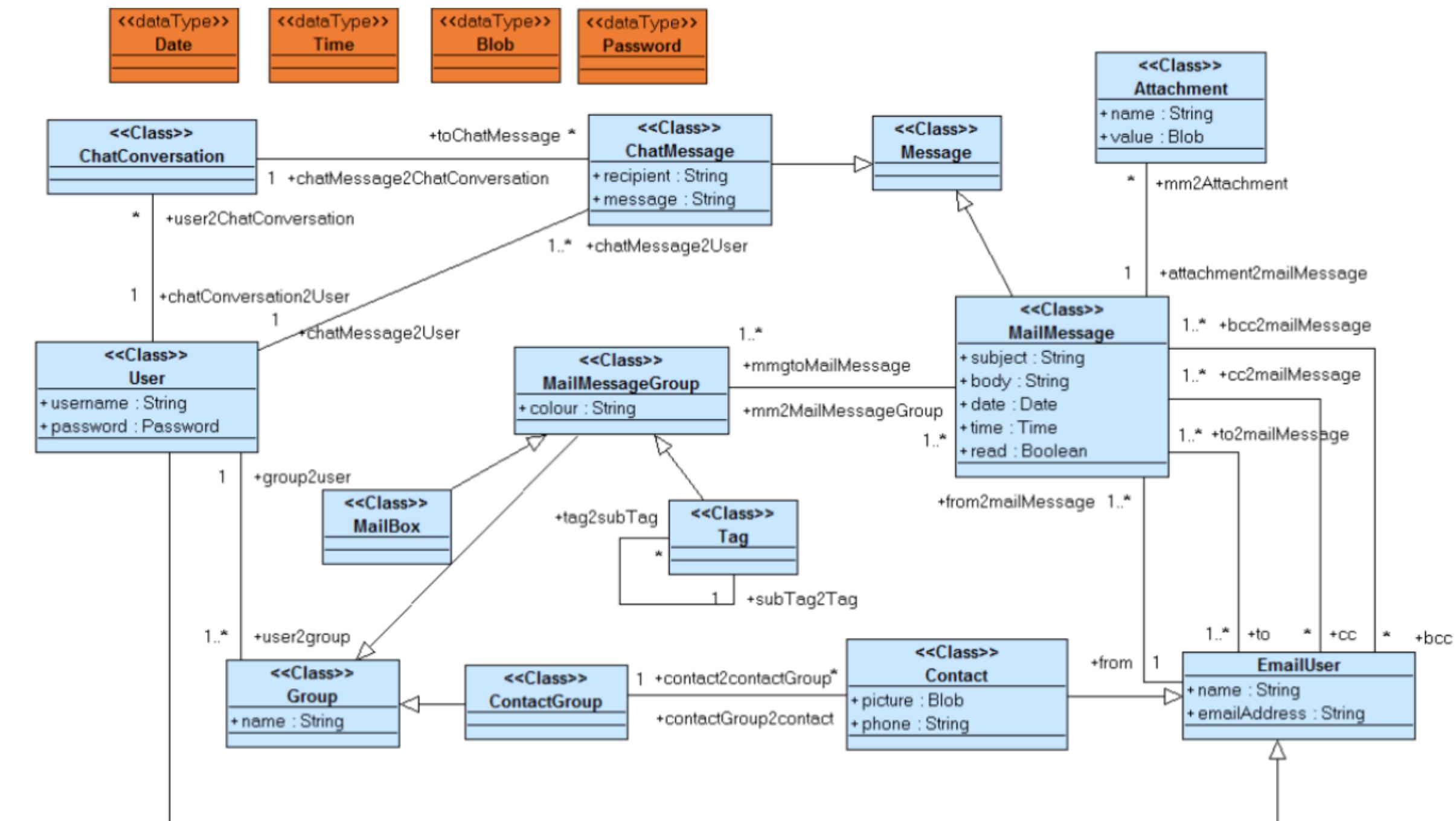
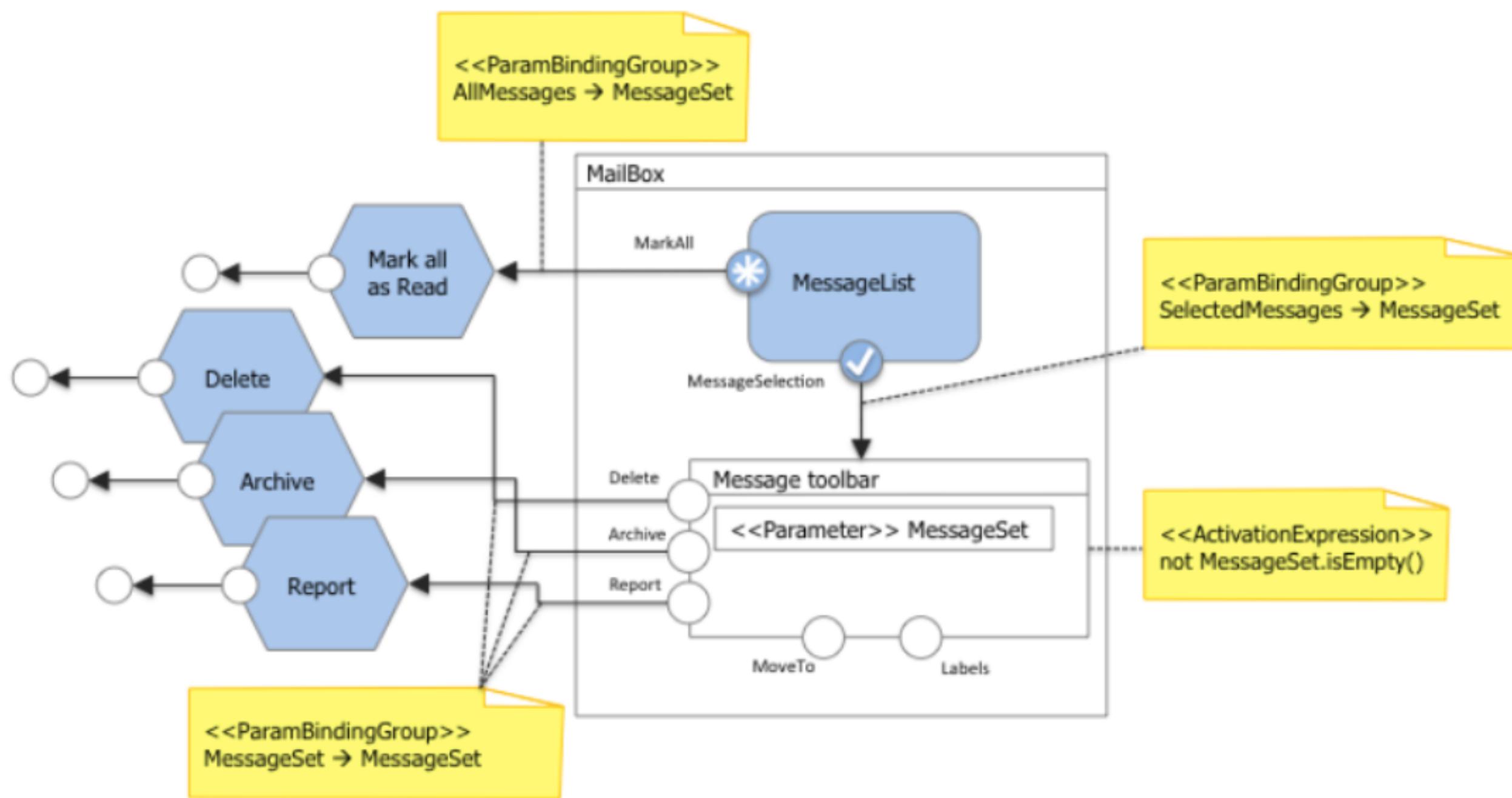
# “Tools” for Internet Applications

---

- Software Specification (UML, OpenAPI, IFML)
- Software Architecture (Web MVC, SOA, Micro Services)
- Software Patterns (Observer, Chain of Respons., Facade, Builder, ...)
- Programming Languages (Statically Typed, Dynamic, Concurrent, ...)
- Software Frameworks (Web, Component, Reactive, Data-Abstraction,...)
- Development Methods (Agile, TDD, BDD, Continuous Integration, C. Delivery)
- Deployment Tools (Cloud Managers, Containers, )

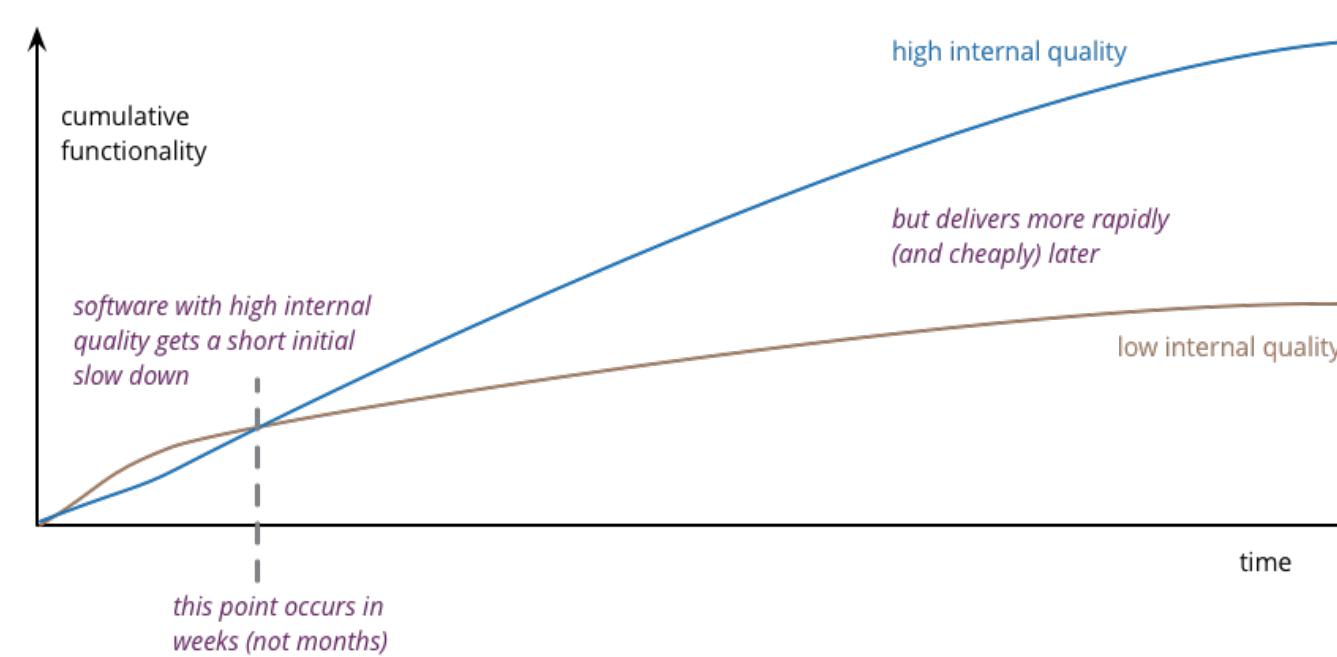
# Software Specification for Internet Applications

- Data schema specification
- Behaviour specification
- Interface-flow specification
- Security specification



# Software Architecture for Internet Applications

- Architecture refers to the internal design of a software system
- It describes the way the highest level components are wired together.
- A good architecture allows a system to be expanded with new capabilities
- A good architecture pays off in quality



in [martinfowler.com/architecture/](http://martinfowler.com/architecture/)

## What is architecture?

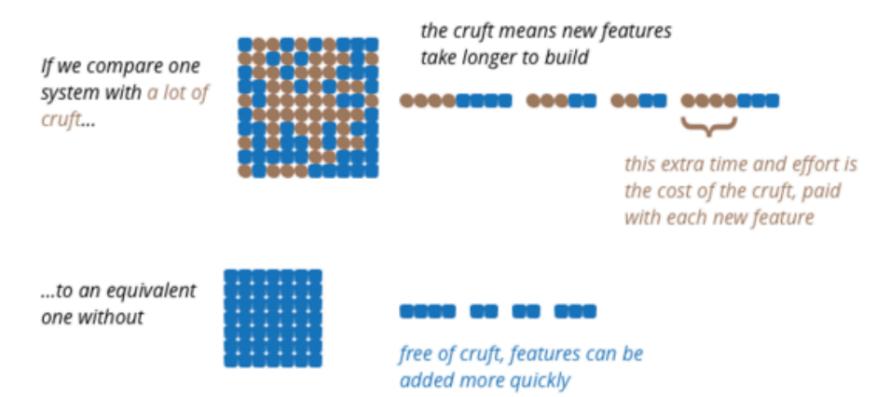
People in the software world have long argued about a definition of architecture. For some it's something like the fundamental organization of a system, or the way the highest level components are wired together. My thinking on this was shaped by an email exchange with Ralph Johnson, who questioned this phrasing, arguing that there was no objective way to define what was fundamental, or high level and that a better view of architecture was **the shared understanding that the expert developers have of the system design**.



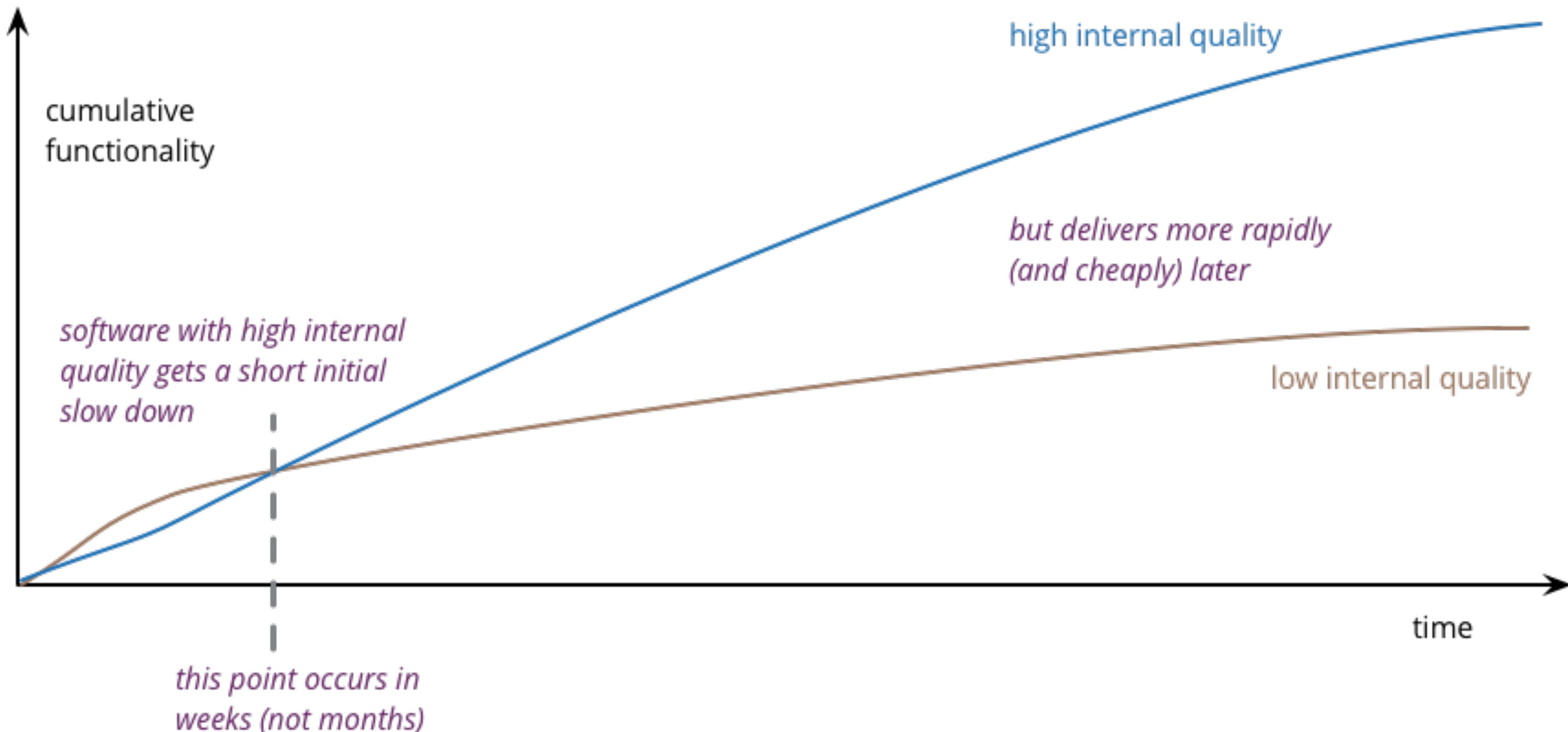
Ralph Johnson, speaking at QCon

## Why does architecture matter?

Architecture is a tricky subject for the customers and users of software products - as it isn't something they immediately perceive. But a poor architecture is a major contributor to the growth of **cruff** - elements of the software that impede the ability of developers to understand the software. Software that contains a lot of cruff is much harder to modify, leading to features that arrive more slowly and with more defects.



# Software Architecture for Internet Applications



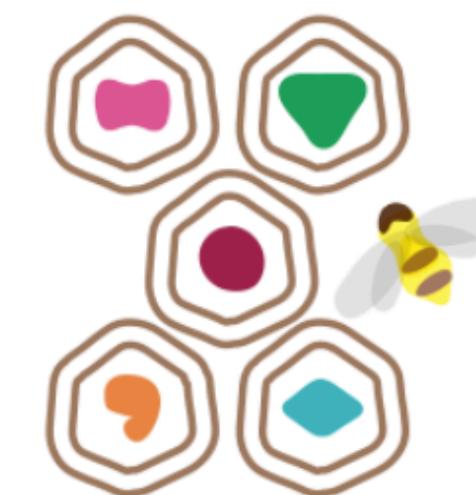
in [martinfowler.com/architecture/](http://martinfowler.com/architecture/)

# Software Architecture for Internet Applications

## Application Boundary

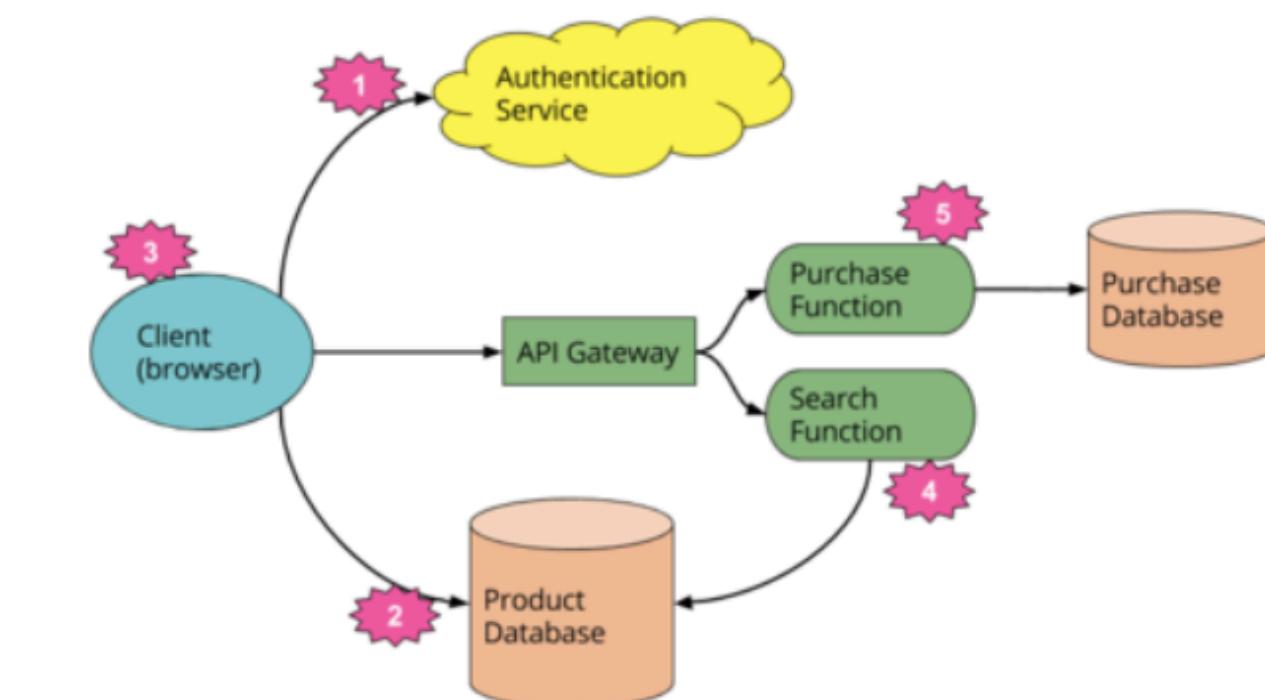
One of the undecided problems of software development is deciding what the boundaries of a piece of software is. (Is a browser part of an operating system or not?) Many proponents of Service Oriented Architecture believe that applications are going away – thus future enterprise software development will be about

## Microservices Guide

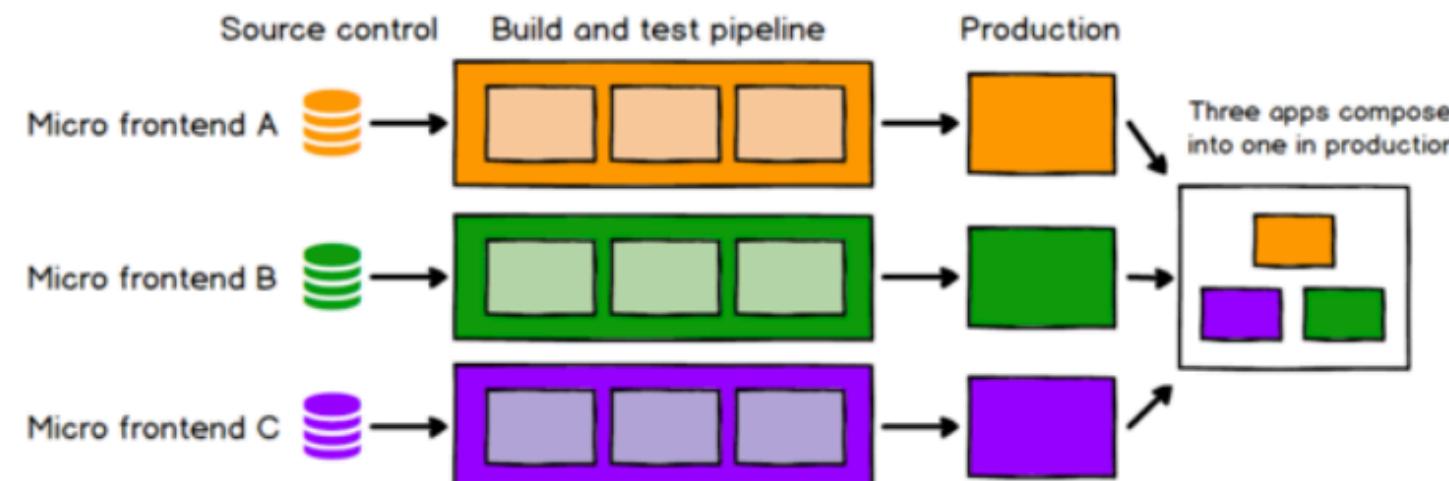


The microservice architectural pattern is an approach to developing a single application as a

## Serverless Architectures



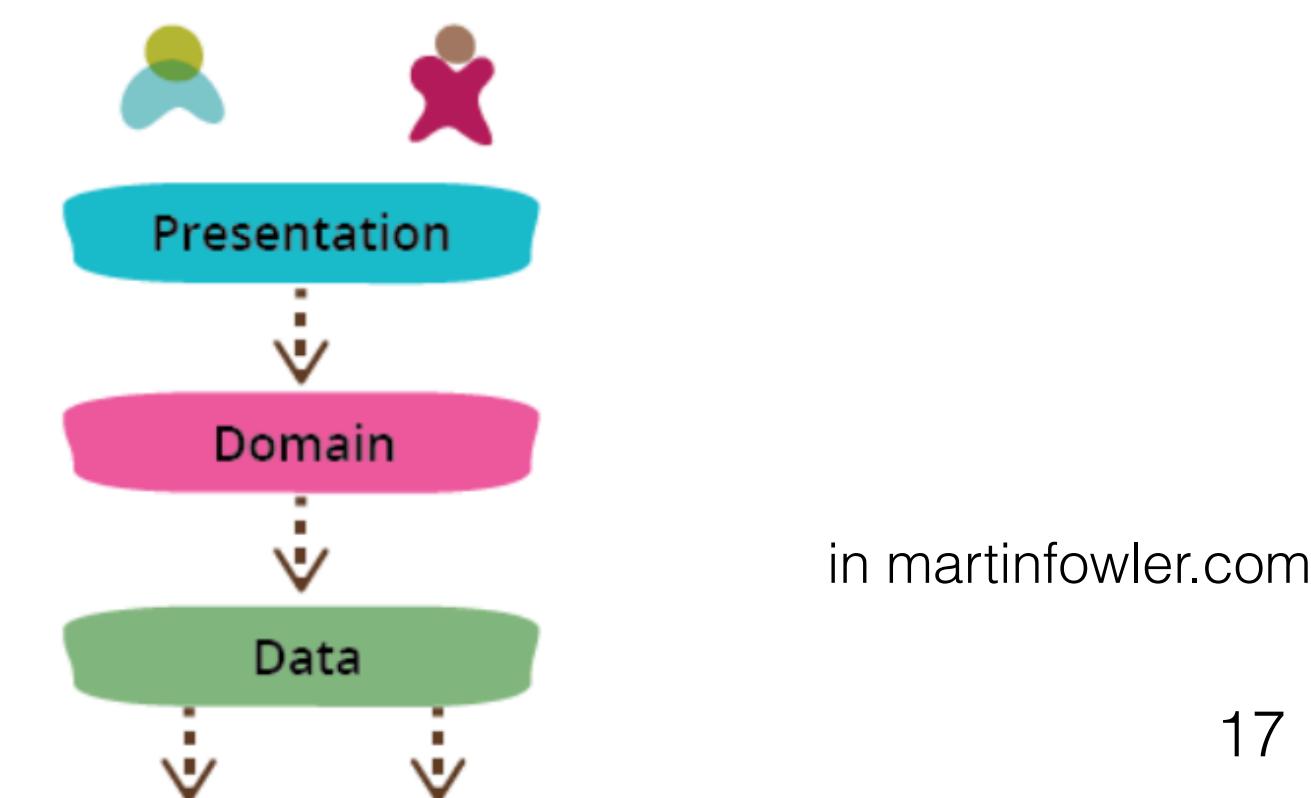
## Micro Frontends



## GUI Architectures

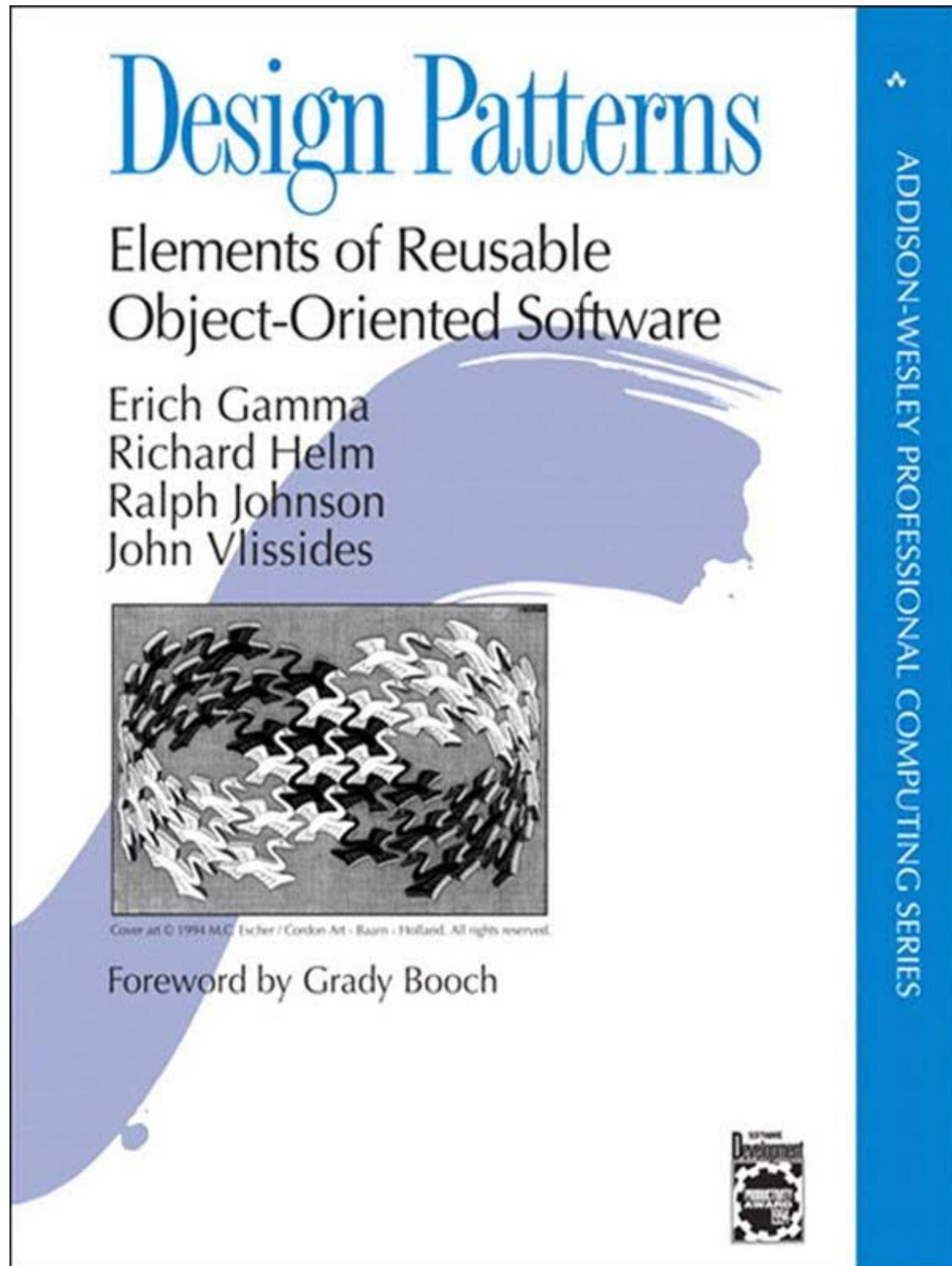
In the mid 2000s I was pursuing a couple writing projects that could have turned into books, but haven't yet made it. One was on the architecture of user interfaces. As part of this work, I drafted a description of how GUI architectures evolved, comparing the default approach of Forms and Controls with the the Model-View-Controller (MVC) pattern. MVC is one of the most ill-understood patterns in the software world

## Presentation Domain Data Layering



# (Design) Patterns for Internet Applications

- Observer (Web Controllers, Reactive web)
- Chain of Responsibility (Security filters on requests)
- Facade (Service objects, REST interfaces, ORMs)
- Builders (inner to outer representations of data)
- ...
- Frameworks implement design and architectural patterns and styles
  - Layered Architecture
  - Model View Controller
  - Inversion of control
  - REST interfaces



# Software Frameworks for Internet Applications

---

- provide **re-usable code** (as libraries)
- provides **controlled and managed resources**
  - e.g. transactions, log, security
- introduce **abstraction layers**
  - to hide complexity of concrete execution scenarios (hardware/software configuration)
  - Sometimes by scaffolding code (does not evolve well)
- support **test driven development** and **code evolution**
- They work by explicit **configuration** or by **conventions**
- **Improve the overall quality! (correction, maintainability, extensibility)**



Project

[Maven Project](#)[Gradle Project](#)

Language

[Java](#)[Kotlin](#)[Groovy](#)

Spring Boot

[2.2.0 M5](#)[2.2.0 \(SNAPSHOT\)](#)[2.1.9 \(SNAPSHOT\)](#)[2.1.8](#)

Dependencies



Start projects with

#### Developer Tools

##### Spring Boot DevTools

Provides fast application restarts, LiveReload, and configurations for enhanced development experience.



##### Lombok

Java annotation library which helps to reduce boilerplate code.



##### Spring Configuration Processor

Generate metadata for developers to offer contextual help and “code completion” when working with custom configuration keys (ex.application.properties/.yml files).



#### Web

##### Spring Web

Build web, including RESTful, applications using Spring MVC. Uses Apache Tomcat as the default



##### Spring Reactive Web

Build reactive web applications with Spring WebFlux and Netty.



##### Rest Repositories

Exposing Spring Data repositories over REST via Spring Data REST.



# Software Frameworks for Internet Applications

- provide **re-usable code** (as libraries)
- provides **controlled and managed resources**
  - e.g. transactions, log, security

```
UserTransaction utx = entityManager.getTransaction();
try {
    utx.begin();
    businessLogic();
    utx.commit();
} catch(Exception ex) {
    utx.rollback();
    throw ex;
}
```

scenario (and evolve well)

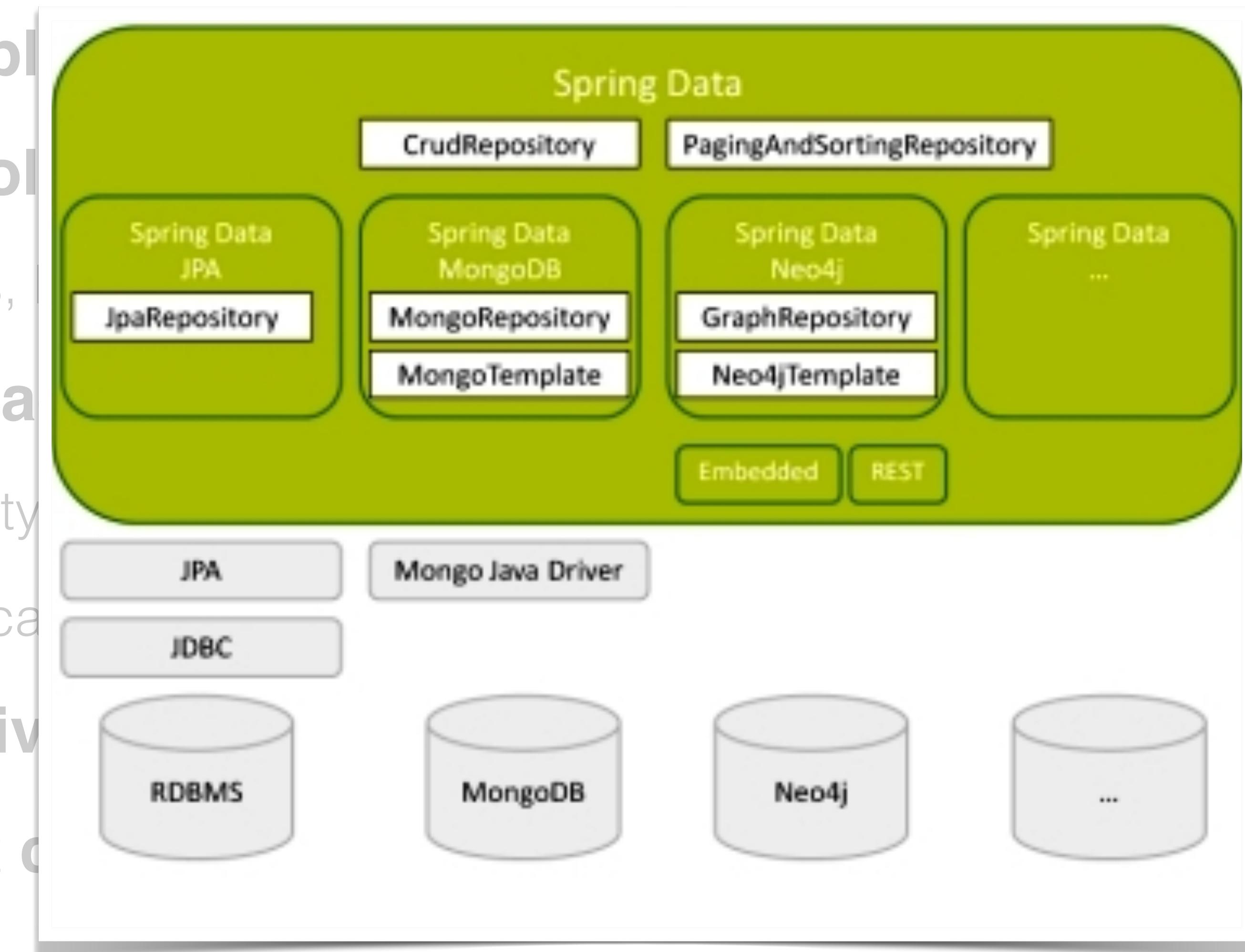
```
@Transactional
public void businessLogic() {
    ... use entity manager inside a transaction ...
}
```

- it's repetitive and error prone
- any error can have a very high impact
- errors are hard to debug and reproduce
- this decreases the readability of the code base
- What if this method calls another transactional method?

<https://dzone.com/articles/how-does-spring-transactional>

# Software Frameworks for Internet Applications

- provide **re-usability**
- provides **control**
  - e.g. transactions, security
- introduce **abstraction**
  - to hide complexity
  - Sometimes by scaling
- support **test driven development**
- work by explicit configuration



<https://www.infoq.com/articles/spring-data-intro/>

# A spectrum of frameworks for a spectrum of domains

---

- Web Frameworks
- Data manipulation Frameworks
- Resource Oriented Frameworks (REST)
- Process Oriented Frameworks
- Client-side frameworks

# Software Frameworks for Internet Applications

---

- Examples of Web Frameworks:
  - Ruby on Rails, Django and Python, Spring and Java, Cake and PHP, nodeJS, Meteor, Revel and Go
- Examples of Client Frameworks:
  - AngularJS, React, Vue, Lightweight form
- Examples of Data Frameworks:
  - LINQ, Hibernate (JPA), ...
- Examples of Web Service Frameworks/Languages:
  - WS-BPEL...
- Examples of Multi-tier Languages:
  - Ocaml (w/ Ocsigen), Elm, LINKS, UrWeb, Loom

# Software Frameworks for Web Applications

---

- Python (+Django)
  - Easy-to-learn programming language
  - Easy-to-use data structures
  - Available libraries



# Software Frameworks for Web Applications

---

- Based on Ruby (dynamically typed language)
  - Implements the MVC architectural pattern
  - Pattern components assembled by **conventions** on folders, filenames, and language identifiers
- Very flexible programming language
  - Everything is “re-programmable”
- Rails is a versatile tool
  - Support for scaffolding, migrating code and data, and TDD
- Convention over configuration (even more)
- Big community
  - Big pool of top-of-the-line gems



# Software Frameworks for Web Applications

- Java + J2EE / Spring / Play
- Most used programming language
  - Statically typed and dynamically assembled
  - Well known
  - Easy to start web development
- Huge amount of ready-to-use libraries (Beans)
- Industrial grade efficient implementations
  - Beans framework (MVC is just a module - webmvc)
  - Patterns are assembled **programmatically**, or by XML **configuration** files



# Software Frameworks for Web Applications

---

- Elixir + Phoenix is a web development framework written in Elixir which implements the server-side Model View Controller (MVC) pattern.
- Provides high developer productivity and high application performance
- Scaffolding tools like Rails and Django
- Provides LiveView
  - based on web sockets
  - efficiently handle cross border events
  - efficiently refresh web pages based on server side templates

# Software Frameworks for Web Applications

- Spring + Kotlin
- Advantages:
  - It's Completely Interoperable With Java
  - It's (way) More Concise Than Java
  - Safer Code
  - It Comes With a Smarter and Safer Compiler
  - It's Easier to Maintain
  - It's Been Created to Boost Your Productivity
  - It "Spoils" You with Better Support for Functional Programming
  - It Has Null in Its Type System



<https://dzone.com/articles/what-are-the-biggest-advantages-of-kotlin-over-jav>

<https://spring.io/blog/2017/01/04/introducing-kotlin-support-in-spring-framework-5-0>

# Jobs for Internet Applications

A **software architect** is a **software developer** expert who makes high-level design choices and dictates technical standards, including **software** coding standards, tools, and platforms.



[www.roberthalf.com](http://www.roberthalf.com)

**Software architect - Wikipedia**  
[https://en.wikipedia.org/wiki/Software\\_architect](https://en.wikipedia.org/wiki/Software_architect)

[>About Featured Snippets](#) [! Feedback](#)



[Gift This Course](#) [Wishlist](#)

## Go Full Stack with Spring Boot and React

Build Your First Full Stack Application with React and Spring Boot. Become a Full Stack Web Developer Now!

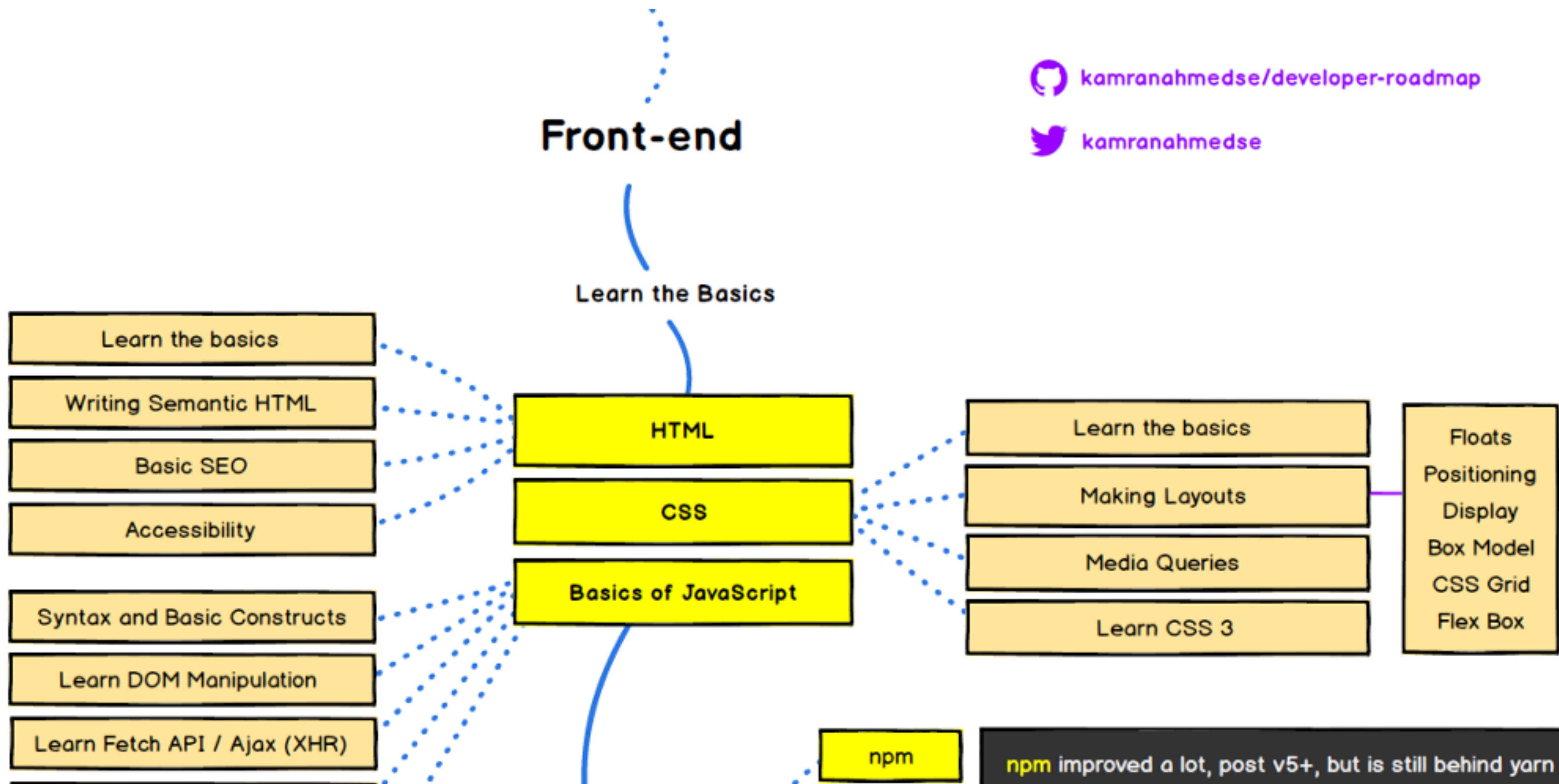
★★★★★ 4.5 (378 ratings) 1,918 students enrolled

Created by in28Minutes Official Last updated 8/2019 English English

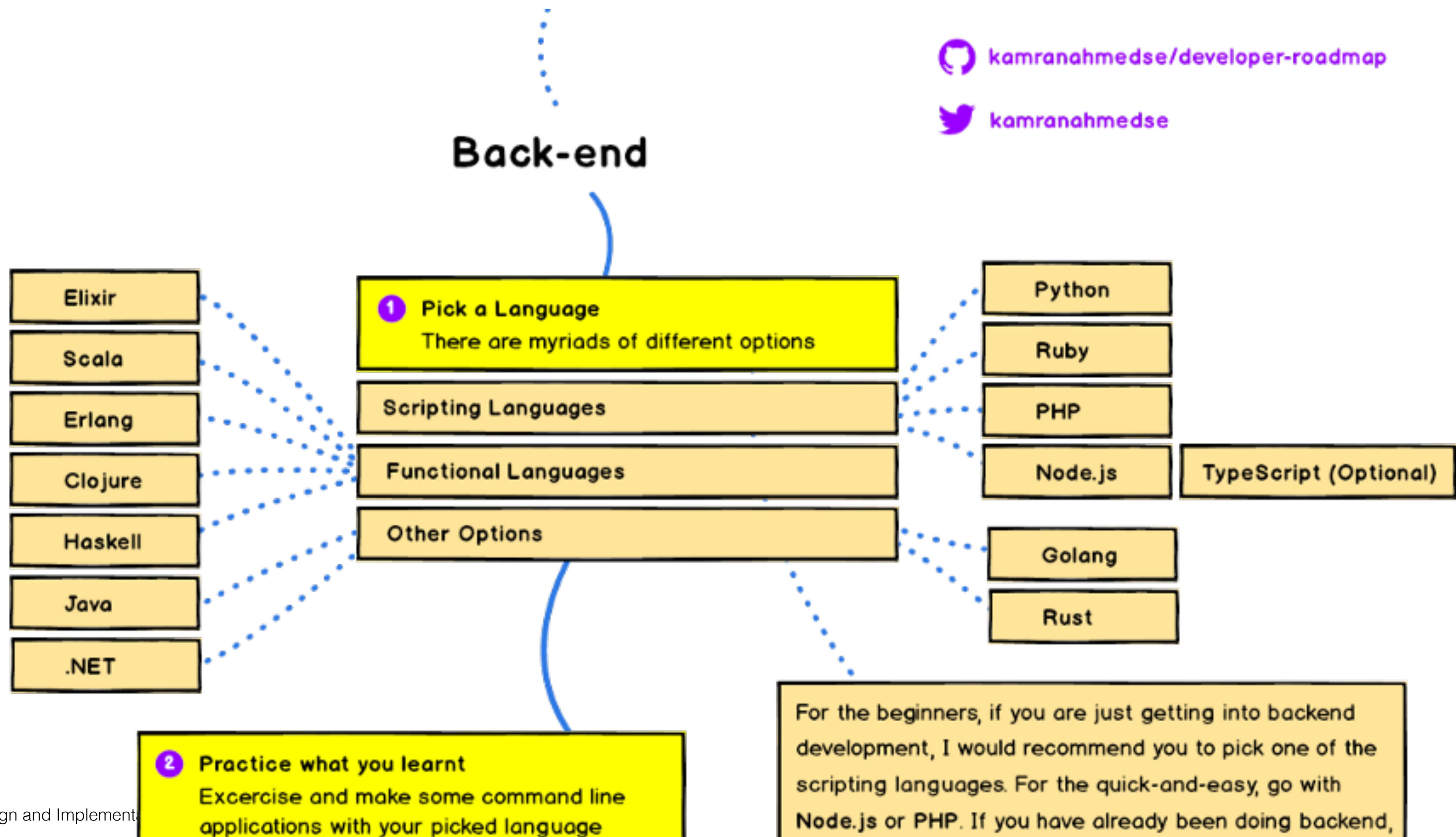


Preview this course

# Programming Languages for Internet Applications



# Programming Languages for Internet Applications



# Development Methods for Internet Applications

---

- Test Driven Development
  - Founded as part of the “extreme programming (XP)” methodology (1999)
  - Part of the Agile methodology
  - Steps:  
Add a test; Run all tests and see if the new test fails; Write the code; Run tests; Refactor code; Repeat
- Behaviour Driven Development
  - Tests are complete examples
  - Generic Tests and Test Generation  
(e.g. QuickCheck)

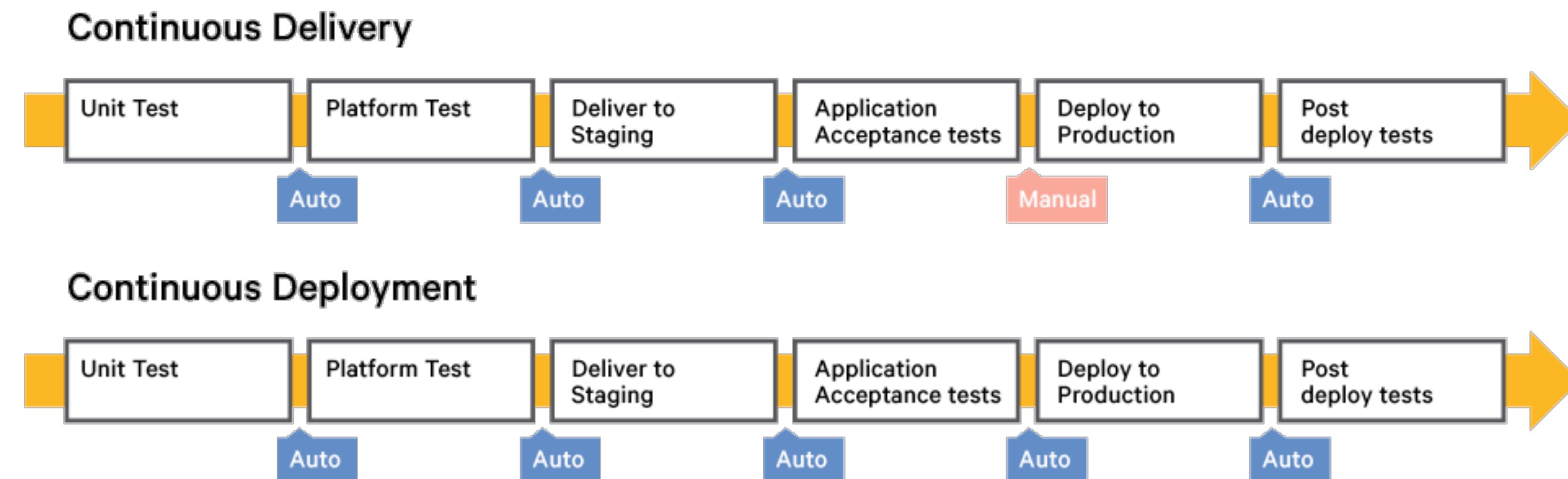
# Deployment Methods for Internet Applications

- Software development is increasingly competitive
- Any mistake can be extremely expensive
- Pressure is on to deliver fast and change even faster
- Companies deploy software at an astonishing pace:
  - Amazon: “every 11.7 seconds”
  - Netflix: “thousands of times per day”
  - Facebook: “bi-weekly app updates”



# Deployment Methods for Internet Applications

- Processes and Methods for software construction and software deployment (DevOps)
- Specification and development methods
- Testing tools and toolchains
- Validation and Verification techniques



# Summary

---

# Course Overview

# Internet Applications Design and Implementation

---

We focus on the **principles and concepts on the development of Internet applications**.

The syllabus follows an approach based on the fundamentals of software development based on **web and service oriented architectural patterns, advanced modularity mechanisms, data persistency abstractions, good development practices, performance concerns, and validation techniques**.

Lectures run along **practical assignments** and the **development of a running project** using frameworks, languages, and programming tools for Internet Applications that ensure the safety and compliance of the solution with relation to a specification

# Goals: To Know

---

- Essential aspects of **architectural patterns** for inversion of control and software architectures specific for Internet Applications.
- **Principles of the development** of web applications and single page web applications.
- Mechanisms of **specifying and implementing web services** and web service orchestrations.
- **Internal structure** of an Internet **browser** and its **client applications**.
- Principles of **data-centric** and **user-centric development** in the context of Internet applications.
- Main **data abstraction** mechanisms used in Internet applications.
- Major performance **pitfalls** of Internet applications and their workarounds.
- Main specification and implementation mechanisms for **security policies in Internet Applications**.

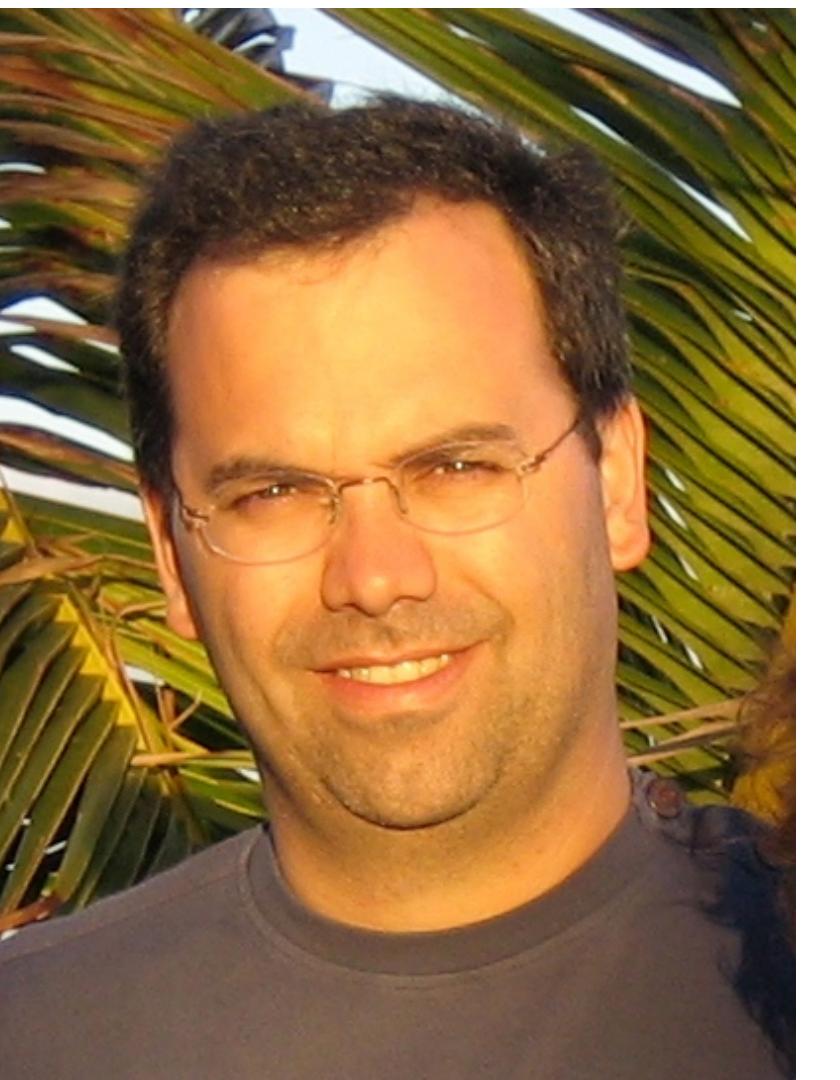
# Goals: To Do

---

- **Use development frameworks** that implement architectural styles for Internet applications.
- **Specify and build** web and cloud **applications** to support thin, flat, and native clients.
- **Specify and build** client **applications with reactive and rich behaviour**.
- **Implement authentication mechanisms** and **specify** the core **security rules** of an Internet Application
- Specify and efficiently use abstraction data layers such as **Object Relational Mappings** in Internet applications.
- **Design and deploy** Internet Applications that are efficient and maintainable.

# Team

---



João Costa Seco



Eduardo Geraldo

# Logistics (Plan)

---

- Weekly pre-recorded YouTube videos (approximately 1h per week)
- Interactive discussions (Tue. 15h-16h) — must see videos first
- Running project developed along the semestre (partial deliveries)
- Online Labs (Introductory Video + Q&A on Discord/Zoom)
- One-on-one Online Hours (by appointment)
- Resources
  - Youtube (lecture and demo videos)
  - Bitbucket (slides, assignments, started code, submission system, pipelines)
  - Discord (direct contact, conversation, questions)
  - Piazza (structured answers, announcements) — Check Piazza for all the links needed.

# Evaluation

---

- Written evaluation component (50%) — 2 Tests or Exam
- Laboratory work component (50%)
  - TDD development of a sample Internet Application (with pipelines)
  - mandatory deliverables: (Data Model & API, Server, IFML Spec, Final)
  - a deployed bitbucket project with tags for all delivered versions (tags will be provided)

**If you don't know how to operate with git, go learn TODAY!**

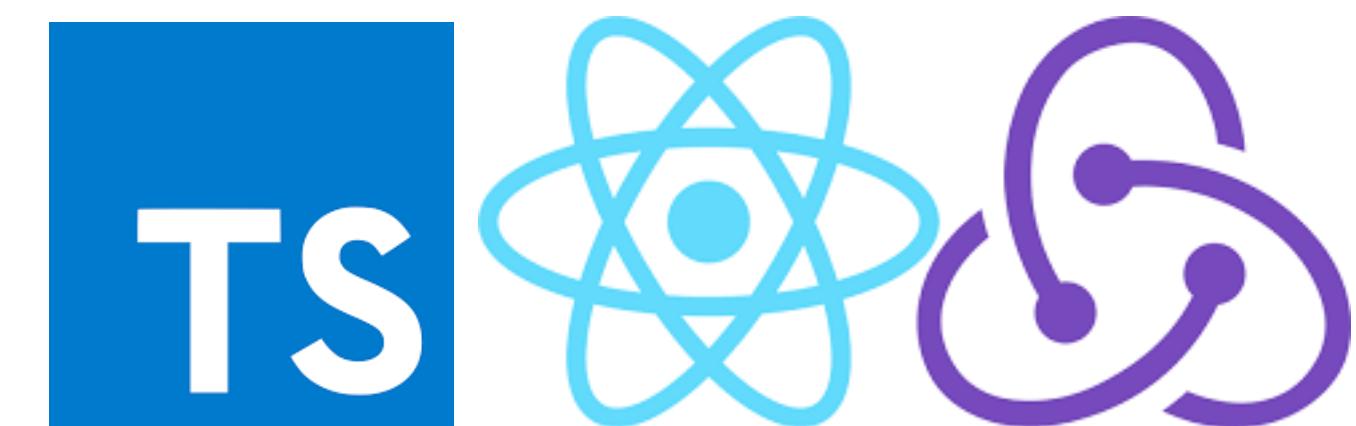
- work is evaluated for functionality, performance, method, etc.
- teams of **3** members (named commits maybe used to distinguish between members)
- deliveries include a written report, the final one includes a presentation with demo (20m)

# Lecture Plan

Week	Lecture	Lab	Project
1	Overview and Logistics	Presentation of project, data modeling	
2	Software Architecture. Service based architectures and their specification. Specification of RESTful APIS and beyond.	Implementing a webservice with a REST controller	
3	Frameworks for web and service-based applications	Designing a RESTful API using OpenAPI	RESTful API specification (9 Oct)
4	Data Abstraction. Data Access Patterns.	Implementing a Layered Architecture (Part 1)	
5	Data Abstraction in Spring (SpringData)	Implementing a Layered Architecture (Part 2)	
6	Security in Internet Applications	Implementing a Security Layer	
7	Test Driven Development	Q&A about project development	Server Component (30 Oct)
8	Guest Lecture about micro-service architectures		
9	Client Applications	Design of a pure HTML/JS client	
10	Client Frameworks and Languages	Implementing a client application using OpenAPI	
11	Specification and Implementation of Interactive Systems - IFML	Interface design with IFML	IFML design (4 Dec)
12	Model transformations	Implementation of a UI	
13	State Management	Q&A about project development	
14	Guest Lecture about client frameworks	Q&A about project development	The complete system (22 Dec)

# Lab Exercises

- Tech Stack (mandatory):
  - Server-side: SpringBoot + Kotlin + Swagger + JUnit5 + MySQL
  - Client-side: TypeScript + React + Redux
- Tools stack
  - git (bitbucket — mandatory), with pipelines (optional)
  - IntelliJ
  - httpie/curl/postman



# Project Deliveries

---

- A single project from the beginning:
  - Data-driven development of service based application, specification of data model and API
  - User-driven development of a progressive/single page client application, specification of user interaction
- A single bitbucket (mandatory) repository with client and server code, documentation, presentation and report
- Reports will include UserStories, UML/ER, IFML, OpenAPI spec, security spec
- Unit and Integration Test suite (including security aspects)
- Evaluation will cover both documentation, funcional correctness, code construction, coverage, security and performance issues.

# Project assignment 2021

---

Grant application system

# Project assignment 2021 — Grant application system

---

The project that you will implement this semester is a  
**management system for student grant applications.**

You will implement the process of submitting and evaluating **grant applications**,  
managed by the system and interfacing with several participants.

# Project assignment 2021 — Grant application system

---

The system's behaviour starts by the **creation of grant calls**, and declaration of which **data items** should be submitted in each application. A grant application to a grant call is submitted by a **student of an institution**, giving its details. The needed items include personal info and curriculum vitae items.

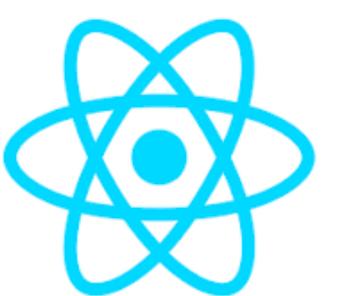
**Reviewers**, coming from institutions, are part of one or more **evaluation panels**, commanded by a **panel chair**. Reviewers submit **evaluations** to grant proposals once the submission deadline is passed and they are open for evaluation.

(more details on the system and the process as we go along...)

# Bibliography



learn play download interact  
tutorial handbook samples language spec



# Bibliography

---

- Marco Brambilla and Piero Fraternali. Interaction Flow Modeling Language – Model-Driven UI Engineering of Web and Mobile Apps with IFML. Morgan Kaufmann. 2014
- Martin L. Abbott and Michael T. Fischer, The Art of Scalability: Scalable Web Architecture, Processes and Organizations for the Modern Enterprise, Addison-Wesley Professional. 2009
- Martin Fowler. Patterns of Enterprise Application Architecture. Addison-Wesley. 2002
- Software Architecture in Practice (3rd ed). Len Bass, Paul Clements, and Rick Kazman. Addison-Wesley 2015.
- Craig Walls. Spring in Action (4th edition). Manning. 2015

[spring.io](http://spring.io)

[facebook.github.io/react/](https://facebook.github.io/react/)

[typescriptlang.org](https://typescriptlang.org)

[kotlinlang.org](https://kotlinlang.org)



# Temas de Dissertação de Mestrado

---

- Contexto Académico
  - **Advances of SNITCH in Spring.** Desenvolvimento de ferramentas de controlo de segurança para Java e Java Spring (continuação de 2 teses de mestrado) — (Equipa: João Costa Seco, Eduardo Geraldo)
  - **Linguagem para processos de negócio** implementação de um ambiente de programação para uma linguagem baseada em grafos de processos. Colaboração com a universidade de Copenhaga (continuação de 1 tese de mestrado).
- Contexto Académico-Empresarial (OutSystems)
  - diversos temas relacionados com o desenvolvimento de ferramentas de programação (abordagens baseadas em linguagens de programação: ICL, CVS). Temas sobre transformação de modelos e desenvolvimento de User-Interfaces.
- Contexto Académico-Empresarial (VORTEX/Altran)
  - diversos temas relacionados com o desenvolvimento de ferramentas de verificação de código de sistemas de tempo real.

# Internet Applications Design and Implementation

2020 - 2021

(Lab class 1)

**MIEI - Integrated Master in Computer Science and Informatics  
Specialization block**

**João Costa Seco ([joao.seco@fct.unl.pt](mailto:joao.seco@fct.unl.pt))  
Eduardo Geraldo ([e.gerald@campus.fct.unl.pt](mailto:e.gerald@campus.fct.unl.pt))**



FACULDADE DE  
CIÊNCIAS E TECNOLOGIA  
UNIVERSIDADE NOVA DE LISBOA

# Just start to model the database

---

- Use lucidchart to do a ER that covers the assignment cases
- Discuss it with the instructor, submission due in 2 weeks together with a RESTful API (starts next week).
- Establish a team of 3 students, create a bitbucket repository and share it with the instructors ([joao.seco@fct.unl.pt](mailto:joao.seco@fct.unl.pt) and [e.geraldo@campus.fct.unl.pt](mailto:e.geraldo@campus.fct.unl.pt))
- Commit a pdf and tag it (DataModel)...

# Project assignment 2021 — Grant application system

---

The project that you will implement this semester is a  
**management system for student grant applications.**

You will implement the process of submitting and evaluating **grant applications**,  
managed by the system and interfacing with several participants.

# Project assignment 2021 — Grant application system

---

The system's behaviour starts by the **creation of grant calls**, and declaration of which **data items** should be submitted in each application. A grant application to a grant call is submitted by a **student of an institution**, giving its details. The needed items include personal info and curriculum vitae items.

**Reviewers**, coming from institutions, are part of one or more **evaluation panels**, commanded by a **panel chair**. Reviewers submit **evaluations** to grant proposals once the submission deadline is passed and they are open for evaluation.

(more details on the system and the process as we go along...)

# Internet Applications Design and Implementation

## 2020 - 2021

### (Lecture 2 - Software Architecture)

**MIEI - Integrated Master in Computer Science and Informatics  
Specialization block**

**João Costa Seco ([joao.seco@fct.unl.pt](mailto:joao.seco@fct.unl.pt))**

(with previous participations of Jácome Cunha ([jacome@fct.unl.pt](mailto:jacome@fct.unl.pt)) and João Leitão ([jc.leitao@fct.unl.pt](mailto:jc.leitao@fct.unl.pt)))



FACULDADE DE  
CIÊNCIAS E TECNOLOGIA  
UNIVERSIDADE NOVA DE LISBOA

# Outline

---

- Software Architecture - Introduction
- Software Architecture for Internet Applications
  - Three-tier architecture
  - Service-based architectures
  - Microservice-based architectures
- Frameworks at the service of Software Architecture
- The architectural style REST to instantiate webservices
- Specifying webservices with OpenAPI and Spring

# Internet Applications Design and Implementation

2020 - 2021

(Lecture 2, Part 1 - Software Architecture - Introduction)

**MIEI - Integrated Master in Computer Science and Informatics  
Specialization block**

**João Costa Seco ([joao.seco@fct.unl.pt](mailto:joao.seco@fct.unl.pt))**

(with previous participations of Jácome Cunha ([jacome@fct.unl.pt](mailto:jacome@fct.unl.pt)) and João Leitão ([jc.leitao@fct.unl.pt](mailto:jc.leitao@fct.unl.pt)))

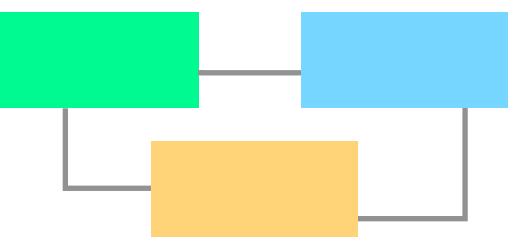


FACULDADE DE  
CIÊNCIAS E TECNOLOGIA  
UNIVERSIDADE NOVA DE LISBOA

# Software Architecture

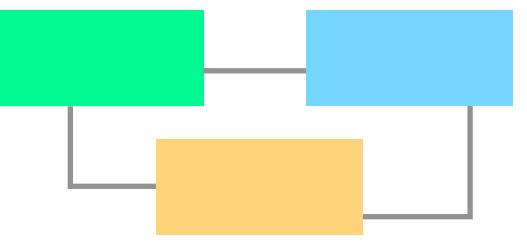
Introduction

based on the book “Software Architectures in Practice”



# Software Architecture

- What is software architecture?
- What are the benefits of using one?

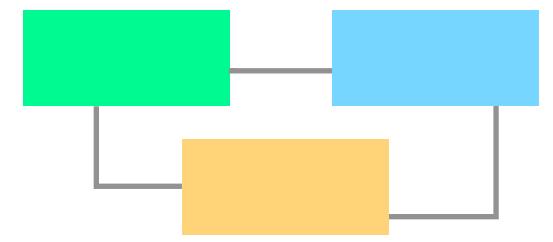


# Software Architecture

- What is software architecture?

“The software architecture of a system is the set of structures needed to reason about the system, which comprise software elements, relations among them, and properties of both.” (in Software Architectures in Practice)

- Structures can be:
  - the module decomposition structure, which divide computational responsibilities and work assignment (among teams). Identify modules or components
  - runtime structures (connectors) that deal with the communication between components (eg services)
  - organisational structures. How components are developed, tested, deployed



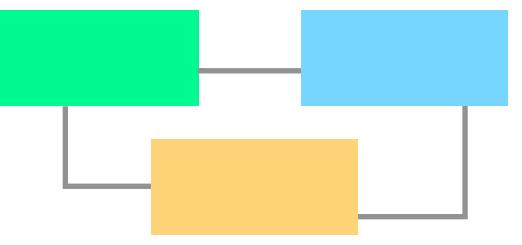
# Software Architecture...

... is a form of Abstraction  
(different views over the same system)

... is in every software system  
(from caos to tidy)

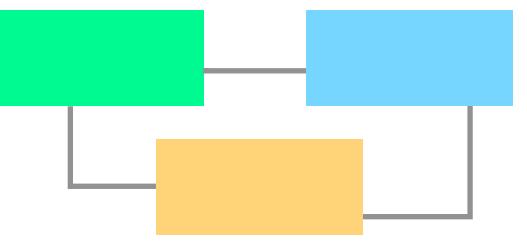
... includes Behaviour  
(names and connectors have semantics)

**Not All Architectures Are Good Architectures**



# Software Architecture (Structures)

- Module structures
  - What is the primary functional responsibility assigned to each module?
  - What are the dependencies to other software elements?
  - What modules are each module related to? by generalisation or specialisation.
- Component and connector structures
  - How do modules interact?
  - What are the shared data stores?
  - What is the data flow in the system?
  - Can the structure change? how?
  - What are the security requirements? performance bottlenecks?
- Allocation structures
  - What is the hardware/cloud infrastructure? module ownership? which are the regressions tests? etc.



# Architectural Patterns

- Pre-determined compositions of architectural elements provide strategies for solving common problems in software systems.
- Examples:
  - Layered pattern — Linear (unidirectional) dependencies between multiple elements
  - Shared-data pattern — Components and connectors to create and manipulate persistent data, connectors are languages like SQL.
  - Client-server pattern — Components: Clients and servers; Connectors: protocols and languages
  - Multi-tier pattern — A generic deployment structure of components in different infrastructures
  - Competence center — Work assignment division by expertise (eg. departments)

# Internet Applications Design and Implementation

## 2020 - 2021

(Lecture 2, Part 2 - Software Architecture - Internet Applications)

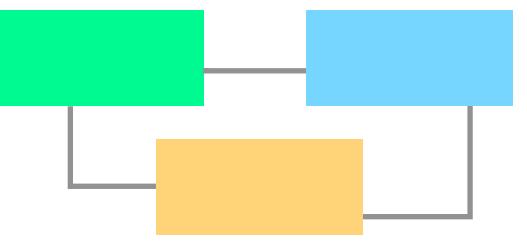
**MIEI - Integrated Master in Computer Science and Informatics  
Specialization block**

**João Costa Seco ([joao.seco@fct.unl.pt](mailto:joao.seco@fct.unl.pt))**

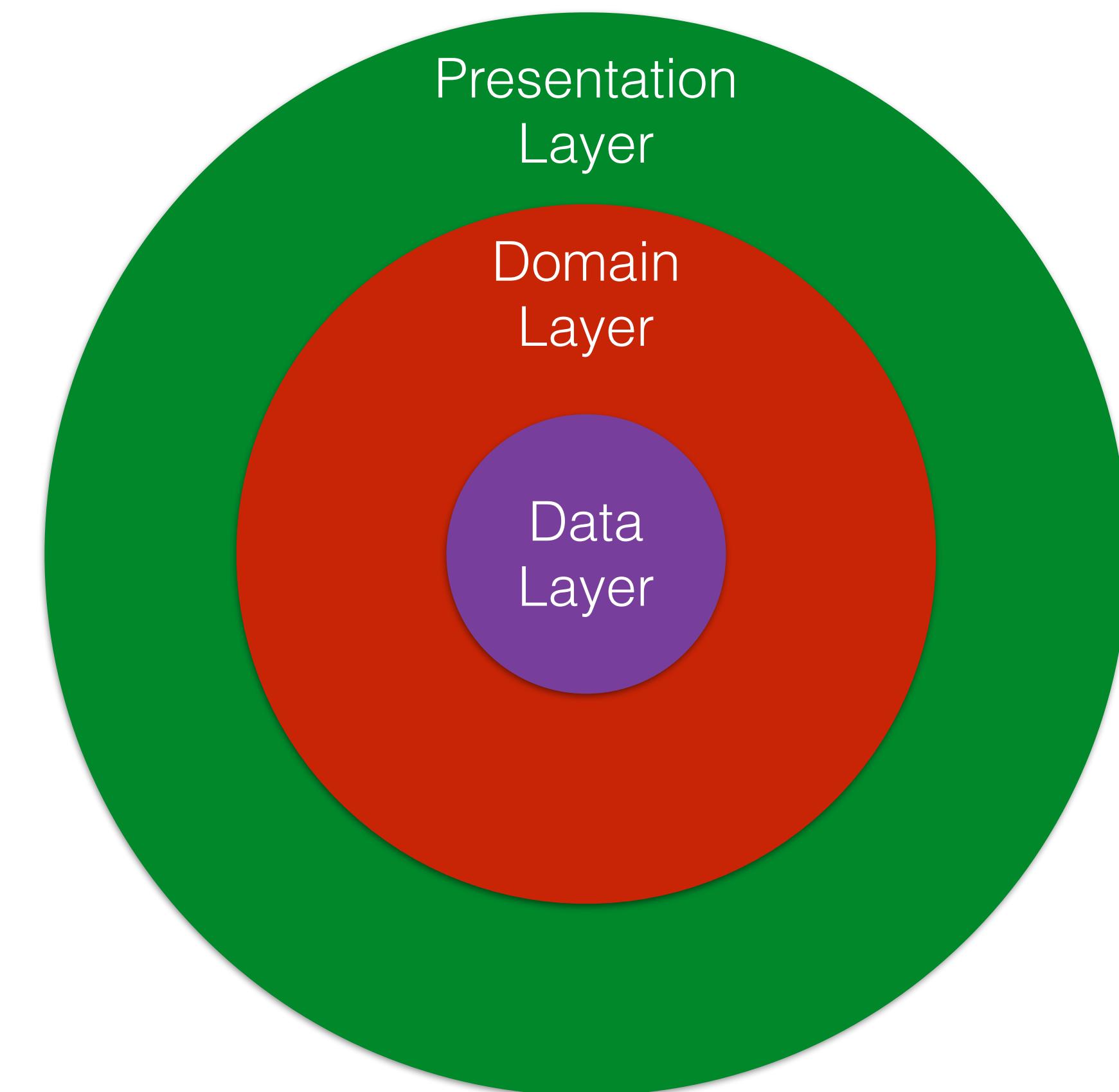
(with previous participations of Jácome Cunha ([jacome@fct.unl.pt](mailto:jacome@fct.unl.pt)) and João Leitão ([jc.leitao@fct.unl.pt](mailto:jc.leitao@fct.unl.pt)))



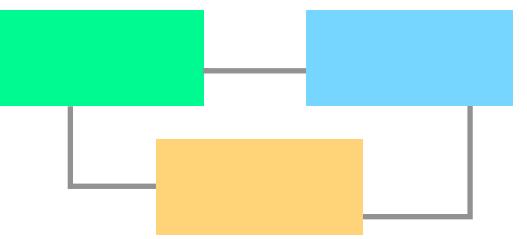
FACULDADE DE  
CIÊNCIAS E TECNOLOGIA  
UNIVERSIDADE NOVA DE LISBOA



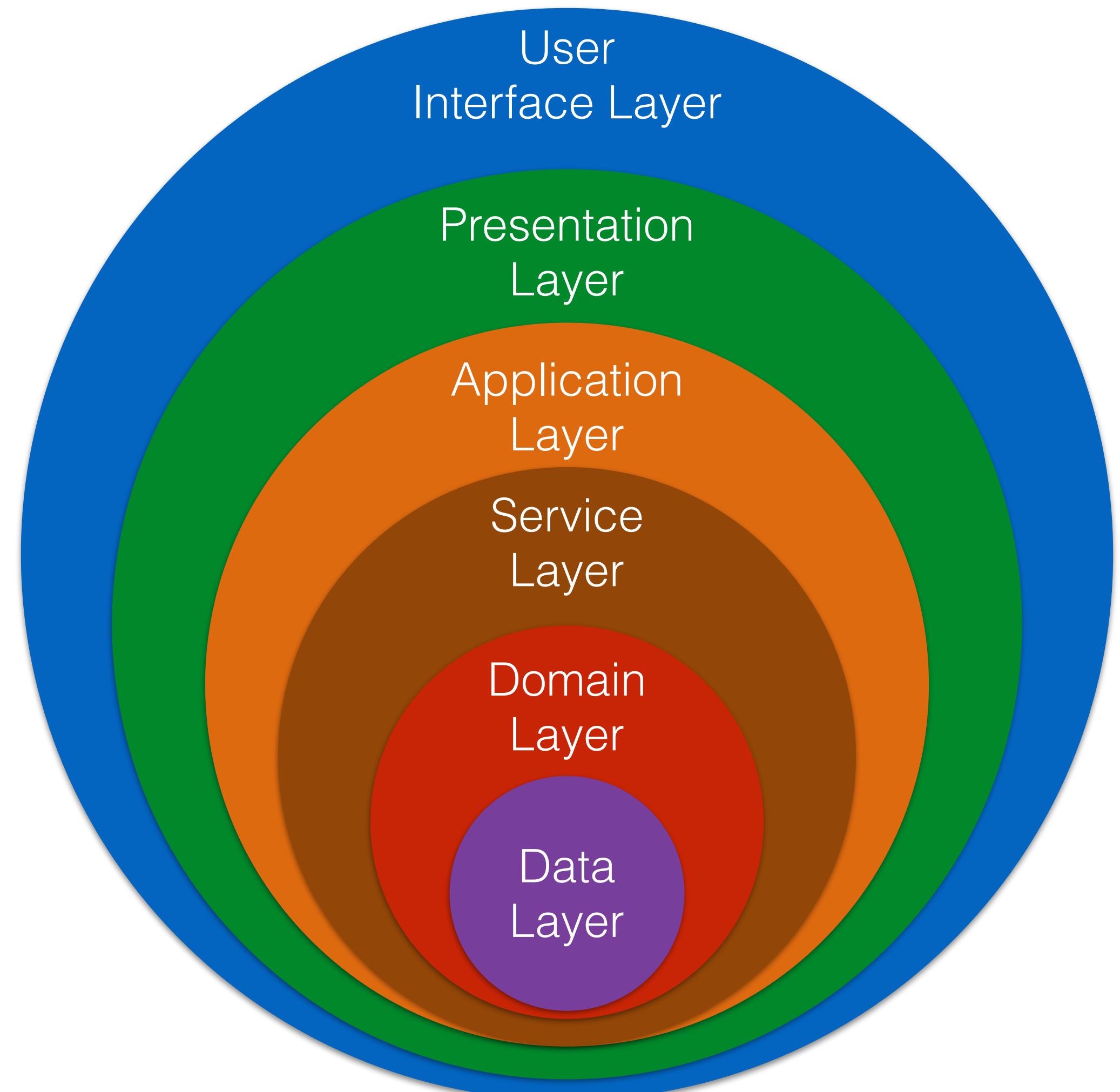
# Internet Applications are Data-Centric



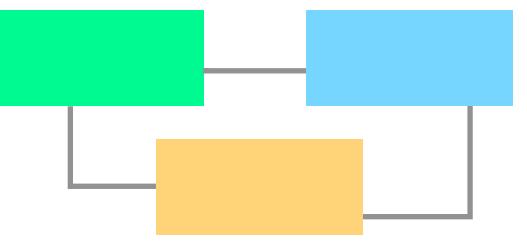
Patterns of Enterprise Application Architecture



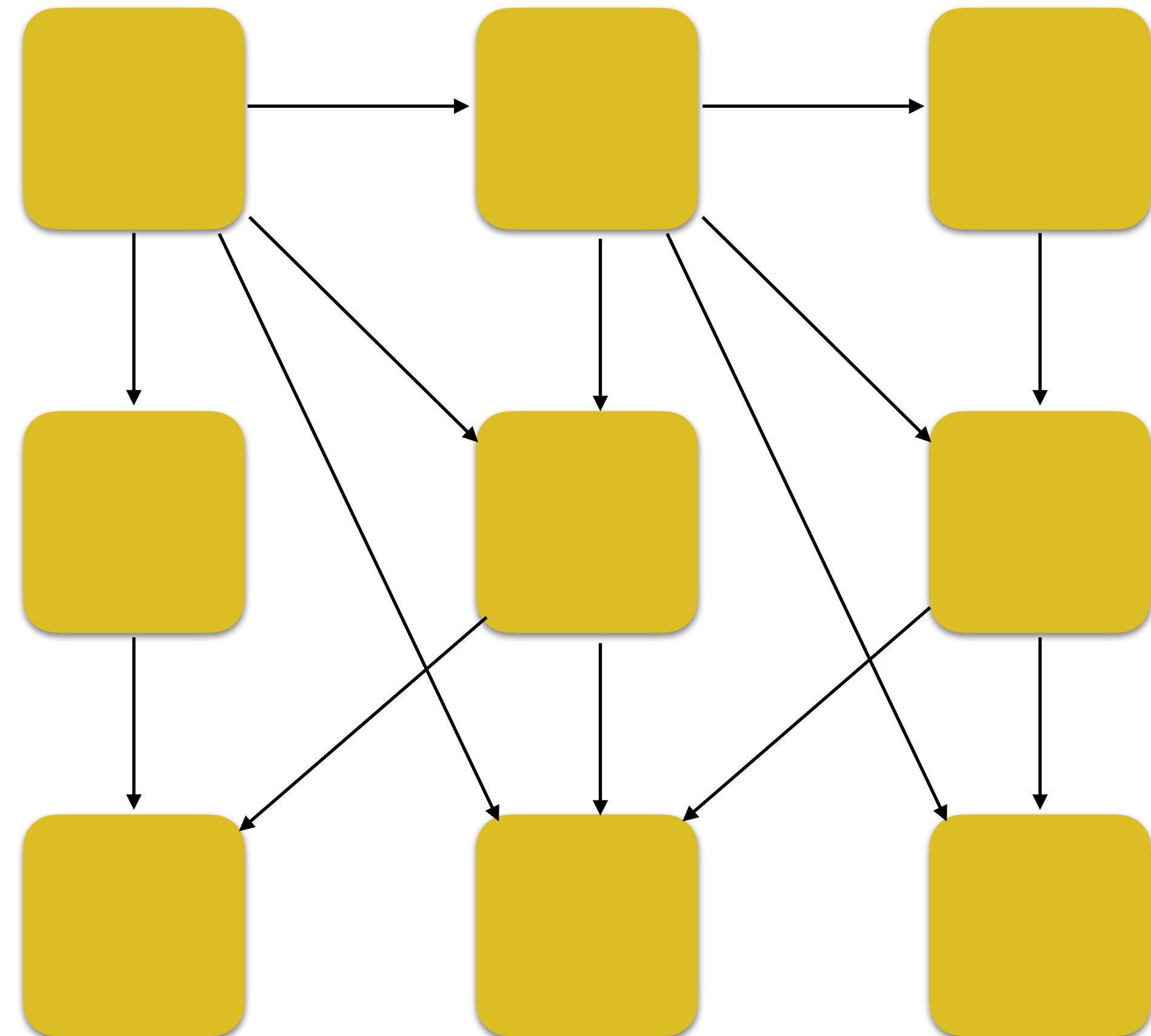
# Internet Applications are Data-Centric



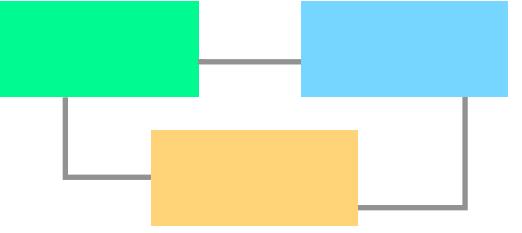
<https://dzone.com/articles/layered-architecture-is-good>



# Internet Applications are also Decentralised

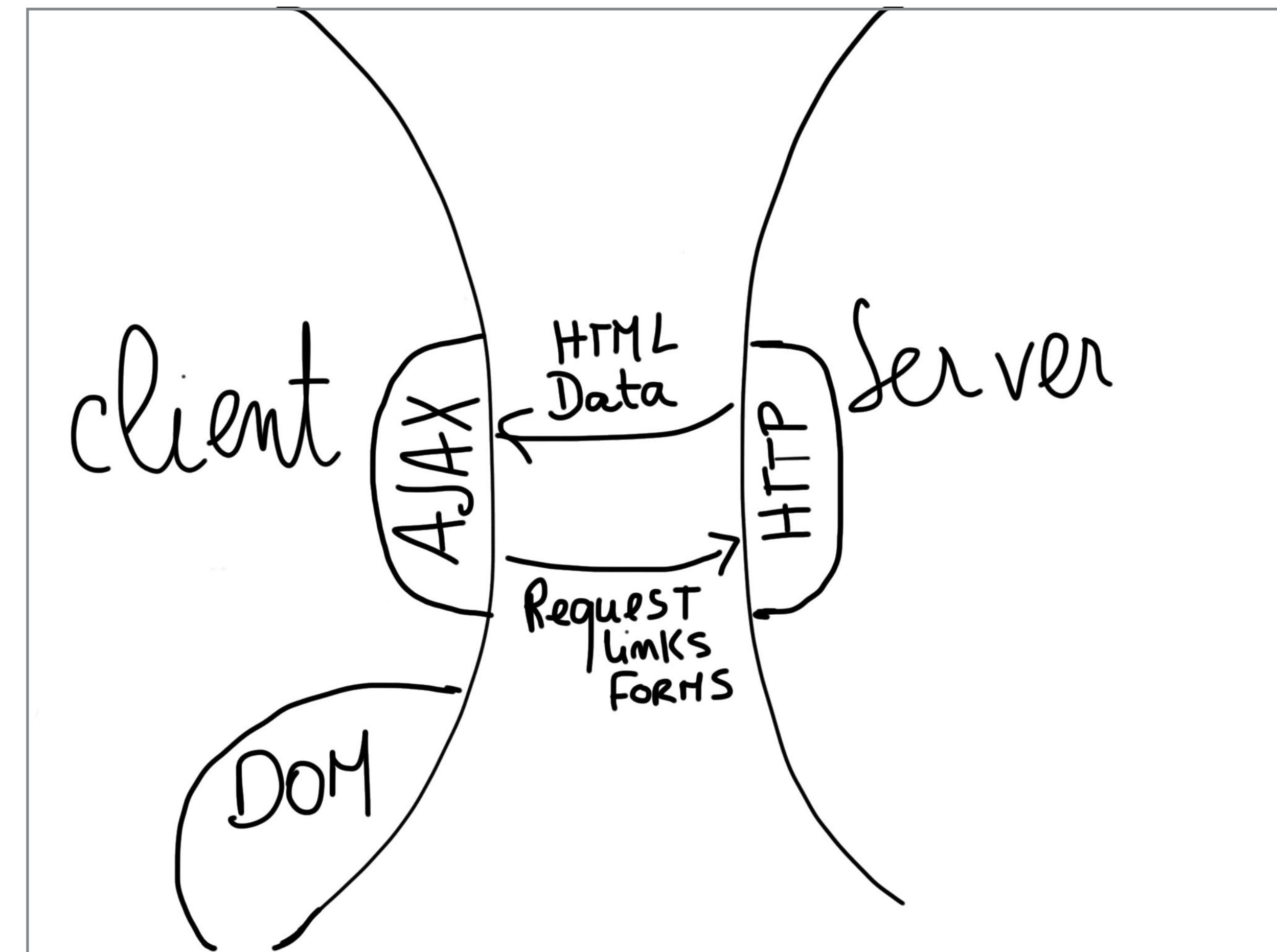


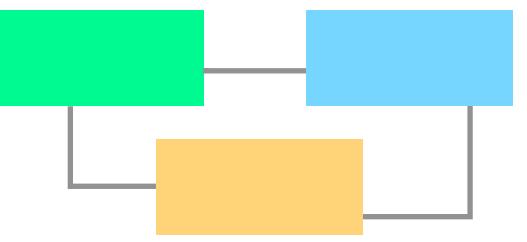
<https://dzone.com/articles/introduction-to-microservices-part-1>



# (Logical) Architecture of Web applications

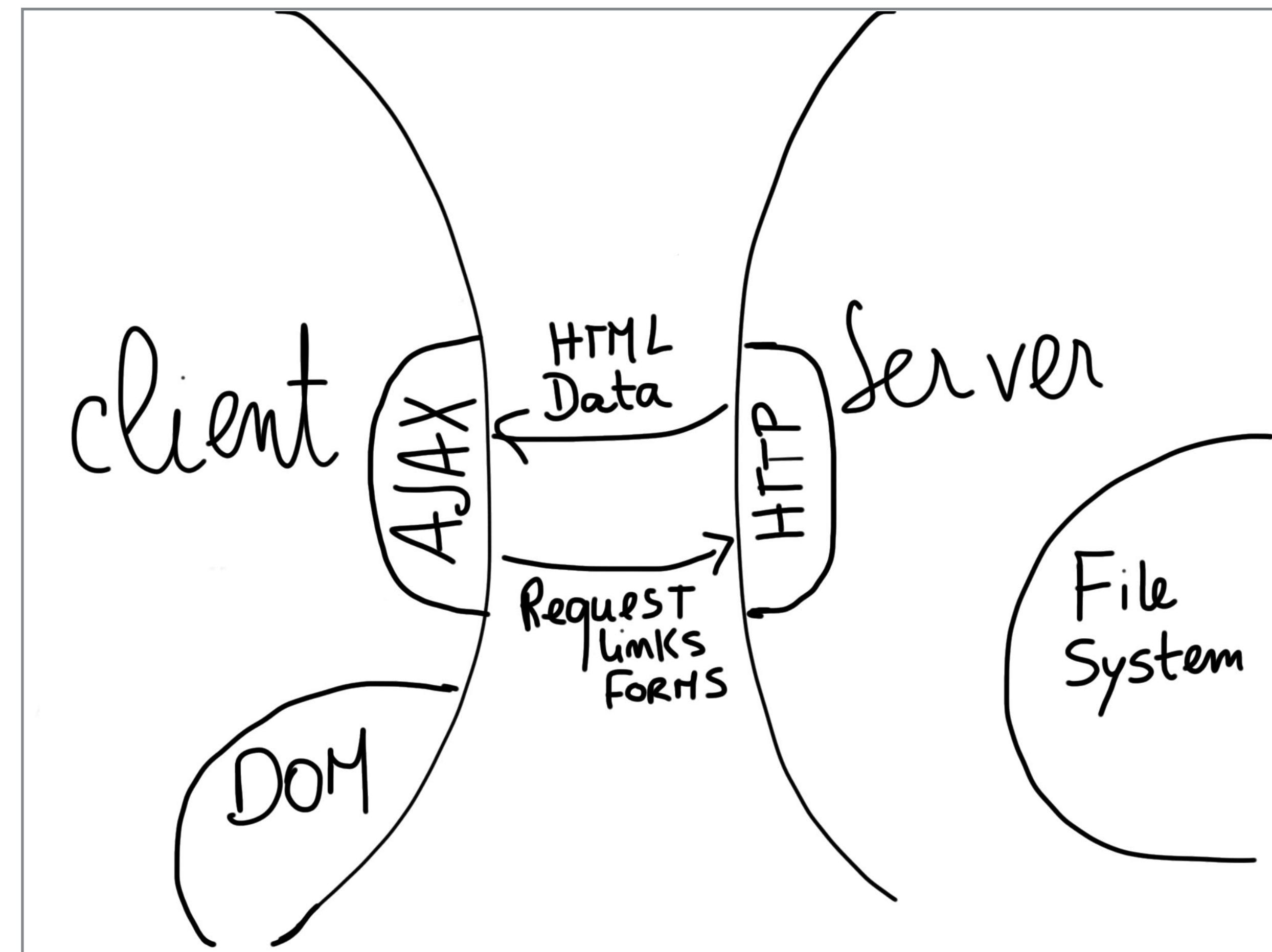
- Tech Details: Interconnection based on the HTTP protocol
  - Method, path, arguments, (a)synchrony, multi-typed response

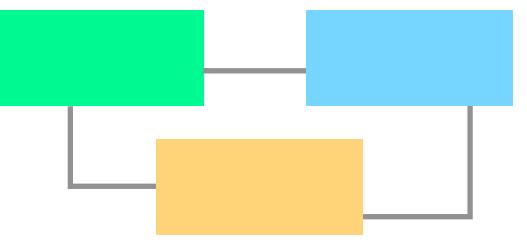




# Architecture of Web applications

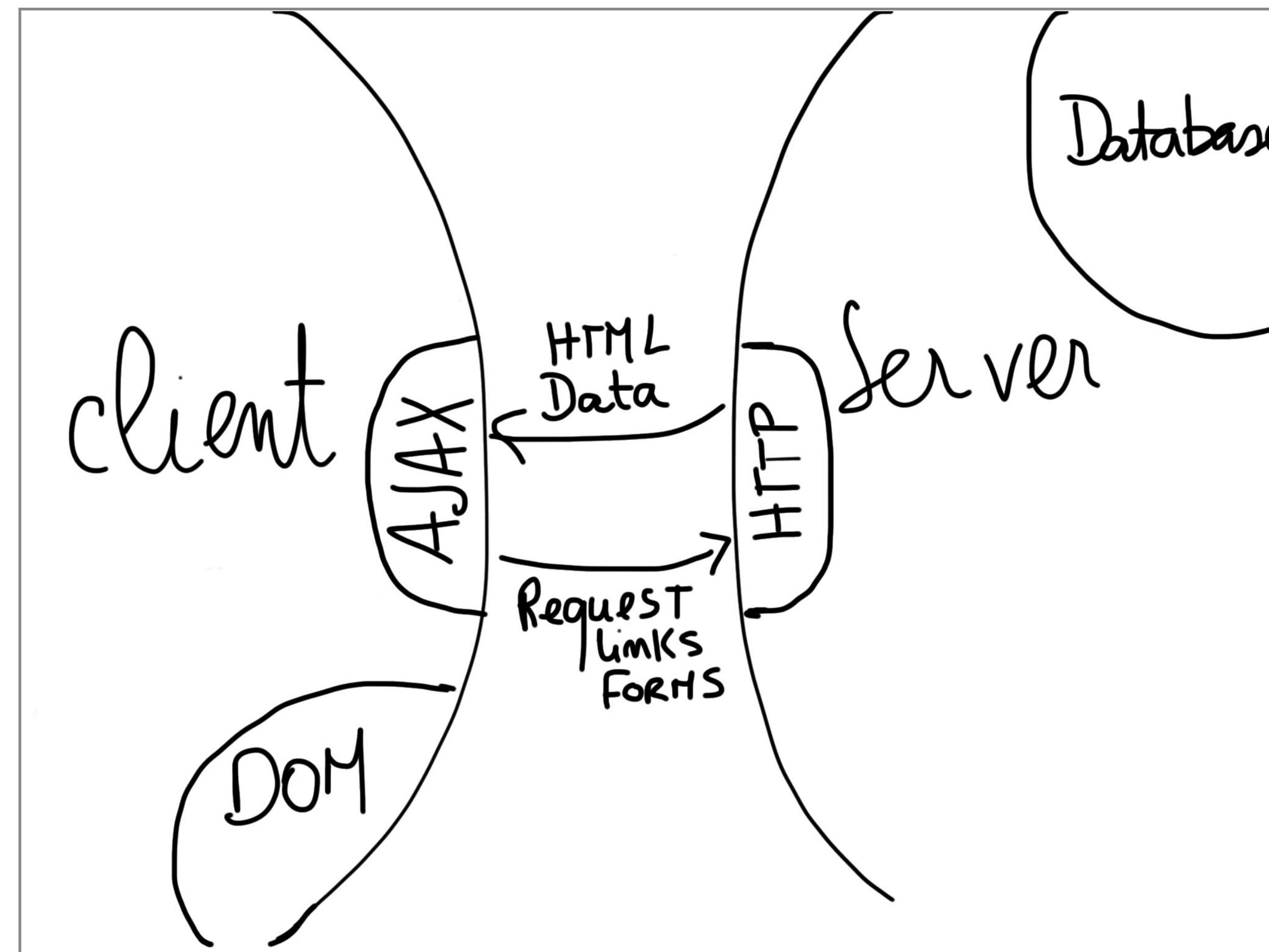
- Static HTML pages stored in the file system

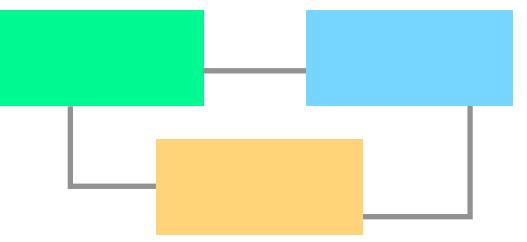




# Architecture of Web applications

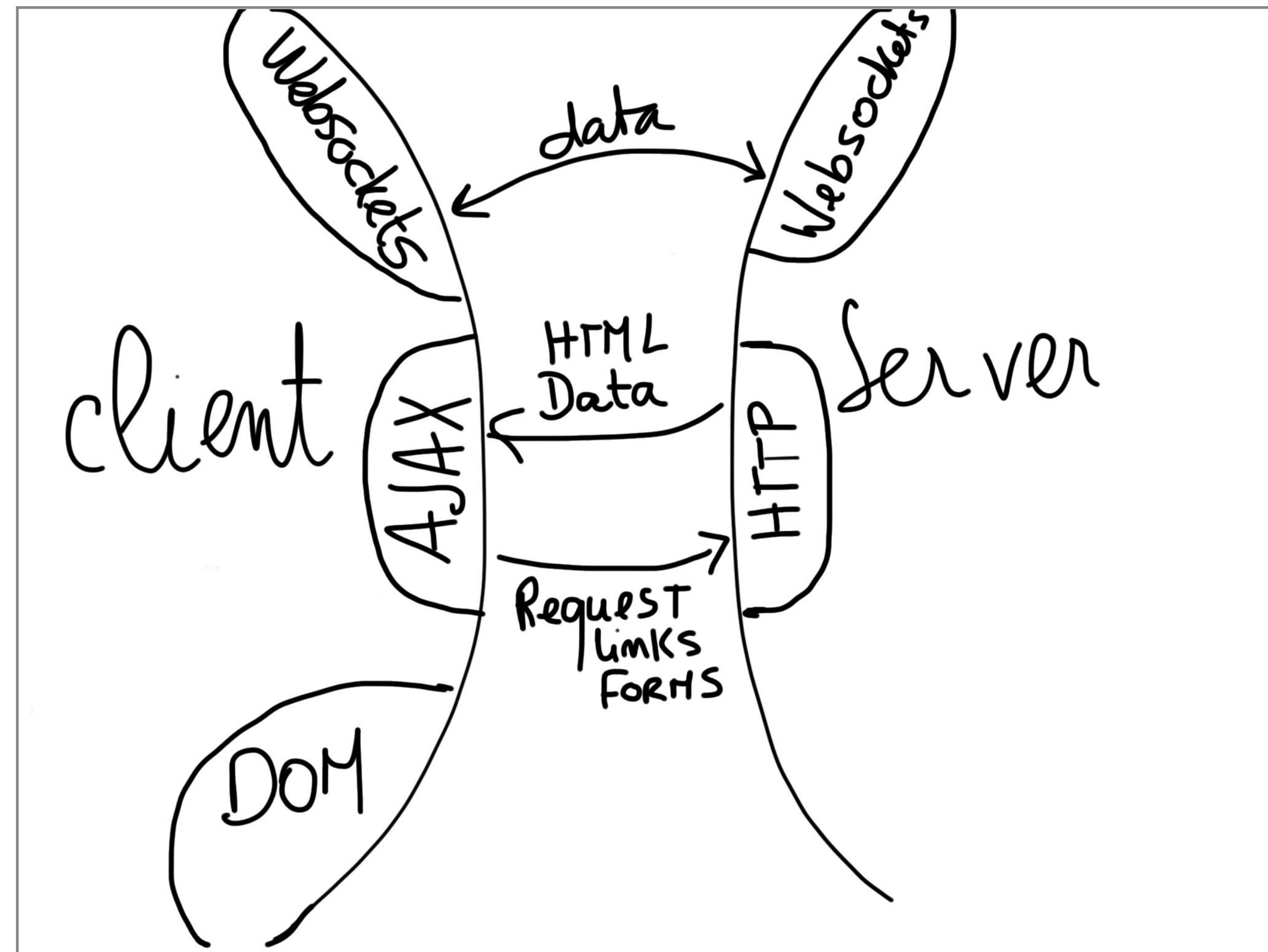
- Dynamic HTML pages based on data stored in some database.



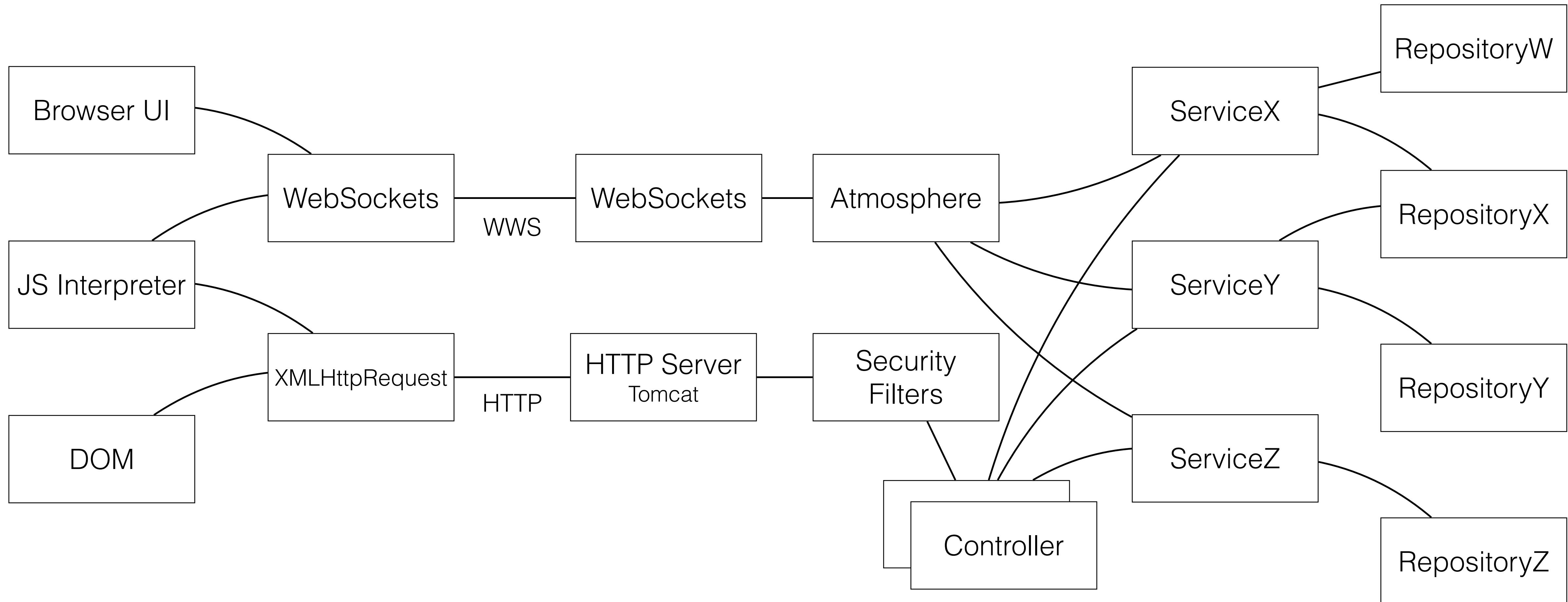
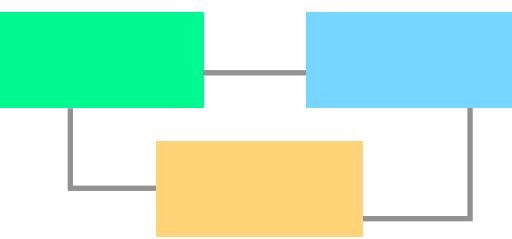


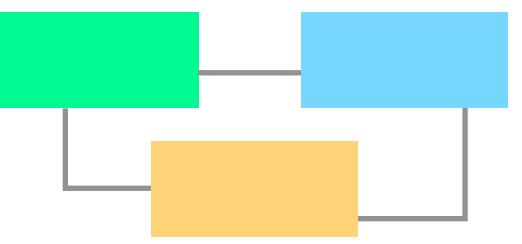
# Architecture of Web applications

- Dynamic HTML pages with permanent connection with the server to exchange data.



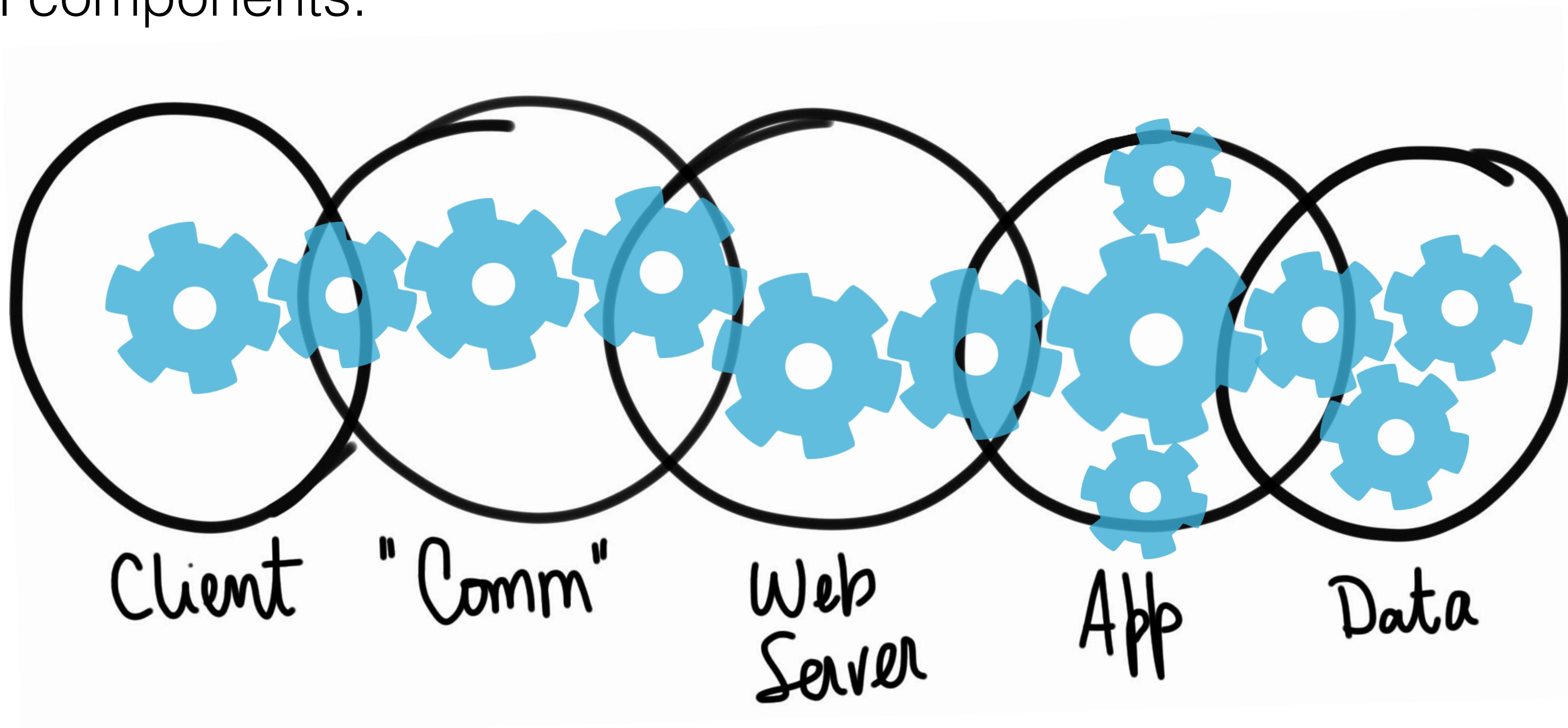
# Architecture of Web applications

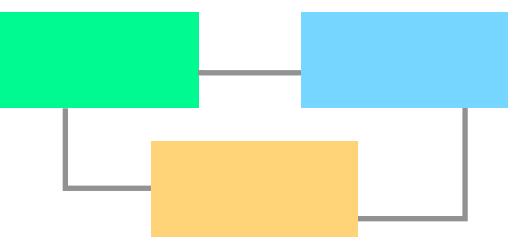




# Architecture of Web applications - The Big Picture

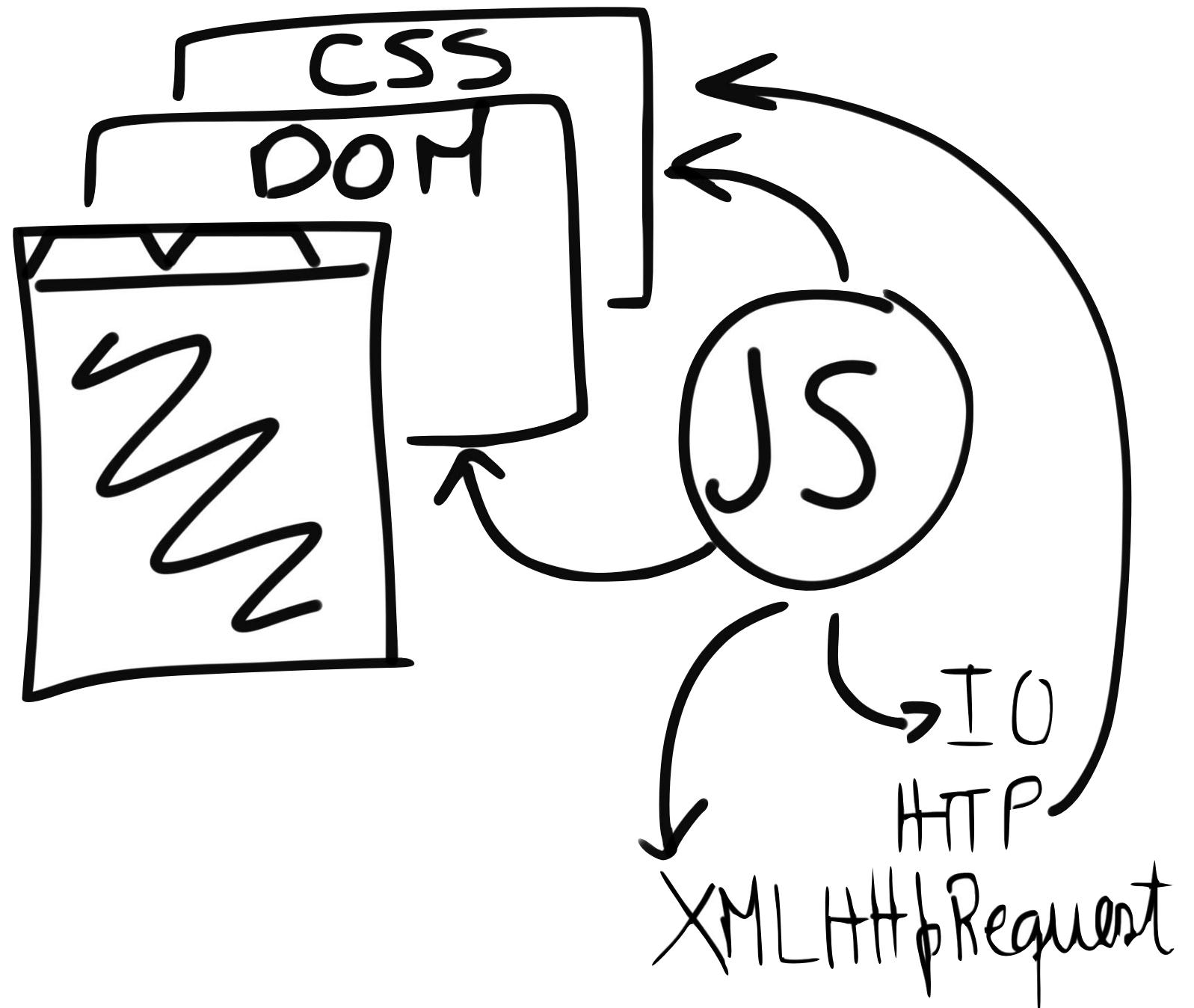
- A web application is made of code deployed to the independent and different physical components.

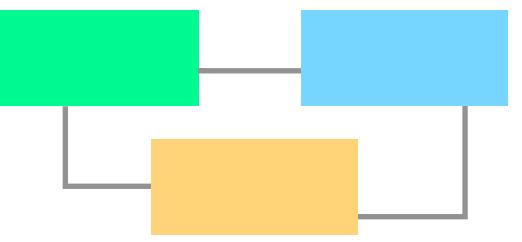




# Web client architecture

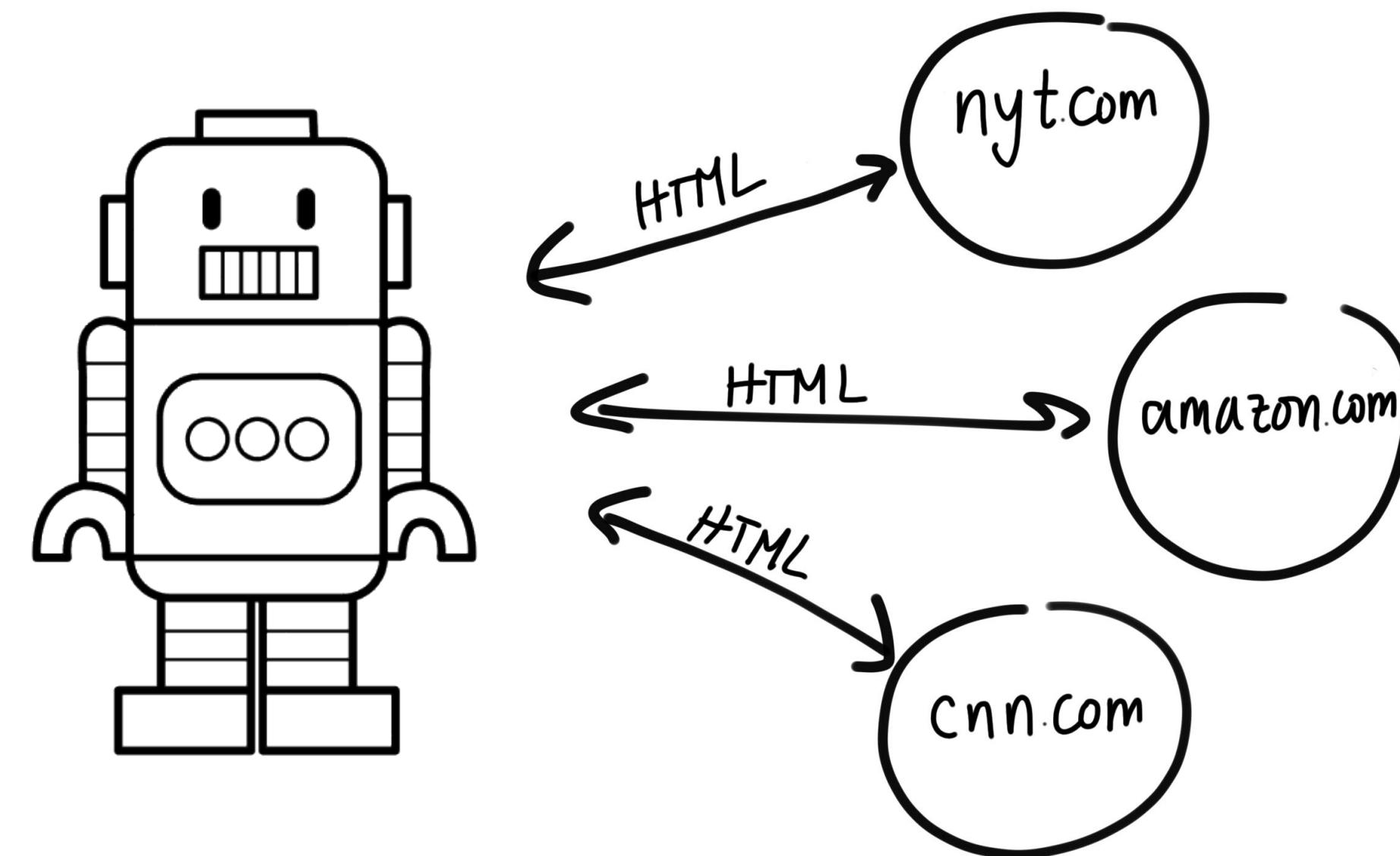
- Browser (HTML5)
  - HTML (structure and semantics)
  - CSS (style and UI behaviour)
  - JS + AJAX,  
Socket interfaces (behaviour)
  - DOM  
(the supporting data structure)
  - UI Events & callbacks  
(mechanism for dynamic structuring of behaviour)

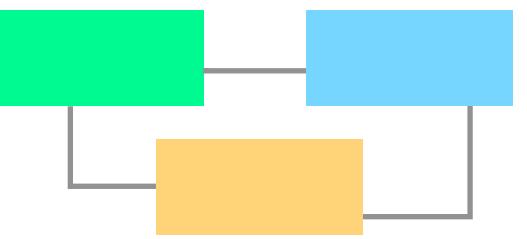




# Web client architecture

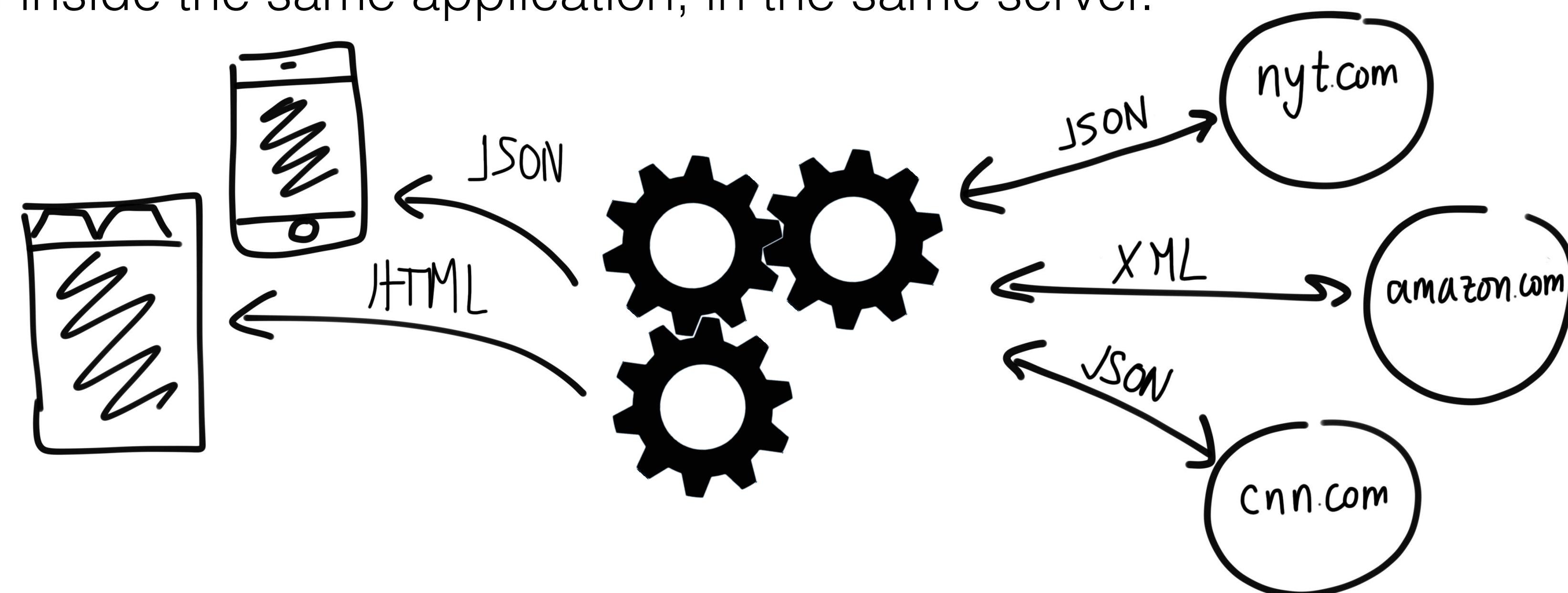
- Other kind of web clients (asking for HTML)
  - simulate web requests and sessions with web-servers
  - parse/crawl the results to extract information
  - should be built with web-services instead (if possible).

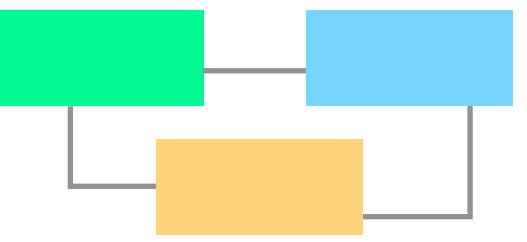




# Service based web client architecture

- Provide web content based on data providing services
  - Data can be exchanged in “machine-friendly” formats.  
(e.g. JSON, XML)
  - Combined and refurbished in HTML or data formats.
  - Even reused inside the same application, in the same server.





# Interconnection layer (low-level support)

- HTTP/1.1 (*Hypertext Transfer Protocol*) Protocol
  - Method: GET, HEAD, POST, PUT, DELETE (3 more)
  - Arguments (query string and body)
  - Multi-typed message body
  - Cookies
  - Return codes: 1XX, 2XX, 3XX, 4XX, 5XX
- Websockets (standard RFC6455 2011 - ws:// wss://)
  - supported by browsers and web servers to allow two way data communication between client and servers
- HTTP/2 approved May 2015.
  - Faster, compressed, and cyphered transmission of data
- TLS (successor of SSL)
  - Provides cryptographic support for web communications (handshake+symmetric crypto)

1xx Informational  
**100** Continue  
**101** Switching Protocols  
**102** Processing  
2xx Success  
**200** OK  
**201** Created  
**202** Accepted  
**203** Non-authoritative Information  
**204** No Content  
**205** Reset Content  
**206** Partial Content  
**207** Multi-Status  
**208** Already Reported  
**226** IM Used  
3xx Redirection  
**300** Multiple Choices  
**301** Moved Permanently  
**302** Found  
**303** See Other  
**304** Not Modified  
**305** Use Proxy  
**307** Temporary Redirect  
**308** Permanent Redirect  
4xx Client Error  
**400** Bad Request  
**401** Unauthorized  
**402** Payment Required  
**403** Forbidden  
**404** Not Found  
**405** Method Not Allowed  
**406** Not Acceptable  
**407** Proxy Authentication Required  
**408** Request Timeout  
**409** Conflict  
**410** Gone  
**411** Length Required  
**412** Precondition Failed  
**413** Payload Too Large  
**414** Request-URI Too Long  
**415** Unsupported Media Type  
**416** Requested Range Not Satisfiable  
**417** Expectation Failed  
**418** I'm a teapot  
**421** Misdirected Request  
**422** Unprocessable Entity  
**423** Locked  
**424** Failed Dependency  
**426** Upgrade Required  
**428** Precondition Required  
**429** Too Many Requests  
**431** Request Header Fields Too Large  
**444** Connection Closed Without Response  
**451** Unavailable For Legal Reasons  
**499** Client Closed Request  
5xx Server Error  
**500** Internal Server Error  
**501** Not Implemented  
**502** Bad Gateway  
**503** Service Unavailable  
**504** Gateway Timeout  
**505** HTTP Version Not Supported  
**506** Variant Also Negotiates  
**507** Insufficient Storage  
**508** Loop Detected  
**510** Not Extended  
**511** Network Authentication Required  
**599** Network Connect Timeout Error

<https://httpstatuses.com/>

# Web server / App server architecture

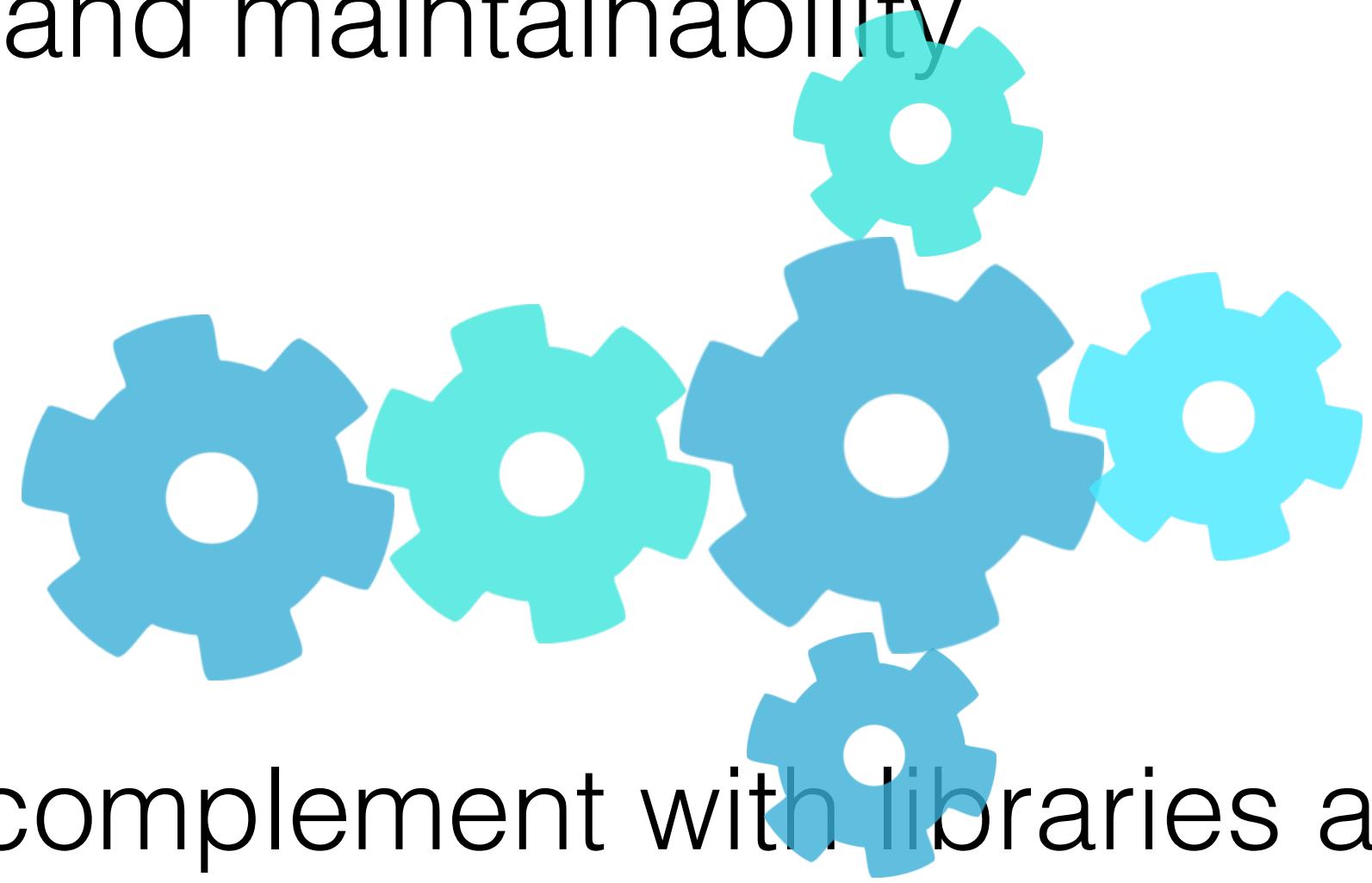
---

- Web servers handle HTTP requests, map URLs to local files, execute local scripts (e.g. CGI, PHP), or locally bound code (e.g. Servlets).
- App Servers modularly manage bound code, and associated resources (e.g. sessions, context, connections).
  - One web server, many applications.
  - Allows the assembly of components of applications (controllers, views, models)

# Web architectures, patterns and styles

---

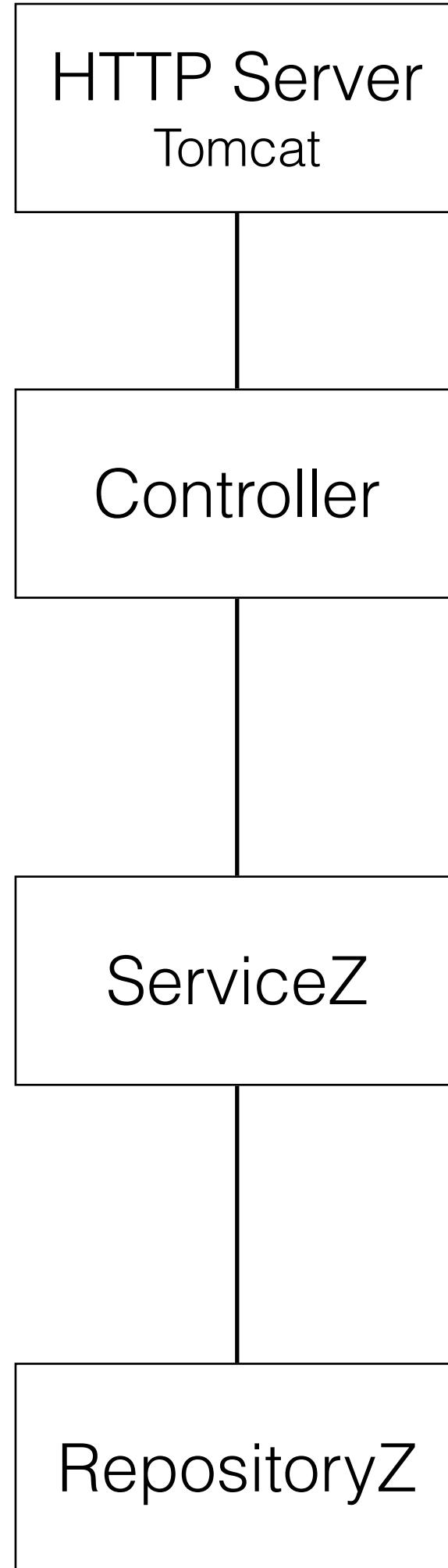
- Increase the level of abstraction, reusability, and maintainability
  - Software Architectures
  - Architectural and design patterns
  - Architectural styles
- Software frameworks implement some, and complement with libraries and tools.
- User-defined pieces are required to specify the “core” logic, and configure general purpose code.
- All implement the “inversion of control” pattern.



An architecture built with Spring



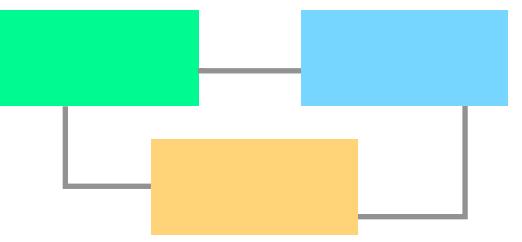
# Example of an Architecture built with Spring



- Spring is a component framework
- Resolves component dependencies by dependency injection
- Uses annotations to configure components

```
@RestController  
@RequestMapping("/")  
class EmpController(val employees:EmployeeService) {  
  
    // http GET :8080/api/projects/2/team  
    @GetMapping( "/api/projects/{id}/team")  
    fun teamMembersOfProject(  
        @PathVariable id:String  
    )  
        = employees.teamMembersOfProject(id)  
  
    }  
  
    @Service  
    class EmployeeService(val employees:EmployeeRepository) {  
        fun teamMembersOfProject(id:String) = employees.findAll()  
    }  
  
    interface EmployeeRepository : CrudRepository<Employee, Long>
```

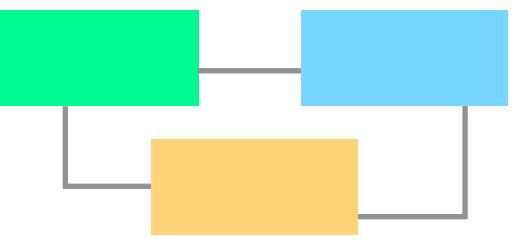
# Service Based Architectures



# Service Oriented Architectures

- Are the technological and methodological basis for building open-ended Internet Applications.
- Provide a model of distributed computation based on loosely coupled interactions.
- Define heterogeneous ecosystems of service implementations.
- Use implementation independent data formats (JSON, XML)
- Allows independent development of services by different vendors and technologies
- A service:
  - Is a logical representation of a repeatable business activity that has a specified outcome (e.g., check customer credit, provide weather data, consolidate drilling reports)
  - Is self-contained
  - May be composed of other services
  - Is a “black box” to consumers of the service

<https://web.archive.org/web/20160819141303/http://opengroup.org/soa/source-book/soa/soa.htm>



# Web architectures, patterns, and styles

---

- Web services are usually defined over HTTP protocol
- **SOAP** (*Simple Object Access Protocol*)
  - Operation based protocol (on HTTP) to implement web services (XML as format)
- **REST** (*Representational State Transfer*)
  - Resource based architectural style to implement web services over HTTP (or another connection protocol)

# Micro Service Architectures

---

- Are an extreme interpretation of service based architectures.
- Have smaller grained services and interfaces.
- Provide independent and lightweight deployment.
- Allow flexible management (e.g. replicas).
- Based on a clear service ownership model  
(team responsible for all stages of dev&ops).
- Isolated persistent state (**sometimes bad**).

<https://martinfowler.com/microservices/>

# Amazon's API Mandate (by Jeff Bezos, 2002)

---

- All teams will henceforth expose their data and functionality through service interfaces.
- Teams must communicate with each other through these interfaces.
- There will be no other form of inter-process communication allowed: no direct linking, no direct reads of another team's data store, no shared-memory model, no back-doors whatsoever. The only communication allowed is via service interface calls over the network.
- It doesn't matter what technology you use.
- All service interfaces, without exception, must be designed from the ground up to be externalizable. That is to say, the team must plan and design to be able to expose the interface to developers in the outside world. No exceptions.
- The mandate closed with: Anyone who doesn't do this will be fired. Thank you; have a nice day!

# Internet Applications Design and Implementation

2020 - 2021

(Lecture 2, Part 3 - Software Architecture - Frameworks)

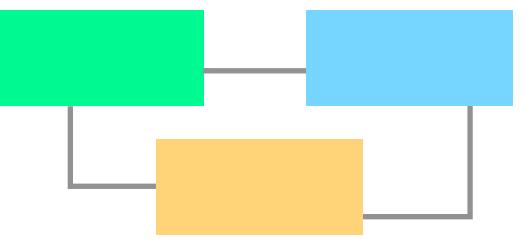
**MIEI - Integrated Master in Computer Science and Informatics  
Specialization block**

**João Costa Seco ([joao.seco@fct.unl.pt](mailto:joao.seco@fct.unl.pt))**

(with previous participations of Jácome Cunha ([jacome@fct.unl.pt](mailto:jacome@fct.unl.pt)) and João Leitão ([jc.leitao@fct.unl.pt](mailto:jc.leitao@fct.unl.pt)))

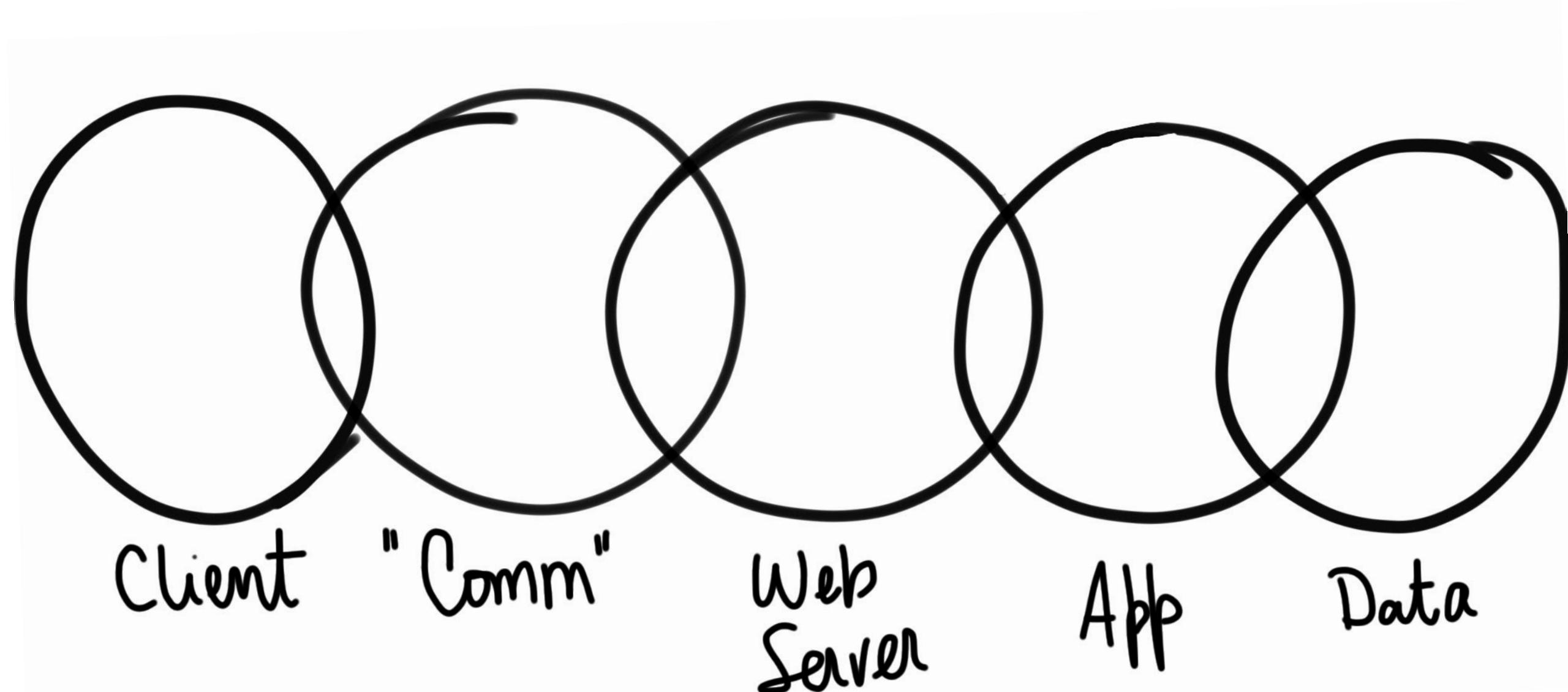


FACULDADE DE  
CIÊNCIAS E TECNOLOGIA  
UNIVERSIDADE NOVA DE LISBOA

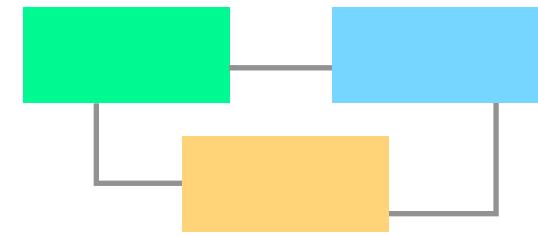


# Web architectures, patterns and styles

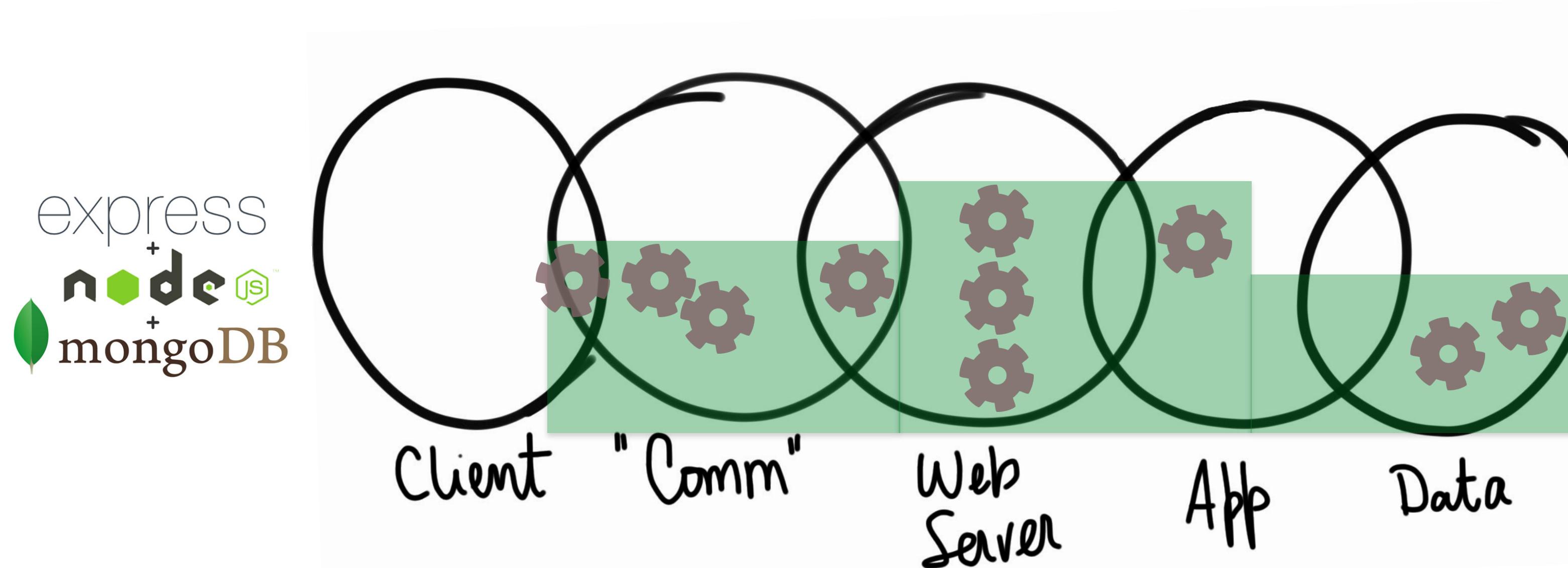
- Most common web applications follow the MVC architectural pattern.
  - Model layer - isolate the representation of persistent data and its operations, validations and conditions
  - Controller - contains the core application logic implementing the application interface (e.g. ad-hoc URL mapping, REST convention)
  - View - defines the way in which responses are formed (e.g. HTML, JSON)



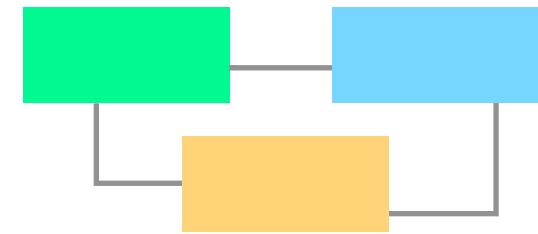
# Web architectures, patterns and styles



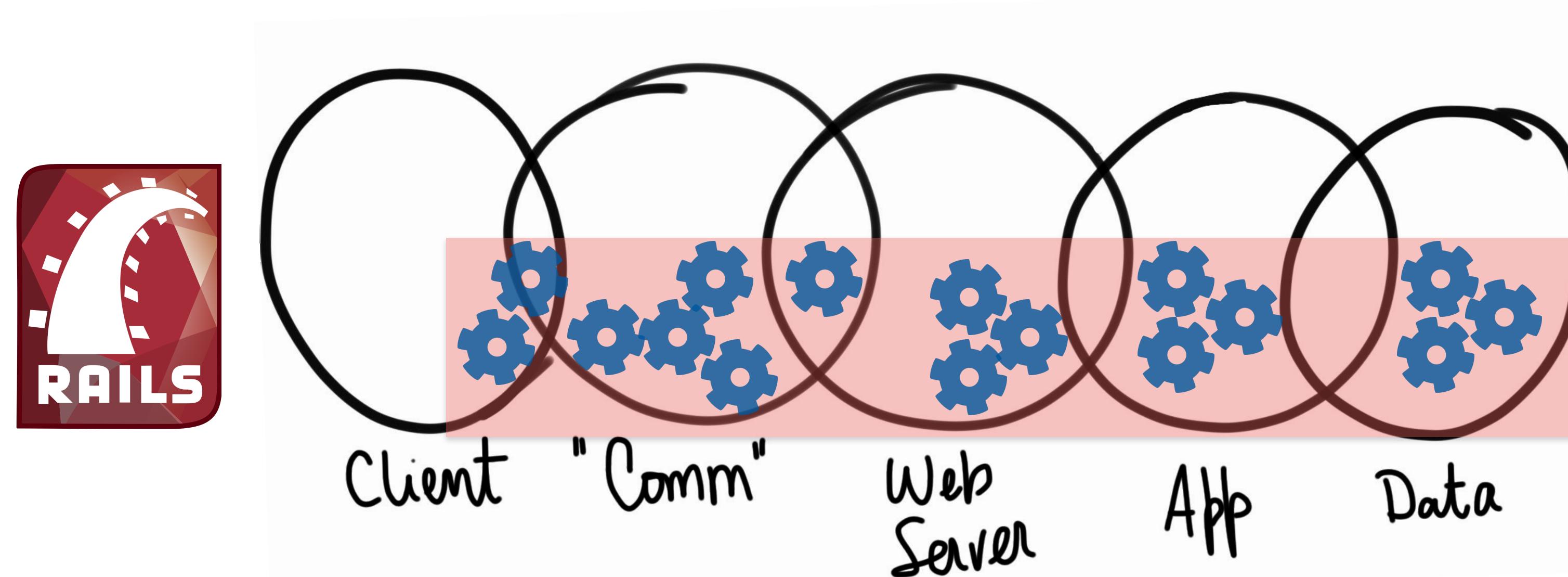
- Most common web applications follow the MVC architectural pattern.
  - Model layer - isolate the representation of persistent data and its operations, validations and conditions
  - Controller - contains the core application logic implementing the application interface (e.g. ad-hoc URL mapping, REST convention)
  - View - defines the way in which responses are formed (e.g. HTML, JSON)



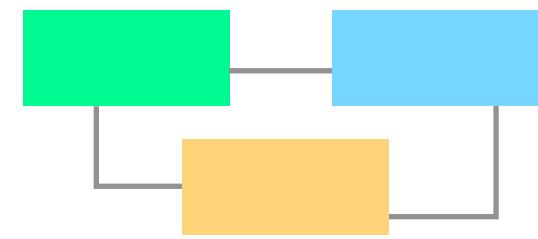
# Web architectures, patterns and styles



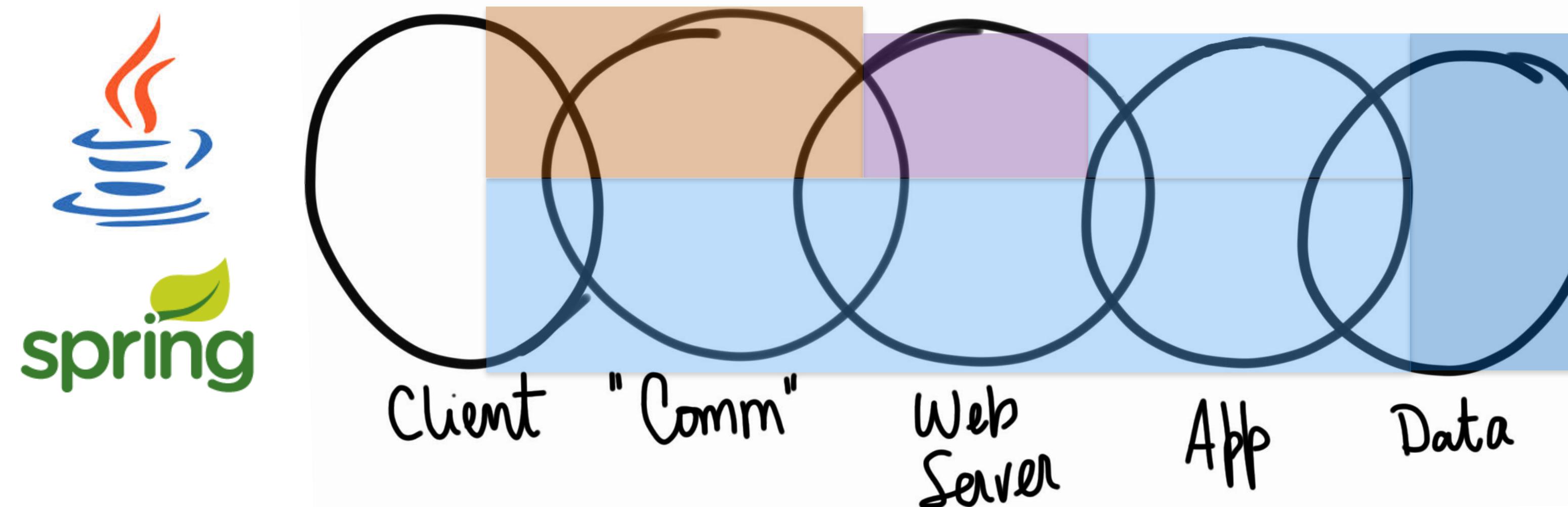
- Most common web applications follow the MVC architectural pattern.
  - Model layer - isolate the representation of persistent data and its operations, validations and conditions
  - Controller - contains the core application logic implementing the application interface (e.g. ad-hoc URL mapping, REST convention)
  - View - defines the way in which responses are formed (e.g. HTML, JSON)

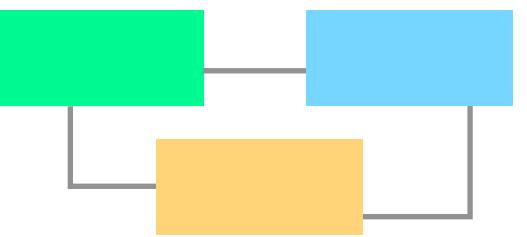


# Web architectures, patterns and styles



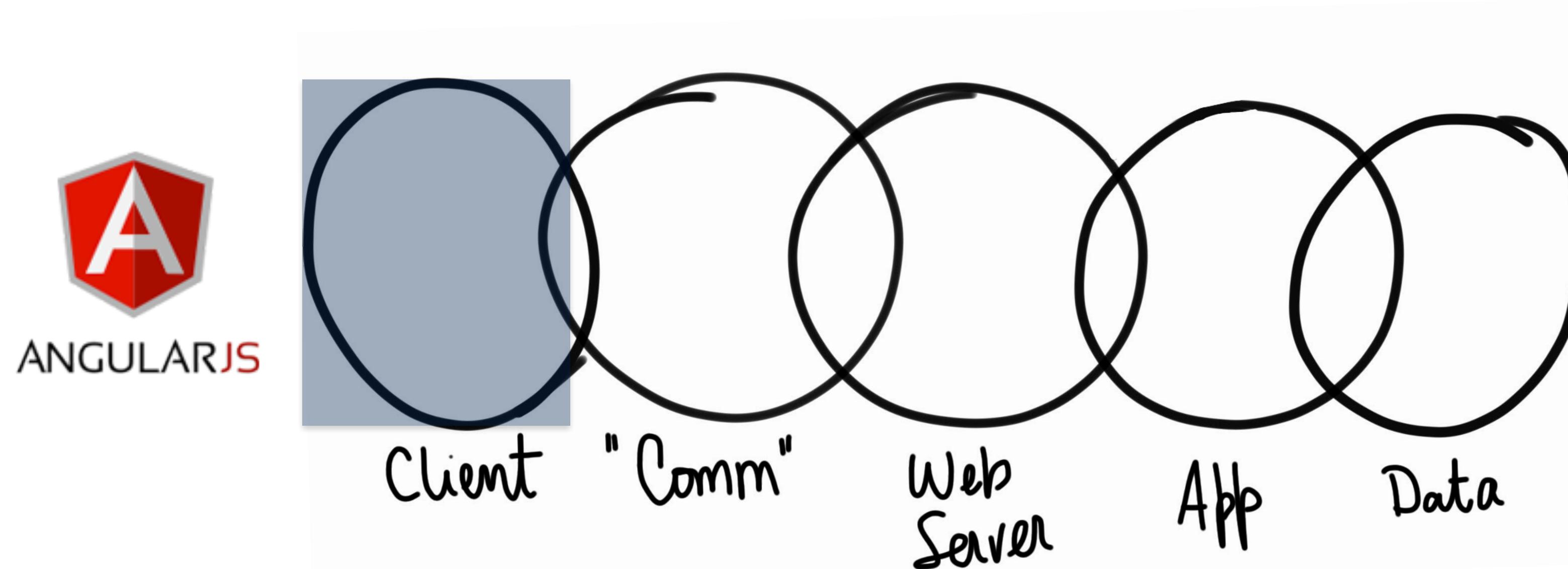
- Most common web applications follow the MVC architectural pattern.
  - Model layer - isolate the representation of persistent data and its operations, validations and conditions
  - Controller - contains the core application logic implementing the application interface (e.g. ad-hoc URL mapping, REST convention)
  - View - defines the way in which responses are formed (e.g. HTML, JSON)



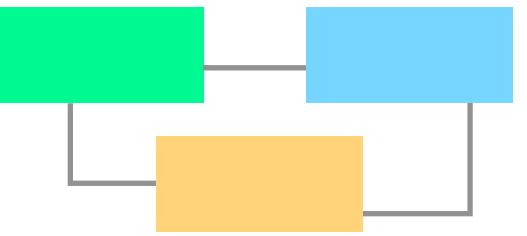


# Web architectures, patterns and styles

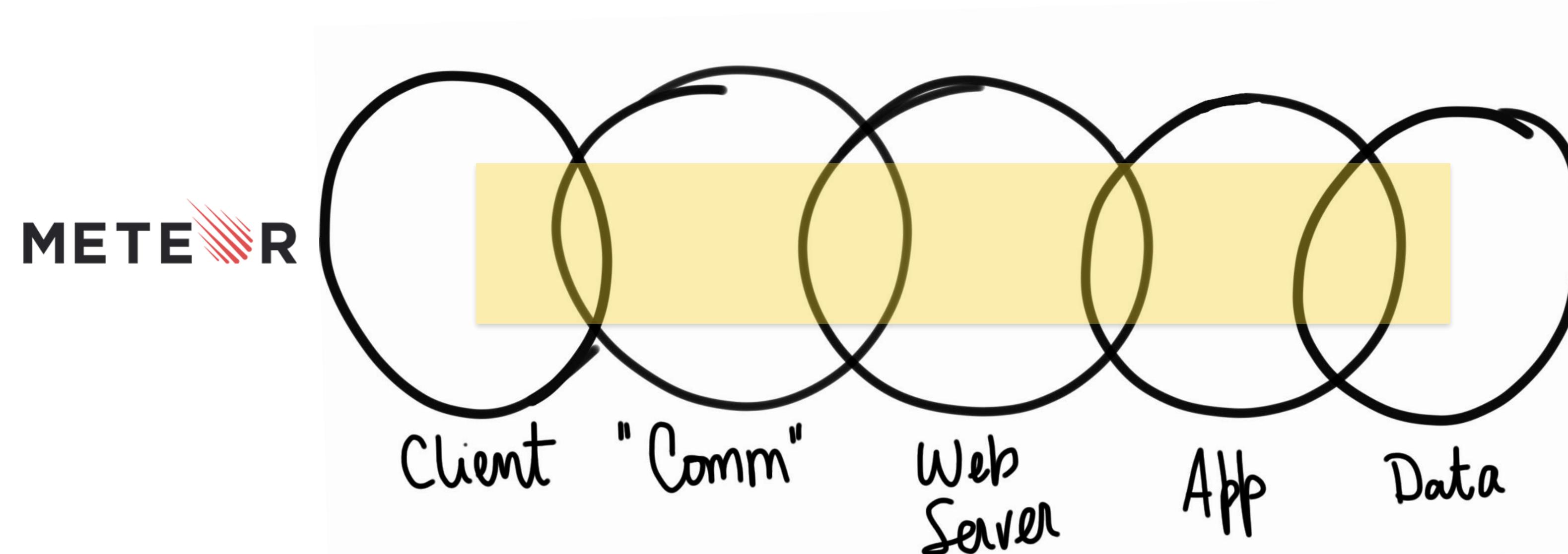
- Most common web applications follow the MVC architectural pattern.
  - Model layer - isolate the representation of persistent data and its operations, validations and conditions
  - Controller - contains the core application logic implementing the application interface (e.g. ad-hoc URL mapping, REST convention)
  - View - defines the way in which responses are formed (e.g. HTML, JSON)



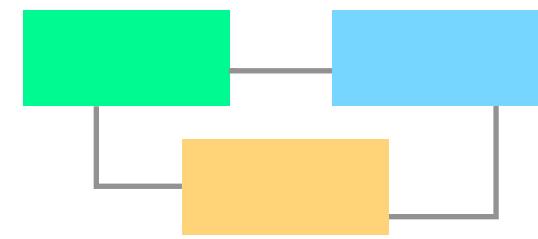
# Web architectures, patterns and styles



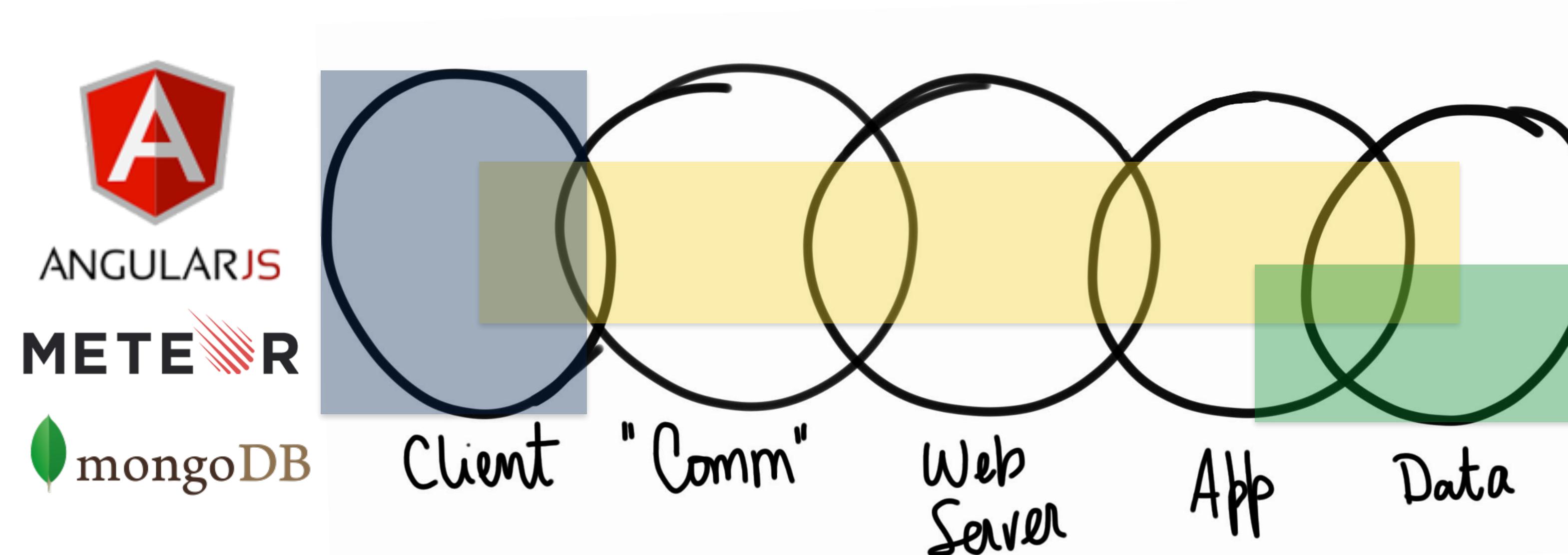
- Most common web applications follow the MVC architectural pattern.
  - Model layer - isolate the representation of persistent data and its operations, validations and conditions
  - Controller - contains the core application logic implementing the application interface (e.g. ad-hoc URL mapping, REST convention)
  - View - defines the way in which responses are formed (e.g. HTML, JSON)



# Web architectures, patterns and styles

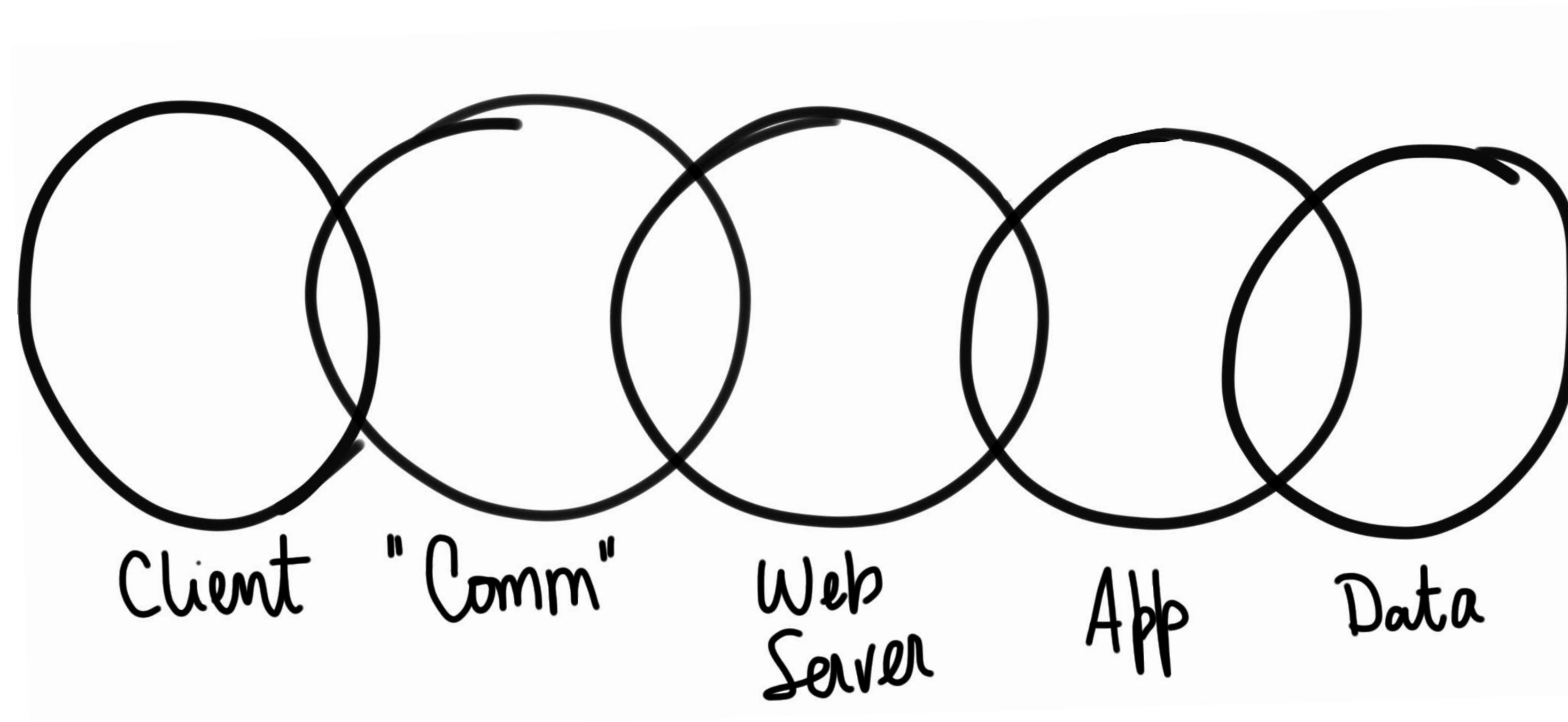


- Most common web applications follow the MVC architectural pattern.
  - Model layer - isolate the representation of persistent data and its operations, validations and conditions
  - Controller - contains the core application logic implementing the application interface (e.g. ad-hoc URL mapping, REST convention)
  - View - defines the way in which responses are formed (e.g. HTML, JSON)



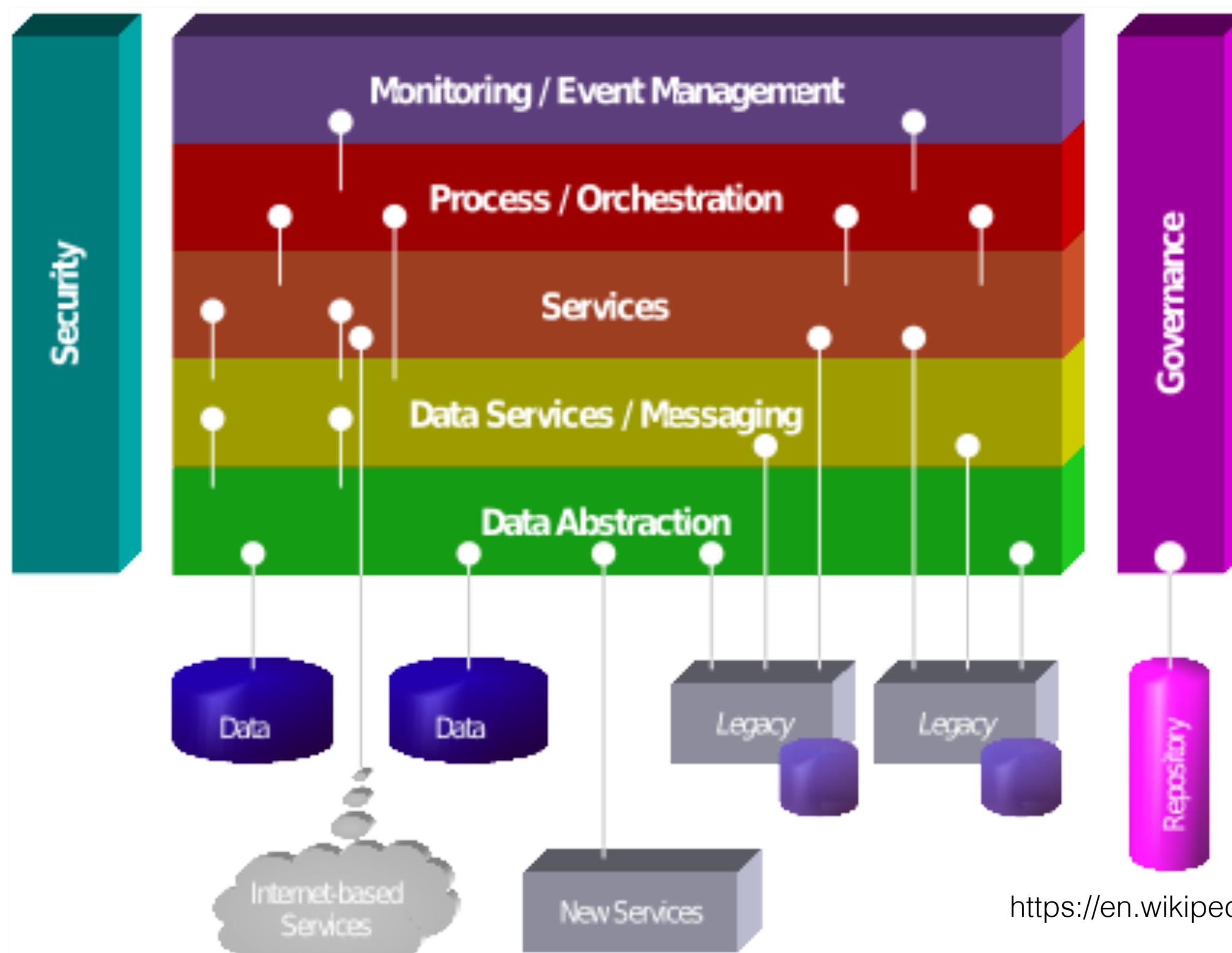
# Summary - Web Frameworks

- Web Frameworks are “languages” that carry libraries and abstractions that get compiled to run on the “web virtual machine”.



# (web & local) Services

- Service oriented architectures are a way of decoupling implementation from use.
- Services are implemented based on a “contract” or interface and provided by a broker.



[https://en.wikipedia.org/wiki/Service-oriented\\_architecture](https://en.wikipedia.org/wiki/Service-oriented_architecture)

# Service Orchestration Languages

- Spring Web Flow

```
<?xml version="1.0" encoding="UTF-8"?>
<flow xmlns="http://www.springframework.org/schema/webflow"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xsi:schemaLocation="http://www.springframework.org/schema/webflow
                          http://www.springframework.org/schema/webflow/spring-webflow-2.0.xsd"
```

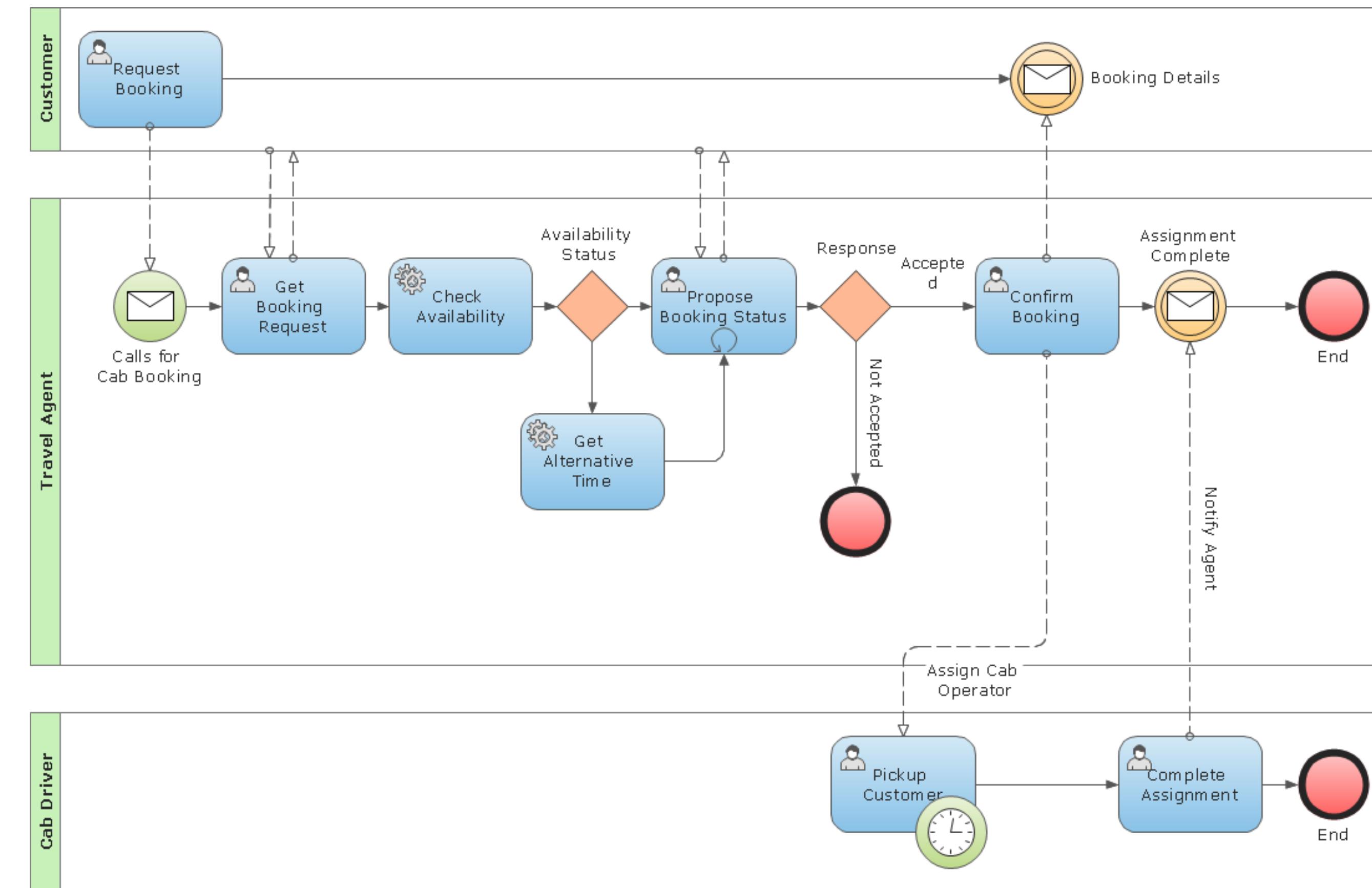
```
<start-state="welcome">

    <view-state id="welcome" view="/welcome.jsp">
        <transition on="continue" to="finish"/>
        <transition on="cancel" to="cancelled"/>
    </view-state>
```



# Process Specification Languages

- From processes to code...



# Internet Applications Design and Implementation

2020 - 2021

(Lecture 2, Part 4 - Software Architecture - RESTful applications)

**MIEI - Integrated Master in Computer Science and Informatics  
Specialization block**

**João Costa Seco ([joao.seco@fct.unl.pt](mailto:joao.seco@fct.unl.pt))**

(with previous participations of Jácome Cunha ([jacome@fct.unl.pt](mailto:jacome@fct.unl.pt)) and João Leitão ([jc.leitao@fct.unl.pt](mailto:jc.leitao@fct.unl.pt)))



FACULDADE DE  
CIÊNCIAS E TECNOLOGIA  
UNIVERSIDADE NOVA DE LISBOA

# Restful interface design (Recap)

---

- Follows an architectural style (convention)
  - Architectural style that promotes a simpler and more efficient way of providing and connecting web services. Built on top of basic HTTP
- Promotes the decoupling from Data-centric server side applications and client user-centric applications
- Implementations provide (convenient) flavours
  - Web-service style pure JSON/XML Data
  - Complete/partial HTML view responses
  - Javascript code responses (e.g. Rails AJAX responses)
- Fielding, Roy Thomas (2000). "Chapter 5: Representational State Transfer (REST)".  
Architectural Styles and the Design of Network-based Software Architectures (Ph.D.).  
University of California, Irvine

# REST - Representational State Transfer

---

- Resource Based
- Representation
- Uniform Interface
- Stateless
- Cacheable
- Client-Server
- Layered System
- Code on Demand (optional)

# Representational State Transfer

---

- Resource Based
  - vs Action Based
  - Nouns and not verbs to identify data in the system
  - Identified (represented) by URI
  - Aliasing is admissible
- Representation
- Uniform Interface
- Stateless
- Cacheable
- Client-Server
- Layered System
- Code on Demand (not talking about it)

# Representational State Transfer

---

- Resource Based
- Representation
  - JSON or XML representation of the state of a given resource transferred between client and server at a given verb in a given URL.
  - Well identified interface (the information retrieved at an URL — the type)
- Uniform Interface
- Stateless
- Cacheable
- Client-Server
- Layered System
- Code on Demand (not talking about it)

# Representational State Transfer

---

- Resource Based
- Representation
- Uniform Interface
  - standard HTTP verbs (GET, PUT, POST, DELETE)
  - standard HTTP response (status code, info in the response body)
  - Uniform structure of URIs with a name, identifying the resource
  - References inside responses must be complete.
- Stateless
- Cacheable
- Client-Server
- Layered System
- Code on Demand (not talking about it)

# Representational State Transfer

---

- Resource Based
- Representation
- Uniform Interface
- Stateless
  - Server does not hold session state
  - Messages are self contained
- Cacheable
- Client-Server
- Layered System
- Code on Demand (not talking about it)

# Representational State Transfer

---

- Resource Based
- Representation
- Uniform Interface
- Stateless
- Cacheable
  - Responses can be tagged as cacheable (in the server)
  - (also) Bookmarkable
- Layered System
- Code on Demand (not talking about it)

# Representational State Transfer

---

- Resource Based
- Representation
- Uniform Interface
- Stateless
- Cacheable
- Layered System
  - Establishes an API between a client and a “database”
  - Code on Demand (not talking about it)



## 6. Real REST Examples

Here's a very partial list of service providers that use a REST API. Note that some of them also support a WSDL (Web Services) API, in addition, so you can pick which to use; but in most cases, when both alternatives are available, REST calls are easier to create, the results are easier to parse and use, and it's also less resource-heavy on your system.

So without further ado, some REST services:

- The Google Glass API, known as "[Mirror API](#)", is a pure REST API. Here is [an excellent video talk](#) about this API. (The actual API discussion starts after 16 minutes or so.)
- Twitter has a **REST API** (in fact, this was their original API and, so far as I can tell, it's still the main API used by Twitter application developers),
- [Flickr](#),
- [Amazon.com](#) offer several REST services, e.g., for their [S3 storage solution](#),
- [Atom](#) is a RESTful alternative to RSS,
- [Tesla Model S](#) uses an (undocumented) REST API between the car systems and its Android/iOS apps.

in ... <http://rest.elkstein.org/2008/02/real-rest-examples.html>

```
interface
procedure ClrScr;
function SetColor(x,y:integer);
function SetTextColor(TxtColor,
                      BackColor:integer;
                      LineNum:integer;
                      ReadLine:char;
                      KeyPressed:boolean);
procedure ClrCol;
```

# Mirror API - Google Glasses

## Contacts

For Contacts Resource details, see the [resource representation](#) page.

Method	HTTP request	Description
URIs relative to <a href="https://www.googleapis.com/mirror/v1">https://www.googleapis.com/mirror/v1</a> , unless otherwise noted		
<a href="#">delete</a>	DELETE /contacts/ <i>id</i>	Deletes a contact.
<a href="#">get</a>	GET /contacts/ <i>id</i>	Gets a single contact by ID.
<a href="#">insert</a>	POST /contacts	Inserts a new contact.
<a href="#">list</a>	GET /contacts	Retrieves a list of contacts for the authenticated user.
<a href="#">patch</a>	PATCH /contacts/ <i>id</i>	Updates a contact in place. This method supports <a href="#">patch semantics</a> .
<a href="#">update</a>	PUT /contacts/ <i>id</i>	Updates a contact in place.

in ... <https://developers.google.com/glass/v1/reference/>

# Mirror API - Google Glasses

## Timeline

For Timeline Resource details, see the [resource representation](#) page.

Method	HTTP request	Description
URIs relative to <a href="https://www.googleapis.com/mirror/v1">https://www.googleapis.com/mirror/v1</a> , unless otherwise noted		
<a href="#">delete</a>	DELETE /timeline/ <i>id</i>	Deletes a timeline item.
<a href="#">get</a>	GET /timeline/ <i>id</i>	Gets a single timeline item by ID.
<a href="#">insert</a>	POST <a href="https://www.googleapis.com/upload/mirror/v1/timeline">https://www.googleapis.com/upload/mirror/v1/timeline</a> and POST /timeline	Inserts a new item into the timeline.
<a href="#">list</a>	GET /timeline	Retrieves a list of timeline items for the authenticated user.
<a href="#">patch</a>	PATCH /timeline/ <i>id</i>	Updates a timeline item in place. This method supports <a href="#">patch semantics</a> .
<a href="#">update</a>	PUT <a href="https://www.googleapis.com/upload/mirror/v1/timeline/">https://www.googleapis.com/upload/mirror/v1/timeline/</a> <i>id</i> and PUT /timeline/ <i>id</i>	Updates a timeline item in place.

# Mirror API - Google Glasses

## Timeline.attachments

For Timeline.attachments Resource details, see the [resource representation](#) page.

Method	HTTP request	Description
URIs relative to <a href="https://www.googleapis.com/mirror/v1">https://www.googleapis.com/mirror/v1</a> , unless otherwise noted		
delete	DELETE /timeline/ <i>itemId</i> /attachments/ <i>attachmentId</i>	Deletes an attachment from a timeline item.
get	GET /timeline/ <i>itemId</i> /attachments/ <i>attachmentId</i>	Retrieves an attachment on a timeline item by item ID and attachment ID.
insert	POST <a href="https://www.googleapis.com/upload/mirror/v1/timeline/itemId/attachments">https://www.googleapis.com/upload/mirror/v1/timeline/<i>itemId</i>/attachments</a>	Adds a new attachment to a timeline item.
list	GET /timeline/ <i>itemId</i> /attachments	Returns a list of attachments for a timeline item.

in ... <https://developers.google.com/glass/v1/reference/>

# RESTful design

---

- Resource = object or representation of something
- Collection = a set of resources
- URI = a path identifying **resources** and allowing actions on them
- URL methods represents standardised actions
  - GET = request resources
  - POST = create resources
  - PUT = update or create resources
  - DELETE = deletes resources
- HTTP Response codes = operation results
  - 20x Ok
  - 3xx Redirection (not modified)
  - 400 Bad Request, 401 Unauthorized, 403 Forbidden, 404 Not Found
  - 5xx Server Error
- Searching, sorting, filtering and pagination obtained by query string parameters
- Text Based Data format (JSON, or XML)

<https://hackernoon.com/restful-api-designing-guidelines-the-best-practices-60e1d954e7c9>

# Example

---

- Application to manage contacts of partner companies (e.g. for security clearance in events)
- Resources
  - Companies (name, address, email, list of contacts (employees))
  - Contact/Employee (name, email, job, company)
- Operations (CRUD)
  - List, add, update, and delete resources

# Partner companies

---

- GET /companies - List all the companies
- GET /companies?search=<criteria> - List all the companies that contain the substring <criteria>
- POST /companies - Create a company described in the payload. The request body must include all the necessary attributes.
- GET /companies/{id} - Shows the company with identifier {id}
- PUT /companies/{id} - Updates the company with {id} having values in the payload. The updatable items may vary (name, email, etc.)
- DELETE /companies/{id} - Removes the company with {id}

# Partner contacts

---

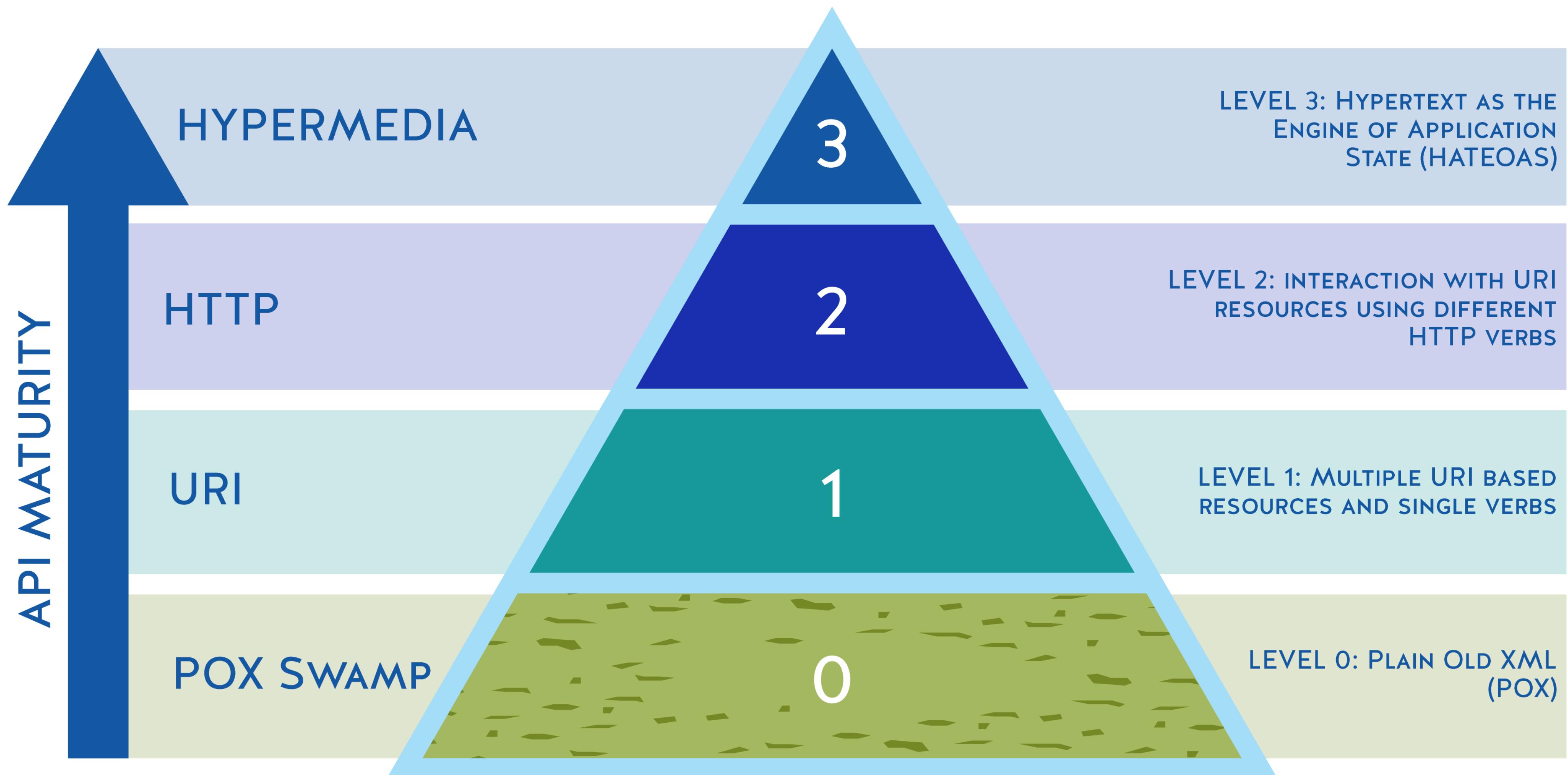
- **GET /contacts** - List all the contacts
- **GET /contacts?search=<criteria>** - List all the contacts that contain the substring **<criteria>**
- **POST /contacts** - Create a contact described in the payload. The request body must include all the necessary attributes.
- **GET /contacts/{id}** - Shows the contact with identifier {id}
- **PUT /contacts/{id}** - Updates the contact with {id} having values in the payload. The updatable items may vary (name, email, etc.)
- **DELETE /contacts/{id}** - Removes the contact with {id}

# Partner contacts of companies

---

- GET /companies/{id}/contacts - List all the contacts of a company
- GET /companies/{id}/contacts?search=<criteria> - List all the contacts of a company that contain the substring <criteria>
- POST /companies/{id}/contacts - Create a contact of company {id} described in the payload. The request body must include all the necessary attributes.
- GET /companies/{id}/contacts/{cid} - Shows the contact of company {id} with identifier {cid}
- PUT /companies/{id}/contacts/{cid} - Updates the contact with {cid} of company {id} having values in the payload. The updatable items may vary (name, email, etc.)
- DELETE /companies/{id}/contacts/{cid} - Removes the contact with {id}

# THE RICHARDSON MATURITY MODEL



# Example: Contacts in a Spring Controller

```
@RestController
@RequestMapping("/people")
public class PeopleController {

    @Autowired
    PeopleRepository people;

    @Autowired
    PetRepository pets;

    @GetMapping("")
    Iterable<Person> getAllPersons(@RequestParam(required = false) String search)
    {
        if( search == null )
            return people.findAll();
        else
            return people.searchByName(search);
    }

    @PostMapping("")
    void addNewPerson(@RequestBody Person p) {
        p.setId(0);
        people.save(p);
    }

    @GetMapping("{id}")
    Optional<Person> getOne(@PathVariable long id) {
        return people.findById(id);
    }
}
```

# JAX-RS: A standard for API declaration

- A lightweight specification method with (Java) annotations
- Implemented by RESTEasy and Jersey
- Similar to Spring annotations
- Official Java Specification
- [//jcp.org/en/jsr/detail?id=339](http://jcp.org/en/jsr/detail?id=339)

```
@Path("/notifications")
public class NotificationsResource {
    @GET
    @Path("/ping")
    public Response ping() {
        return Response.ok().entity("Service online").build();
    }

    @GET
    @Path("/get/{id}")
    @Produces(MediaType.APPLICATION_JSON)
    public Response getNotification(@PathParam("id") int id) {
        return Response.ok()
            .entity(new Notification(id, "john", "test notification"))
            .build();
    }

    @POST
    @Path("/post/")
    @Consumes(MediaType.APPLICATION_JSON)
    @Produces(MediaType.APPLICATION_JSON)
    public Response postNotification(Notification notification) {
        return Response.status(201).entity(notification).build();
    }
}
```

# Internet Applications Design and Implementation

2020 - 2021

(Lecture 2, Part 5 - Software Architecture - OpenAPI)

**MIEI - Integrated Master in Computer Science and Informatics  
Specialization block**

**João Costa Seco ([joao.seco@fct.unl.pt](mailto:joao.seco@fct.unl.pt))**

(with previous participations of Jácome Cunha ([jacome@fct.unl.pt](mailto:jacome@fct.unl.pt)) and João Leitão ([jc.leitao@fct.unl.pt](mailto:jc.leitao@fct.unl.pt)))



FACULDADE DE  
CIÊNCIAS E TECNOLOGIA  
UNIVERSIDADE NOVA DE LISBOA

# Swagger/OpenAPI

---

- Specification language for REST APIs (Yaml or JSON)
- Provides online (reflective) information on service(s)
  - Paths and operations (GET /companies, POST /employees)
  - Input and output parameters for each operation (samples)
  - Authentication methods
  - Contact information, license, terms of use and other information.
- Design, implementation and validation tools
- Editor, UI, Codegen, Spring Annotations
- Extensions to include more information about contracts

# Swagger/OpenAPI - Yaml

---

- General information about the API

```
swagger: "2.0"
info:
  description: "This is a sample directory of partner companies."
  version: "1.0.0"
  title: "Partner Companies"
host: "partners.swagger.io"
basePath: "/"
tags:
- name: "companies"
  description: "Everything about your partner companies"
  externalDocs:
    description: "Find out more"
    url: "http://swagger.io"
- name: "contacts"
  description: "Know all about your partners employees"
schemes:
- "https"
- "http"
paths:
...
definitions:
...
externalDocs:
  description: "Find out more about Swagger"
  url: "http://swagger.io"
```

# Swagger/OpenAPI - Yaml

---

- Specific information about each path/operation available

```
paths:  
  /companies:  
    get:  
      tags:  
        - "companies"  
      summary: "Get the list of all companies"  
      description: ""  
      operationId: "getCompanies"  
      produces:  
        - "application/json"  
      parameters:  
        - in: "query"  
          name: "search"  
          description: "Filter companies by name, description, or address"  
          type: "string"  
          required: false  
      responses:  
        200:  
          description: "successful operation"  
          schema:  
            type: "array"  
            items:
```

# Swagger/OpenAPI - Yaml

---

- Specific information about each path/operation available

```
post:  
  tags:  
    - "companies"  
  summary: "Add a new partner company to the collection"  
  description: ""  
  operationId: "addCompany"  
  consumes:  
    - "application/json"  
  parameters:  
    - in: "body"  
      name: "company"  
      description: "Company object that needs to be added to the collection"  
      required: true  
      schema:  
        $ref: "#/definitions/Company"  
  responses:  
    200:  
      description: "Company added"  
    405:  
      description: "Invalid input"
```

# Swagger/OpenAPI - Yaml

---

- Specific information about each path/operation available

```
/companies/{id}:
  get:
    tags:
      - "companies"
    summary: "Gets an existing company with {id} as identifier"
    description: "Gets an existing company with {id} as identifier"
    operationId: "getCompany"
    parameters:
      - in: "path"
        name: "id"
        description: "The identifier of the company to be updated"
        required: true
        type: "integer"
        format: "int64"
    responses:
      200:
        description: "The company data"
        schema:
          $ref: "#/definitions/Company"
```

# Swagger/OpenAPI - Yaml

---

- Specific information about each path/operation available

```
put:  
  tags:  
    - "companies"  
  summary: "Update an existing company with {id} as identifier"  
  description: "Update an existing company with {id} as identifier"  
  operationId: "updateCompany"  
  consumes:  
    - "application/json"  
  parameters:  
    - in: "path"  
      name: "id"  
      description: "The identifier of the company to be updated"  
      required: true  
      type: "integer"  
      format: "int64"  
    - in: "body"  
      name: "company"  
      description: "Company object that needs to be updated in the collection"  
      required: true  
      schema:  
        $ref: "#/definitions/Company"  
  responses:  
    200:  
      description: "Updated company"  
    400:  
      description: "Invalid ID supplied"  
    404:  
      description: "Company not found"  
    405:  
      description: "Validation exception"
```

# Swagger/OpenAPI - Yaml

---

- Specific information about datatypes

definitions:

Company:

```
  type: "object"
```

required:

- "name"
- "address"
- "email"

properties:

id:

```
      type: "integer"
```

```
      format: "int64"
```

name:

```
      type: "string"
```

```
      example: "ecma"
```

address:

```
      type: "string"
```

```
      example: "Long Street"
```

email:

```
      type: "string"
```

```
      example: "info@acme.com"
```

employees:

```
    type: "array"
```

items:

```
      $ref: "#/definitions/Employee"
```

# Generated API code (in Java)

```
@Api(value = "companies", description = "the companies API")
public interface CompaniesApi {

    @ApiOperation(value = "Add a new partner company to the collection", nickname = "addCompany", notes = "", tags={ "company", })
    @ApiResponses(value = { @ApiResponse(code = 405, message = "Invalid input") })
    @RequestMapping(value = "/companies",
        produces = { "application/json" },
        consumes = { "application/json" },
        method = RequestMethod.POST)
    ResponseEntity<Void> addCompany(@ApiParam(value = "Company object that needs to be added to the collection" ,required=true ) @Valid @RequestBody Company company);

    @ApiOperation(value = "Get the list of all companies", nickname = "getCompanies", notes = "", response = Company.class, responseContainer = "List", tags={ "company", })
    @ApiResponses(value = { @ApiResponse(code = 200, message = "successful operation", response = Company.class, responseContainer = "List") })
    @RequestMapping(value = "/companies",
        produces = { "application/json" },
        consumes = { "application/json" },
        method = RequestMethod.GET)
    ResponseEntity<List<Company>> getCompanies(@ApiParam(value = "Filter companies by name, description, or address") @Valid @RequestParam(value = "search", required = false) String search);

    @ApiOperation(value = "Update an existing company", nickname = "updateCompany", notes = "", tags={ "company", })
    @ApiResponses(value = { @ApiResponse(code = 400, message = "Invalid ID supplied"),
                           @ApiResponse(code = 404, message = "Company not found"),
                           @ApiResponse(code = 405, message = "Validation exception") })
    @RequestMapping(value = "/companies",
        produces = { "application/json" },
        consumes = { "application/json" },
        method = RequestMethod.PUT)
    ResponseEntity<Void> updateCompany(@ApiParam(value = "Company object that needs to be updated in the collection" ,required=true ) @Valid @RequestBody Company company);
}
```

# Generated Model Code

---

```
public class Company {  
    @JsonProperty("id")  
    private Long id = null;  
  
    @JsonProperty("name")  
    private String name = null;  
  
    @JsonProperty("address")  
    private String address = null;  
  
    @JsonProperty("email")  
    private String email = null;  
  
    @JsonProperty("employees")  
    @Valid  
    private List<Employee> employees = null;  
    ...
```

# Online information about API



## company

Show/Hide | List Operations | Expand Operations

GET [/companies](#)

Get the list of all companies

Response Class (Status 200)

successful operation

Model Example Value

```
[  
  {  
    "address": "Long Street",  
    "email": "info@acme.com",  
    "employees": [  
      {  
        "company": {  
          "address": "Long Street",  
          "email": "info@acme.com",  
          "employees": [  
            {  
              "name": "John Doe",  
              "position": "CEO",  
              "reports_to": null  
            }  
          ]  
        }  
      }  
    ]  
  }  
]
```

Response Content Type [application/json](#)

### Parameters

Parameter	Value	Description	Parameter Type	Data Type
search	<input type="text"/>	Filter companies by name, description, or address	query	string

# Online information about API

POST /companies Add a new partner company to the collection

**Parameters**

Parameter	Value	Description	Parameter Type	Data Type
<b>company</b>	(required)	<b>Company object that needs to be added to the collection</b>	body	<b>Model</b> Example Value

Parameter content type: application/json

**Response Messages**

HTTP Status Code	Reason	Response Model	Headers
200	OK		
201	Created		
401	Unauthorized		
403	Forbidden		
404	Not Found		
405	Invalid input		

Try it out!

# Machine readable specification

```
@RestController
@RequestMapping("/product")
@Api(value="onlinestore", description="Operations pertaining to products in Online Store")
public class ProductController {

    private ProductService productService;

    @Autowired
    public void setProductService(ProductService productService) {
        this.productService = productService;
    }

    @ApiOperation(value = "View a list of available products", response = Iterable.class)
    @ApiResponses(value = {
        @ApiResponse(code = 200, message = "Successfully retrieved list"),
        @ApiResponse(code = 401, message = "You are not authorized to view the resource"),
        @ApiResponse(code = 403, message = "Accessing the resource you were trying to reach is forbidden"),
        @ApiResponse(code = 404, message = "The resource you were trying to reach is not found")
    })
    @RequestMapping(value = "/list", method= RequestMethod.GET, produces = "application/json")
    public Iterable<Product> list(Model model){
        Iterable<Product> productList = productService.listAllProducts();
        return productList;
    }
    @ApiOperation(value = "Search a product with an ID", response = Product.class)
    @RequestMapping(value = "/show/{id}", method= RequestMethod.GET, produces = "application/json")
    public Product showProduct(@PathVariable Integer id, Model model){
        Product product = productService.getProductById(id);
        return product;
    }
}
```

# Machine readable specification

The screenshot shows the Swagger UI interface running in a Chrome browser window. The URL in the address bar is `localhost:8080/swagger-ui.html#!/product-controller/listUsingGET`. The main title is **product-controller : Operations pertaining to products in Online Store**. Below the title, there are three operations listed:

- POST /product/add** (green background, labeled **Add a product**)
- DELETE /product/delete/{id}** (red background, labeled **Delete a product**)
- GET /product/list** (blue background, labeled **View a list of available products**)

For the **GET /product/list** operation, the response class is listed as **Status 200** with the message **Successfully retrieved list**. The response model is shown as an empty JSON object: `{}`. The response content type is set to **application/json**. The response messages section includes entries for **401** and **403** status codes, along with a partial entry for **404**.

HTTP Status Code	Reason	Response Model	Headers
401	You are not authorized to view the resource		
403	Accessing the resource you were trying to reach is forbidden		
404	The resource you were trying to reach is not found		

<https://springframework.guru/spring-boot-restful-api-documentation-with-swagger-2/>

# Machine readable specification

```
@Entity
public class Product {
    @Id
    @GeneratedValue(strategy = GenerationType.AUTO)
    @ApiModelProperty(notes = "The database generated product ID")
    private Integer id;
    @Version
    @ApiModelProperty(notes = "The auto-generated version of the product")
    private Integer version;
    @ApiModelProperty(notes = "The application-specific product ID")
    private String productId;
    @ApiModelProperty(notes = "The product description")
    private String description;
    @ApiModelProperty(notes = "The image URL of the product")
    private String imageUrl;
    @ApiModelProperty(notes = "The price of the product", required = true)
    private BigDecimal price;
    ...
}
```

# Machine readable specification

Chrome

Swagger UI

localhost:8080/swagger-ui.html#!/product-controller/showProductUsingGET

GET /product/show/{id} Search a product with an ID

Response Class (Status 200)  
OK

Model Example Value

**Product {**

- description** (string, optional): The product description,
- id** (integer, optional): The database generated product ID,
- imageUrl** (string, optional): The image URL of the product,
- price** (number): The price of the product,
- productId** (string, optional): The application-specific product ID,
- version** (integer, optional): The auto-generated version of the product

**}**

<https://springframework.guru/spring-boot-restful-api-documentation-with-swagger-2/>

# Internet Applications Design and Implementation

2020 - 2021

(Lab class 2)

**MIEI - Integrated Master in Computer Science and Informatics  
Specialization block**

**João Costa Seco ([joao.seco@fct.unl.pt](mailto:joao.seco@fct.unl.pt))  
Eduardo Geraldo ([e.gerald@campus.fct.unl.pt](mailto:e.gerald@campus.fct.unl.pt))**



FACULDADE DE  
CIÊNCIAS E TECNOLOGIA  
UNIVERSIDADE NOVA DE LISBOA

# Lab Class 2&3

# **Swagger/Rest in Spring and Kotlin**

# Lab class 1 - Introduction to Spring and Swagger

---

- In this lab you will learn about using spring boot initializer, to build a controller for a REST API and use swagger editor to specify a functional API implementation. ([editor.swagger.io](https://editor.swagger.io))
- Requirements: Maven, IDE (Eclipse or IntelliJ)
- Lab Protocol:
  1. (done?) Read the project assignment, and design the corresponding ER diagram
  2. Write down the resources identified, and its subresources from a REST design perspective
  3. Create an empty spring application using SpringBoot initializer, from the IDE, or using the URL [start.spring.io](https://start.spring.io).
    - 3.1. Choose appropriate names for the different meta data fields, and choose kotlin as the base language
    - 3.2. Let's keep the stable version 2.1.8 of SpringBoot
    - 3.3. Add the module Spring Web under the Web category
    - 3.4. Be sure to let the IDE and Maven update all dependencies automatically
    - 3.5. Build and Run your application (It starts but does nothing!!)

# Lab class 1 - Introduction to Spring and Swagger

---

- Lab Protocol:
  1. (done?) Read the project assignment, and design the corresponding ER diagram
  2. Write down the resources identified, and its subresources from a REST design perspective
  3. Create an empty spring application using SpringBoot initializer, from the IDE, or using the URL [start.spring.io](http://start.spring.io).
  4. Design (on paper) the API for the Grant Application resource (all operations, and subresources)
  5. Create a class controller for the Grant resource (sample code ahead) with fake data. Implement all the designed endpoints. Define the data classes necessary to transfer data (DTOs). Choose the status codes to be returned carefully.
  6. Add Swagger to your project and define the general configuration.
  7. Add documentation annotations to your controller so that swagger automatically generates the online documentation for your API
  8. Use swagger editor and documentation to learn more



# Lab class 1 - Spring Project with Kotlin

playground ~/Documents/Work/Teaching/2019 - 20

- .idea
- .mvn
- ▼ src
  - main
    - kotlin
      - pt.unl.fct.di.iadi.vetclinic
        - VetclinicApplication.kt
    - resources
      - static
      - templates
      - application.properties
  - test
    - kotlin
      - pt.unl.fct.di.iadi.vetclinic
  - target
    - .gitignore
    - HELP.md
    - mvnw
    - mvnw.cmd
    - playground.iml
    - pom.xml
  - External Libraries
  - Scratches and Consoles

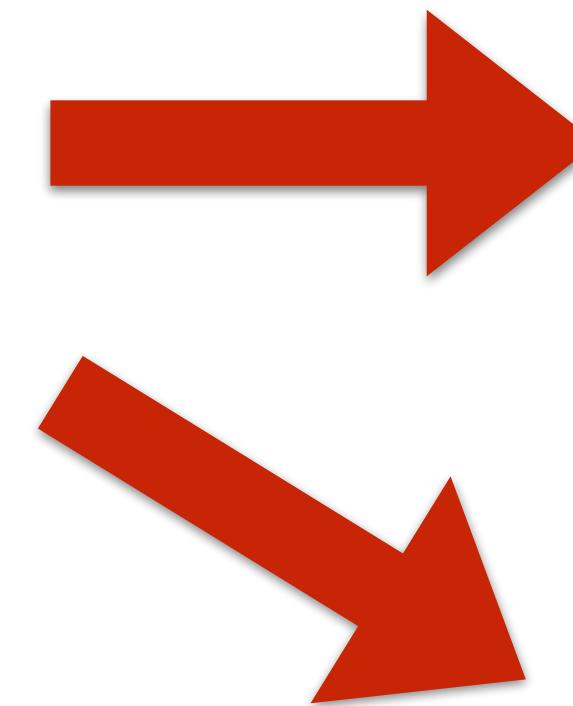
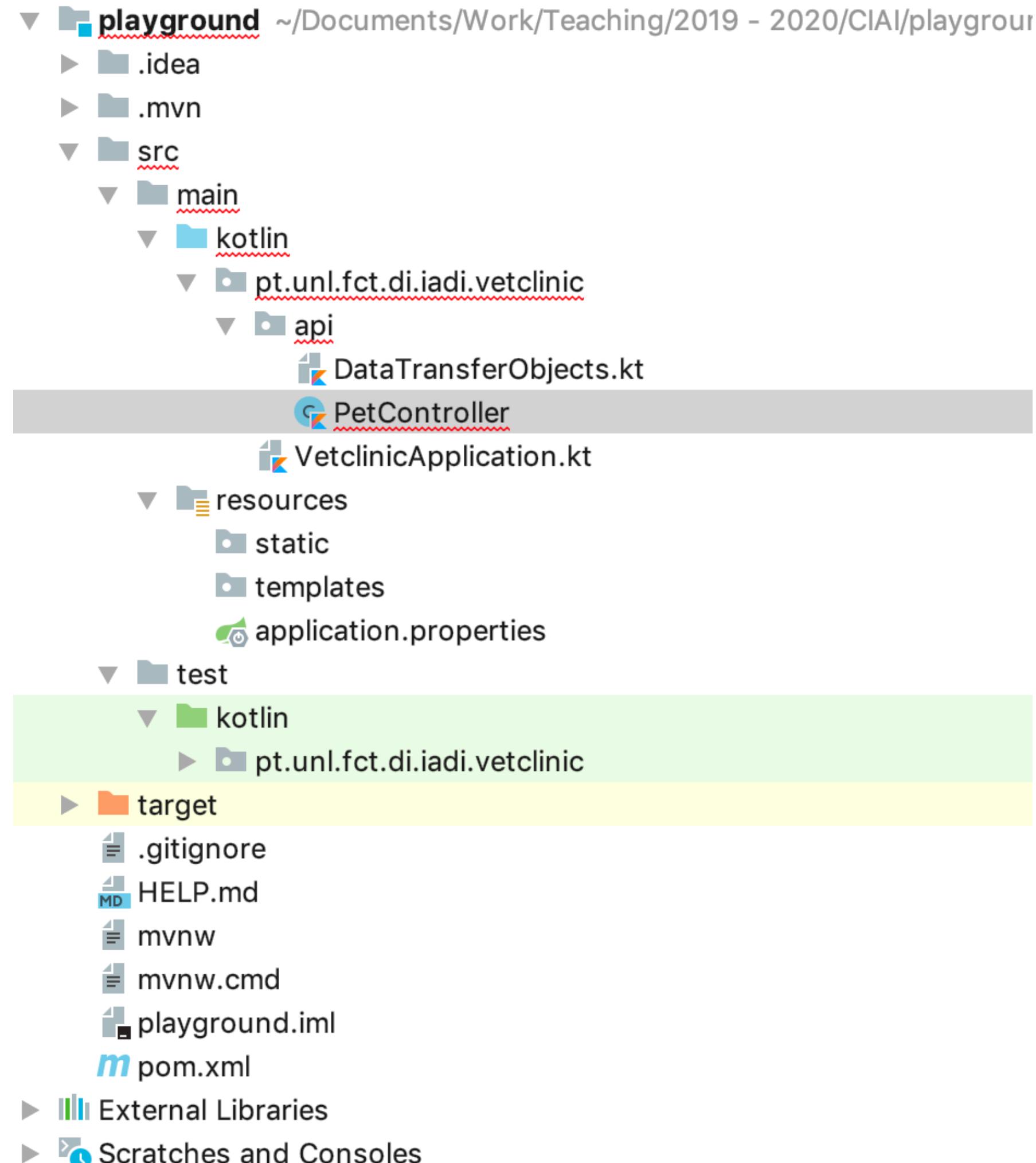


VetclinicApplication.kt

```
1 package pt.unl.fct.di.iadi.vetclinic
2
3 import org.springframework.boot.autoconfigure.SpringBootApplication
4 import org.springframework.boot.runApplication
5
6 @SpringBootApplication
7 class VetclinicApplication
8
9 fun main(args: Array<String>) {
10     runApplication<VetclinicApplication>(*args)
11 }
12
```

```
Starting VetclinicApplicationKt on 10-170-134-79.docente.di.fct.unl.pt with PID 21595 (start)
No active profile set, falling back to default profiles: default
Tomcat initialized with port(s): 8080 (http)
Starting service [Tomcat]
Starting Servlet engine: [Apache Tomcat/9.0.24]
Initializing Spring embedded WebApplicationContext
Root WebApplicationContext: initialization completed in 3454 ms
Initializing ExecutorService 'applicationTaskExecutor'
Tomcat started on port(s): 8080 (http) with context path ''
Started VetclinicApplicationKt in 5.222 seconds (JVM running for 6.834)
```

# Lab class 1 - Controller



```
package pt.unl.fct.di.iadi.vetclinic.api  
  
import org.springframework.web.bind.annotation.GetMapping  
import org.springframework.web.bind.annotation.PathVariable  
import org.springframework.web.bind.annotation.RequestMapping  
import org.springframework.web.bind.annotation.RestController  
  
@RestController  
@RequestMapping(...value: "/pets")  
class PetController {  
  
    @GetMapping(...value: "")  
    fun getAllPets() = emptyList<PetDTO>()  
  
    @GetMapping(...value: "/{id}")  
    fun getOnePet(@PathVariable id: Number) = PetDTO(id: 1, name: "Pantufas", species: "Dog")  
}  
  
package pt.unl.fct.di.iadi.vetclinic.api  
  
data class PetDTO(val id: Number, val name: String, val species: String)
```

# Lab class 1 - Calling a service



- use HTTPie, CURL, or Postman

```
iadi-2019-20-private — bash — 80x24
[iadi 2019 $ http :8080/pets
HTTP/1.1 200
Content-Type: application/json; charset=UTF-8
Date: Tue, 24 Sep 2019 09:55:20 GMT
Transfer-Encoding: chunked

[]

[iadi 2019 $ http :8080/pets/1
HTTP/1.1 200
Content-Type: application/json; charset=UTF-8
Date: Tue, 24 Sep 2019 10:00:08 GMT
Transfer-Encoding: chunked

{
  "id": 1,
  "name": "Pantufas",
  "species": "Dog"
}

iadi 2019 $ ]
```



POSTMAN

# Kotlin References



LEARN

COMMUNITY

TRY ONLINE



Reference

Tutorials

Books

More resources

▶ Overview

▶ Getting Started

▶ Basics

▶ Classes and Objects

▶ Functions and Lambdas

▶ Collections

▶ Multiplatform Programming

▶ Other

▶ Core Libraries

▶ Reference

▶ Java Interop

▶ JavaScript

▶ Native

▶ Coroutines

▶ Tools

▶ Evolution

▶ FAQ

## Learn Kotlin

[Edit Page](#)

All Materials

Getting Started

Migrating from Java

### Documentation

Kotlin documentation is a good place to start, check out these links to get your feet wet:

— Basics

— Idioms

— Interop with Java

### IDE

Many modern IDEs support Kotlin and help in writing idiomatic Kotlin code:

— Kotlin Educational Plugin

— Java2Kotlin converter

### Community

Kotlin community is open, helpful, and welcoming. Don't hesitate to join and ask on any platform you like:

— Blog

— Forum

— Slack

— Stack overflow

### Playground

Hands-on experience is the way to master your Kotlin skills on real examples right in the browser:

— Playground

— Kotlin Examples

— Koans

Reference

▶ Overview

▶ Getting Started

— Basic Syntax

— Idioms

— Coding Conventions

▶ Basics

▶ Classes and Objects

▶ Functions and Lambdas

▶ Collections

▶ Multiplatform Programming

▶ Other

▶ Core Libraries

▶ Reference

## Idioms

A collection of random and frequently used idioms in Kotlin. If you have a favorite idiom, please add it by sending a pull request.

### Creating DTOs (POJOs/POCOs)

```
data class Customer(val name: String, val email: String)
```

provides a `Customer` class with the following functionality:

— getters (and setters in case of `vars`) for all properties— `equals()`— `hashCode()`— `toString()`— `copy()`— `component1()`, `component2()`, ..., for all properties (see [Data classes](#))[PDF Full Kotlin Reference](#)

### Books

### Online Courses

# Lab class 1 - Document the API (Swagger)



```
/** Copyright 2019 João Costa Seco ...*/

package pt.unl.fct.di.iadi.vetclinic.config

import org.springframework.context.annotation.Bean
import org.springframework.context.annotation.Configuration
import springfox.documentation.builders.ApiInfoBuilder
import springfox.documentation.builders.PathSelectors
import springfox.documentation.builders.RequestHandlerSelectors
import springfox.documentation.service.ApiInfo
import springfox.documentation.service.Contact
import springfox.documentation.spi.DocumentationType
import springfox.documentation.spring.web.plugins.Docket
import springfox.documentation.swagger2.annotations.EnableSwagger2

@Configuration
@EnableSwagger2
class SwaggerConfiguration {
    @Bean
    fun api(): Docket =
        Docket(DocumentationType.SWAGGER_2)
            .select()
            .apis(RequestHandlerSelectors.basePackage("pt.unl.fct.di.iadi.vetclinic"))
            .paths(PathSelectors.any())
            .build().apiInfo(apiEndPointsInfo());

    fun apiEndPointsInfo(): ApiInfo =
        ApiInfoBuilder()
            .title("Spring Boot REST API Example for IADI 2019/20")
            .description("IADI 2019 VetClinic REST API")
            .contact(Contact(name = "João Costa Seco", url = "http://ctp.di.fct.unl.pt/~jcs", email = "joao.seco@fct.unl.pt"))
            .license(License(name = "Apache 2.0"))
            .licenseUrl("http://www.apache.org/licenses/LICENSE-2.0.html")
            .version("1.0.0")
            .build()
}
```

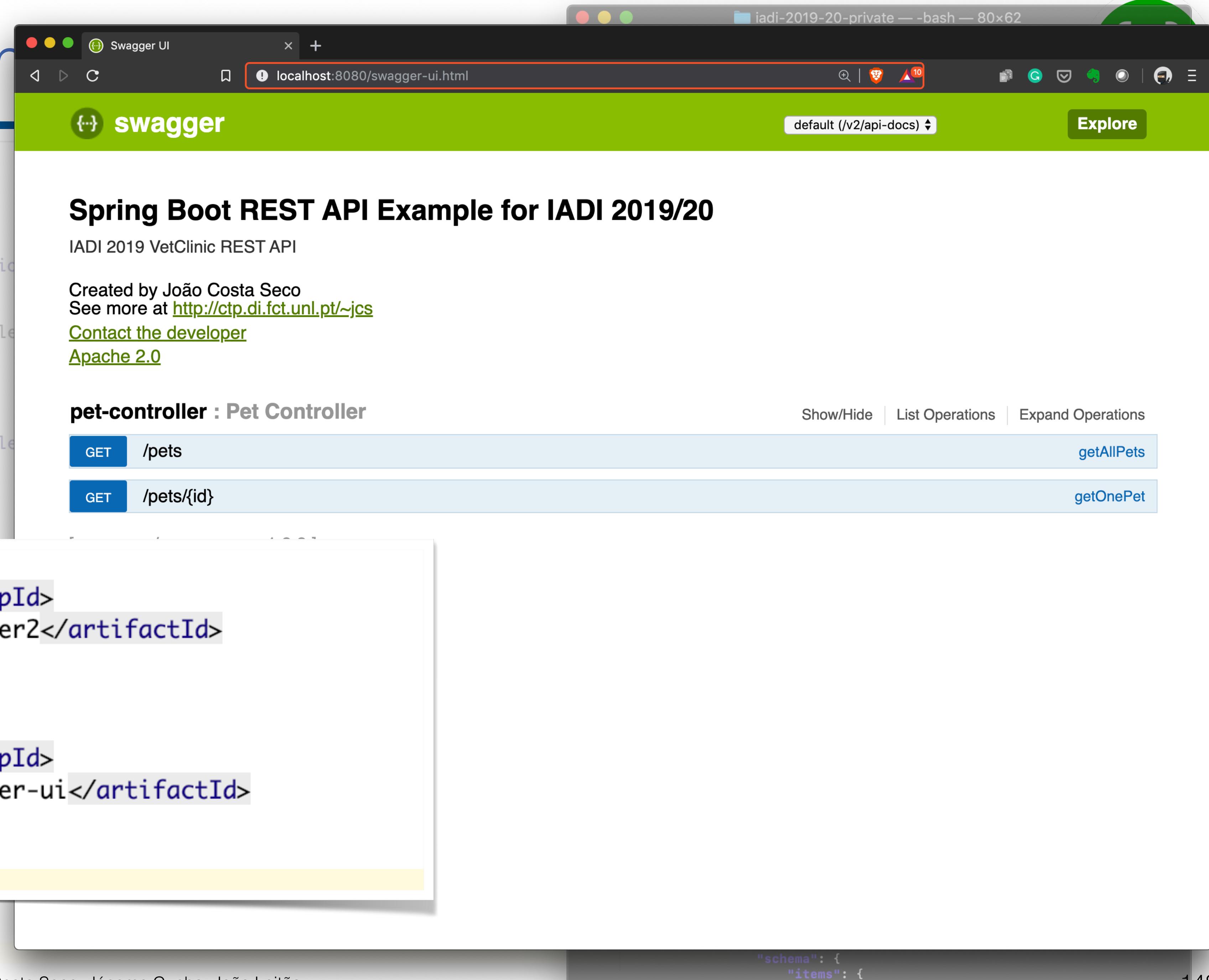
```
iadi 2019 $ http :8080/v2/api-docs
HTTP/1.1 200
Content-Type: application/json; charset=UTF-8
Date: Tue, 24 Sep 2019 10:19:39 GMT
Transfer-Encoding: chunked

{
    "basePath": "/",
    "definitions": {
        "Number": {
            "type": "object"
        },
        "PetDTO": {
            "properties": {
                "id": {
                    "$ref": "#/definitions/Number"
                },
                "name": {
                    "type": "string"
                },
                "species": {
                    "type": "string"
                }
            },
            "required": [
                "id",
                "name",
                "species"
            ],
            "type": "object"
        }
    },
    "host": "localhost:8080",
    "info": {
        "contact": {
            "email": "joao.seco@fct.unl.pt",
            "name": "João Costa Seco",
            "url": "http://ctp.di.fct.unl.pt/~jcs"
        },
        "description": "IADI 2019 VetClinic REST API",
        "license": {
            "name": "Apache 2.0",
            "url": "http://www.apache.org/licenses/LICENSE-2.0.html"
        },
        "title": "Spring Boot REST API Example for IADI 2019/20",
        "version": "1.0.0"
    },
    "paths": {
        "/pets": {
            "get": {
                "consumes": [
                    "application/json"
                ],
                "operationId": "getAllPetsUsingGET",
                "produces": [
                    "*/*"
                ],
                "responses": {
                    "200": {
                        "description": "OK",
                        "schema": {
                            "items": {

```

# Lab class 1 - Document

```
/** Copyright 2019 João Costa Seco ...*/  
  
package pt.unl.fct.di.iadi.vetclinic.config  
  
import org.springframework.context.annotation.Bean  
import org.springframework.context.annotation.Configuration  
import springfox.documentation.builders.ApiInfoBuilder  
import springfox.documentation.builders.PathSelectors  
import springfox.documentation.builders.RequestHandlerSelectors  
import springfox.documentation.service.ApiInfo  
import springfox.documentation.service.Contact  
import springfox.documentation.spi.DocumentationType  
import springfox.documentation.spring.web.plugins.Docket  
import springfox.documentation.swagger2.annotations.EnableSwagger2  
  
@Configuration  
@EnableSwagger2  
class SwaggerConfiguration {  
  
    <dependency>  
        <groupId>io.springfox</groupId>  
        <artifactId>springfox-swagger2</artifactId>  
        <version>2.7.0</version>  
    </dependency>  
    <dependency>  
        <groupId>io.springfox</groupId>  
        <artifactId>springfox-swagger-ui</artifactId>  
        <version>2.7.0</version>  
    </dependency>  
}
```



# Lab class 1 - Documenting REST API

```
/** Copyright 2019 João Costa Seco ...*/  
  
package pt.unl.fct.di.iadi.vetclinic.api  
  
import ...  
  
@ApiController  
@ApiResponses(value = [  
    ApiResponse(code = 200, message = "Successfully registered"),  
    ApiResponse(code = 401, message = "You are not authorized to perform this operation"),  
    ApiResponse(code = 403, message = "Accessing the resource you are not authorized to access"),  
    ApiResponse(code = 404, message = "The resource you are trying to access does not exist")])  
class PetController {  
  
    @ApiOperation(value = "View a list of registered pets",  
        @ApiResponses(value = [  
            ApiResponse(code = 200, message = "Successfully ret...  
            ApiResponse(code = 401, message = "You are not auth...  
            ApiResponse(code = 403, message = "Accessing the re...  
        ]))  
    @GetMapping(...value: "")  
    fun getAllPets(): List<PetDTO> = emptyList()  
  
    @ApiOperation(value = "Get the details of a single pet",  
        @ApiResponses(value = [  
            ApiResponse(code = 200, message = "Successfully ret...  
            ApiResponse(code = 401, message = "You are not auth...  
            ApiResponse(code = 403, message = "Accessing the re...  
            ApiResponse(code = 404, message = "The resource you...  
        ]))  
    @GetMapping(...value: "/{id}")  
    fun getOnePet(@PathVariable id: Number): PetDTO = PetDTO(id: 1,  
        name: "Lucky", type: "Dog", status: "available")  
}
```

The screenshot shows the Swagger UI interface for a Spring Boot REST API. The title of the page is "Spring Boot REST API Example for IADI 2019/20". Below the title, it says "IADI 2019 VetClinic REST API". It credits "Created by João Costa Seco" and provides a link "See more at <http://ctp.di.fct.unl.pt/~jcs>". There are links for "Contact the developer" and "Apache 2.0". The main content area is titled "pet-controller : Management operations of Pets in the IADI 2019 Pet Clinic". It lists two operations: "GET /pets" (View a list of registered pets) and "GET /pets/{id}" (Get the details of a single pet by id). At the bottom, it indicates "[ BASE URL: /, API VERSION: 1.0.0 ]". The top right of the Swagger UI header shows "default (/v2/api-docs)" and "Explore".

# Lab class 1 - Documenting REST APIs

```
/** Copyright 2019 João Costa Seco ...*/  
  
package pt.unl.fct.di.iadi.vetclinic.api  
  
import ...  
  
@ApiController  
@RequestMapping(...value: "/pets")  
class PetController {  
  
    @ApiOperation(value = "View a list of registered pets",  
    @ApiResponses(value = [  
        ApiResponse(code = 200, message = "Successfully retrieved pet details"),  
        ApiResponse(code = 401, message = "You are not authorized to view the resource"),  
        ApiResponse(code = 403, message = "Accessing the resource you were trying to reach is forbidden"),  
        ApiResponse(code = 404, message = "The resource you were trying to reach is not found")  
    ])  
    @GetMapping("")  
    fun getAllPets(): List<PetDTO> = emptyList()  
  
    @ApiOperation(value = "Get the details of a single pet",  
    @ApiResponses(value = [  
        ApiResponse(code = 200, message = "Successfully retrieved pet details"),  
        ApiResponse(code = 401, message = "You are not authorized to view the resource"),  
        ApiResponse(code = 403, message = "Accessing the resource you were trying to reach is forbidden"),  
        ApiResponse(code = 404, message = "The resource you were trying to reach is not found")  
    ])  
    @GetMapping("/{id}")  
    fun getOnePet(@PathVariable id: Number): PetDTO = PetDTO(id: 1,  
    ...)
```

localhost:8080/swagger-ui.html#!/pet45controller/getOnePetUsingGET

Show/Hide | List Operations | Expand Operations

View a list of registered pets | Get the details of a single pet by id

GET /pets

GET /pets/{id}

Response Class (Status 200)  
Successfully retrieved pet details

Model Example Value

```
{  
    "id": {},  
    "name": "string",  
    "species": "string"  
}
```

Response Content Type /\*

Response Messages

HTTP Status Code	Reason	Response Model	Headers
401	You are not authorized to view the resource		
403	Accessing the resource you were trying to reach is forbidden		
404	The resource you were trying to reach is not found		

Try it out!

[ BASE URL: / , API VERSION: 1.0.0 ]



# Use Swagger documentation to learn details

- Editor
- Documentation
- Tutorials online

The screenshot shows the Swagger Editor interface. On the left, a code editor displays a Swagger 2.0 JSON schema for "Partner Companies". The schema includes definitions for "company", "employees", and "user" tags, along with paths for "/companies" and "/users". On the right, the generated API documentation is shown under the heading "Partner Companies 1.0.0". It includes a brief description, links to Swagger documentation, and a dropdown for "Schemes" set to "HTTPS". Below this, there are three operations for the "/companies" path: a GET method to list companies, a POST method to add a new company, and a PUT method to update an existing company. To the right of these, there are sections for "company", "employees", "user", and "Models".

```
1 swagger: "2.0"
2   info:
3     description: "This is a sample directory of partner companies."
4     version: "1.0.0"
5     title: "Partner Companies"
6   host: "partners.swagger.io"
7   basePath: "/"
8   tags:
9     - name: "company"
10    description: "Everything about your partner companies"
11    externalDocs:
12      description: "Find out more"
13      url: "http://swagger.io"
14    - name: "employees"
15      description: "Know all about your partners employees"
16    - name: "user"
17      description: "Operations about users"
18   schemes:
19     - "https"
20     - "http"
21   paths:
22     /companies:
23       get:
24         tags:
25           - "company"
26           summary: "Get the list of all companies"
27           description: ""
28           operationId: "getCompanies"
29           consumes:
30             - "application/json"
31           produces:
32             - "application/json"
33           parameters:
34             - in: "query"
35               name: "search"
36               description: "Filter companies by name, description, or address"
37               type: "string"
38               required: false
39           responses:
40             200:
41               description: "successful operation"
42               schema:
43                 type: "array"
44                 items:
45                   $ref: "#/definitions/Company"
46     post:
```

**Partner Companies 1.0.0**  
[ Base URL: partners.swagger.io/ ]  
This is a sample directory of partner companies.  
Find out more about Swagger

Schemes  
HTTPS

**company** Everything about your partner companies Find out more: <http://swagger.io>

**GET** /companies Get the list of all companies

**POST** /companies Add a new partner company to the collection

**PUT** /companies Update an existing company

**employees** Know all about your partners employees >

**user** Operations about users >

**Models** >

# Internet Applications Design and Implementation

## 2020 - 2021

### (Lecture 3 - Server side programming, Data Sources)

**MIEI - Integrated Master in Computer Science and Informatics  
Specialization block**

**João Costa Seco ([joao.seco@fct.unl.pt](mailto:joao.seco@fct.unl.pt))**

(with previous participations of Jácome Cunha ([jacome@fct.unl.pt](mailto:jacome@fct.unl.pt)) and João Leitão ([jc.leitao@fct.unl.pt](mailto:jc.leitao@fct.unl.pt)))



**FACULDADE DE  
CIÊNCIAS E TECNOLOGIA  
UNIVERSIDADE NOVA DE LISBOA**

# Outline

---

- Recap REST Architectural Style
- Server Side Patterns
  - Model View Controller
  - Dependency Injection
  - Builder
- Data Sources in MVC
- ORM
- JPA and Spring

# Internet Applications Design and Implementation

2020 - 2021

(Lecture 3 - Part 1 - RESTful interfaces in practice)

**MIEI - Integrated Master in Computer Science and Informatics  
Specialization block**

**João Costa Seco ([joao.seco@fct.unl.pt](mailto:joao.seco@fct.unl.pt))**

(with previous participations of Jácome Cunha ([jacome@fct.unl.pt](mailto:jacome@fct.unl.pt)) and João Leitão ([jc.leitao@fct.unl.pt](mailto:jc.leitao@fct.unl.pt)))



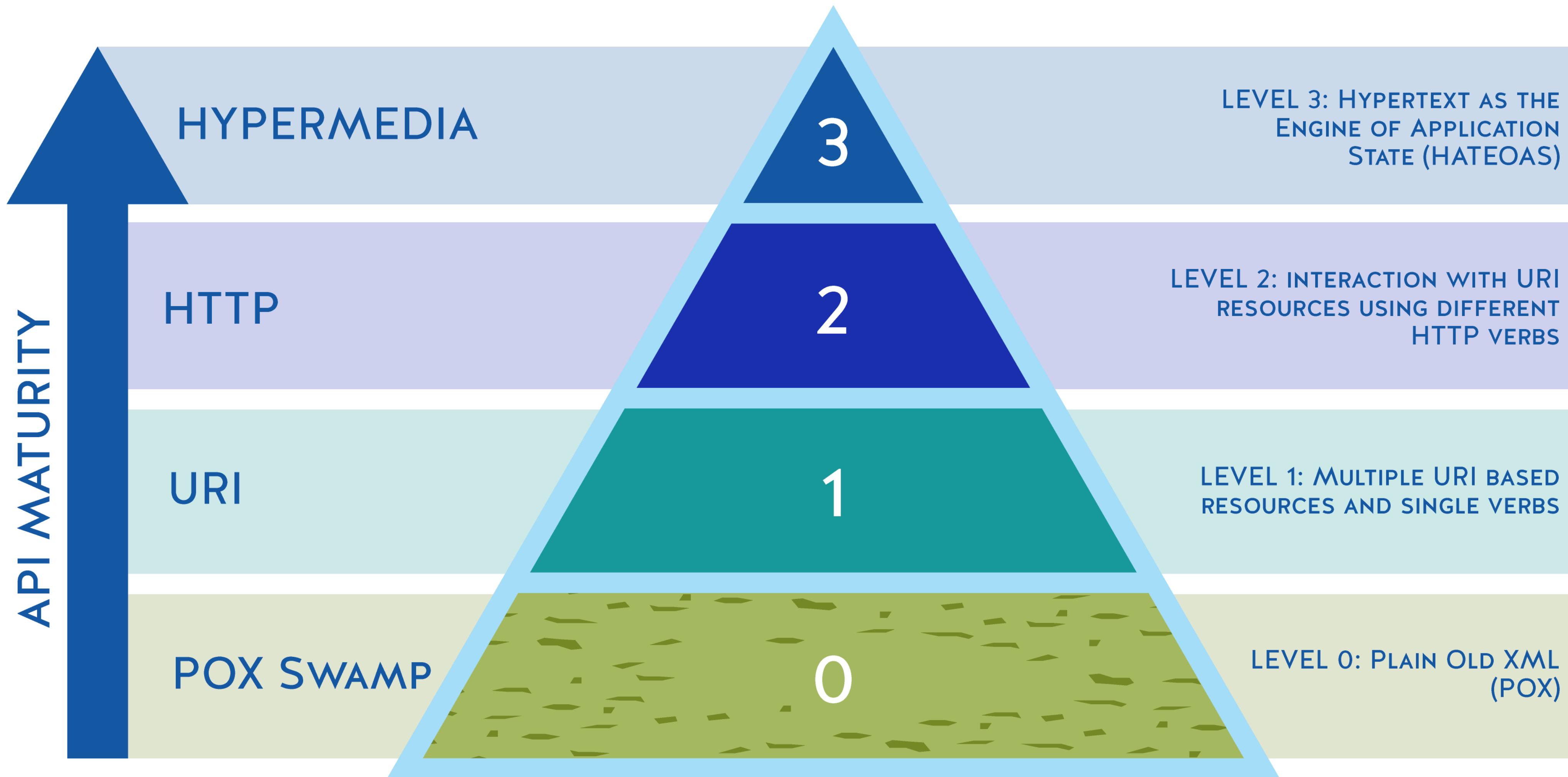
FACULDADE DE  
CIÊNCIAS E TECNOLOGIA  
UNIVERSIDADE NOVA DE LISBOA

# RESTful design

- Resource = object or representation of something
- Collection = a set of resources
- URI = a path identifying **resources** and allowing actions on them
- URL methods represents standardised actions
  - GET = request resources
  - POST = create resources
  - PUT = update or create resources
  - DELETE = deletes resources
- HTTP Response codes = operation results
  - 20x Ok
  - 3xx Redirection (not modified)
  - 400 Bad Request, 401 Unauthorized, 403 Forbidden, 404 Not Found
  - 5xx Server Error
- Searching, sorting, filtering and pagination obtained by query string parameters
- Text Based Data format (JSON, or XML)

<https://hackernoon.com/restful-api-designing-guidelines-the-best-practices-60e1d954e7c9>

# THE RICHARDSON MATURITY MODEL



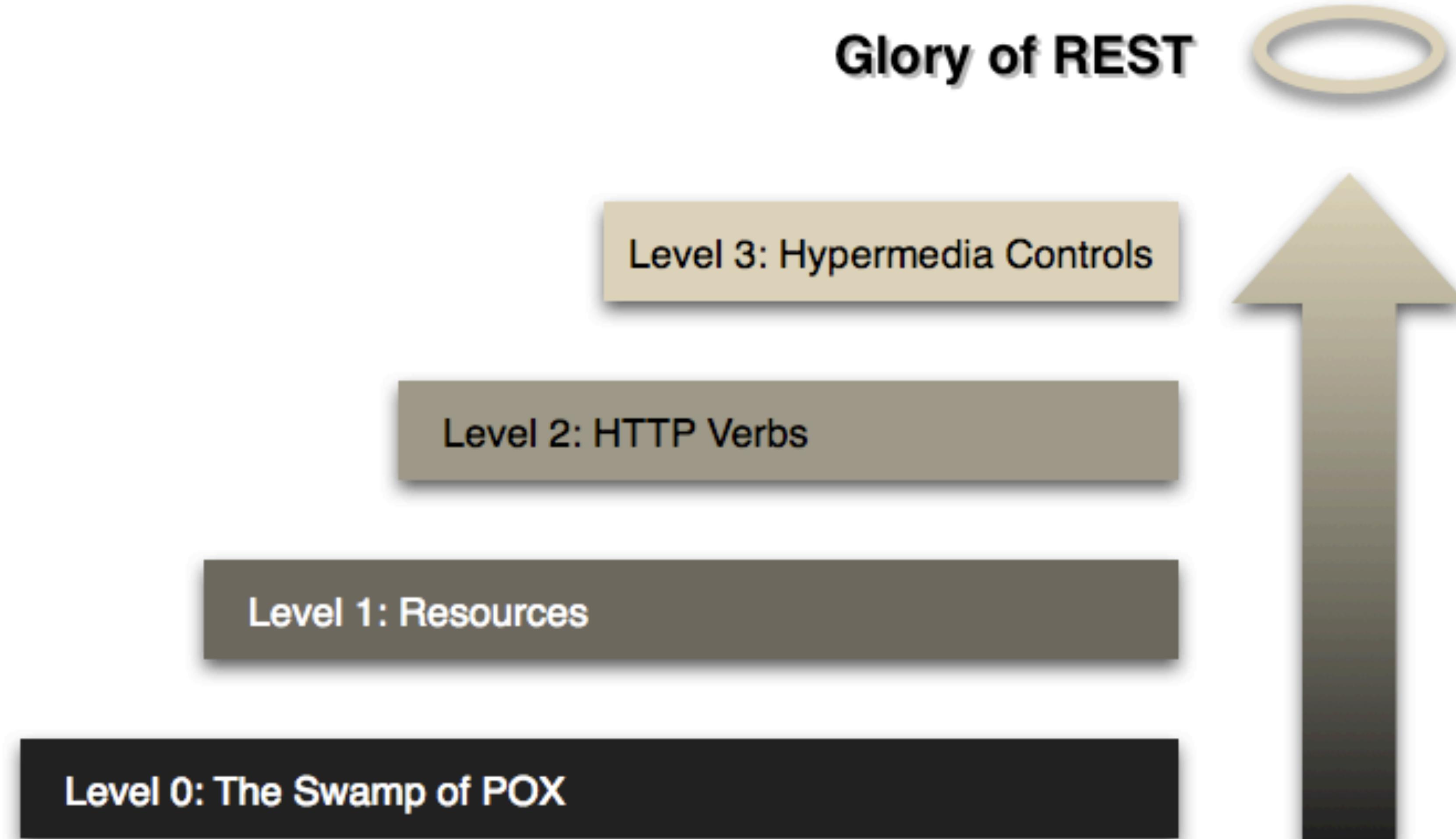
<https://martinfowler.com/articles/richardsonMaturityModel.html>

<http://restcookbook.com/Miscellaneous/richardsonmaturitymodel/>

NORDICAPIS.COM



# Richardson Maturity Model



<https://martinfowler.com/articles/richardsonMaturityModel.html>

<http://restcookbook.com/Miscellaneous/richardsonmaturitymodel/>



# The Richardson Maturity Model - Level 0

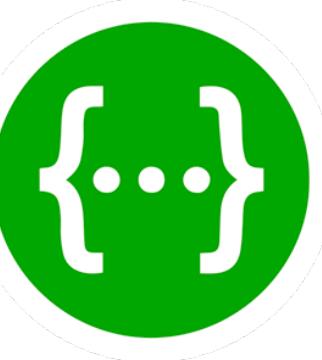
- POX Swamp
  - To send an XML/JSON that contains everything: operation, arguments, options

POST /appointmentService HTTP/1.1  
[various other headers]

<openSlotRequest date = "2010-01-04" doctor = "mjones"/>

```
<openSlotList>
    <slot start = "1400" end = "1450">
        <doctor id = "mjones"/>
    </slot>
    <slot start = "1600" end = "1650">
        <doctor id = "mjones"/>
    </slot>
</openSlotList>
```

# The Richardson Maturity Model - Level 0



- POX Swamp
  - To send an XML/JSON that contains everything: operation, arguments, options

POST /appointmentService HTTP/1.1

[various other headers]

```
<appointmentRequest>
  <slot doctor = "mjones" start = "1400" end = "1450"/>
  <patient id = "jsmith"/>
</appointmentRequest>
```

HTTP/1.1 200 OK

[various headers]

```
<appointmentRequestFailure>
```

```
  <slot doctor = "mjones" start = "1400" end = "1450"/>
  <patient id = "jsmith"/>
  <reason>Slot not available</reason>
</appointmentRequestFailure>
```



# The Richardson Maturity Model - Level 1

- Multiple URI Based Resources and Single verbs

POST /doctors/mjones HTTP/1.1  
[various other headers]

HTTP/1.1 200 OK  
[various headers]

<openSlotRequest date = "2010-01-04"/>

<openSlotList>  
  <slot id = "1234" doctor = "mjones" start = "1400" end = "1450"/>  
  <slot id = "5678" doctor = "mjones" start = "1600" end = "1650"/>  
</openSlotList>

POST /slots/1234 HTTP/1.1  
[various other headers]

HTTP/1.1 200 OK  
[various headers]

<appointmentRequest>  
  <patient id = "jsmith"/>  
</appointmentRequest>

<appointment>  
  <slot id = "1234" doctor = "mjones" start = "1400" end = "1450"/>  
  <patient id = "jsmith"/>  
</appointment>



# The Richardson Maturity Model - Level 1

- Multiple URI Based Resources and Single verbs

```
@Controller @RequestMapping(value = "/pets")
class PetController @Autowired constructor (val db: MongoDB) {
    @RequestMapping(value = "/add", method = arrayOf(RequestMethod.GET))
    public fun add(@RequestParam("ownerId") ownerIdParam: String, model: Model): String {
        db.withSession {
            val owner = Owners.find { id.equal(Id(ownerIdParam)) }.single()
            model.addAttribute("owner", owner)
            val petTypes = PetTypes.find().toList()
            model.addAttribute("petTypes", petTypes)
        }
        return "pets/add"
    }
}
```



# The Richardson Maturity Model - Level 2

- Interaction with URI resources using different HTTP verbs

```
GET /doctors/mjones/slots?date=20100104&status=open HTTP/1.1
```

```
Host: royalhope.nhs.uk
```

```
HTTP/1.1 200 OK
```

```
[various headers]
```

```
<openSlotList>
  <slot id = "1234" doctor = "mjones" start = "1400" end = "1450"/>
  <slot id = "5678" doctor = "mjones" start = "1600" end = "1650"/>
</openSlotList>
```



# The Richardson Maturity Model - Level 2

- Interaction with URI resources using different HTTP verbs

```
POST /slots/1234 HTTP/1.1  
[various other headers]
```

```
<appointmentRequest>  
  <patient id = "jsmith"/>  
</appointmentRequest>
```

```
HTTP/1.1 201 Created  
Location: slots/1234/appointment  
[various headers]
```

```
<appointment>  
  <slot id = "1234" doctor = "mjones" start = "1400" end = "1450"/>  
  <patient id = "jsmith"/>  
</appointment>
```

# The Richardson Maturity Model - Level 3



- Interaction with URI resources using different HTTP verbs

HTTP/1.1 201 Created

Location: slots/1234/appointment

[various headers]

POST /slots/1234 HTTP/1.1

[various other headers]

```
<appointmentRequest>
  <patient id = "jsmith"/>
</appointmentRequest>
```

```
<appointment>
  <slot id = "1234" doctor = "mjones" start = "1400" end = "1450"/>
  <patient id = "jsmith"/>
</appointment>
```

HTTP/1.1 409 Conflict

[various headers]

```
<openSlotList>
  <slot id = "5678" doctor = "mjones" start = "1600" end = "1650"/>
</openSlotList>
```



# The Richardson Maturity Model - Level 4

- Hypermedia Controls - HATEOAS
  - Resources are interconnected by links in the response, one entry point

```
GET /doctors/mjones/slots?date=20100104&status=open HTTP/1.1
```

```
Host: royalhope.nhs.uk
```

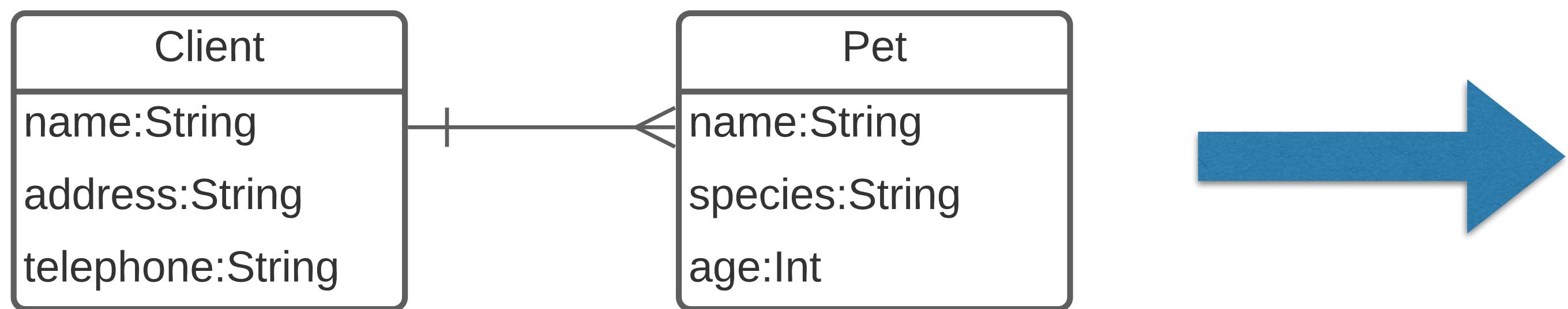
```
HTTP/1.1 200 OK
```

```
[various headers]
```

```
<openSlotList>
  <slot id = "1234" doctor = "mjones" start = "1400" end = "1450">
    <link rel = "/linkrels/slot/book"
          uri = "/slots/1234"/>
  </slot>
  <slot id = "5678" doctor = "mjones" start = "1600" end = "1650">
    <link rel = "/linkrels/slot/book"
          uri = "/slots/5678"/>
  </slot>
</openSlotList>
```

# REST = Resource state transformation

- The resources that are provided by the API do not have to map the structure of the internal system state.
- Provided resources may have a nested structure that results from a relational structure of several database tables.



```
[{"name": "joe",
  "address": "London, UK",
  "telephone": "555000222",
  "pets": [
    {"name": "Max",
     "species": "Canis lupus familiaris",
     "age": 3},
    {"name": "Max",
     "species": "Canis lupus familiaris",
     "age": 3}
  ],
  {"name": "mary",
  "address": ..... }]
```

# Internet Applications Design and Implementation

2020 - 2021

(Lecture 3 - Part 2 - Server-side MVC Architecture)

**MIEI - Integrated Master in Computer Science and Informatics  
Specialization block**

**João Costa Seco ([joao.seco@fct.unl.pt](mailto:joao.seco@fct.unl.pt))**

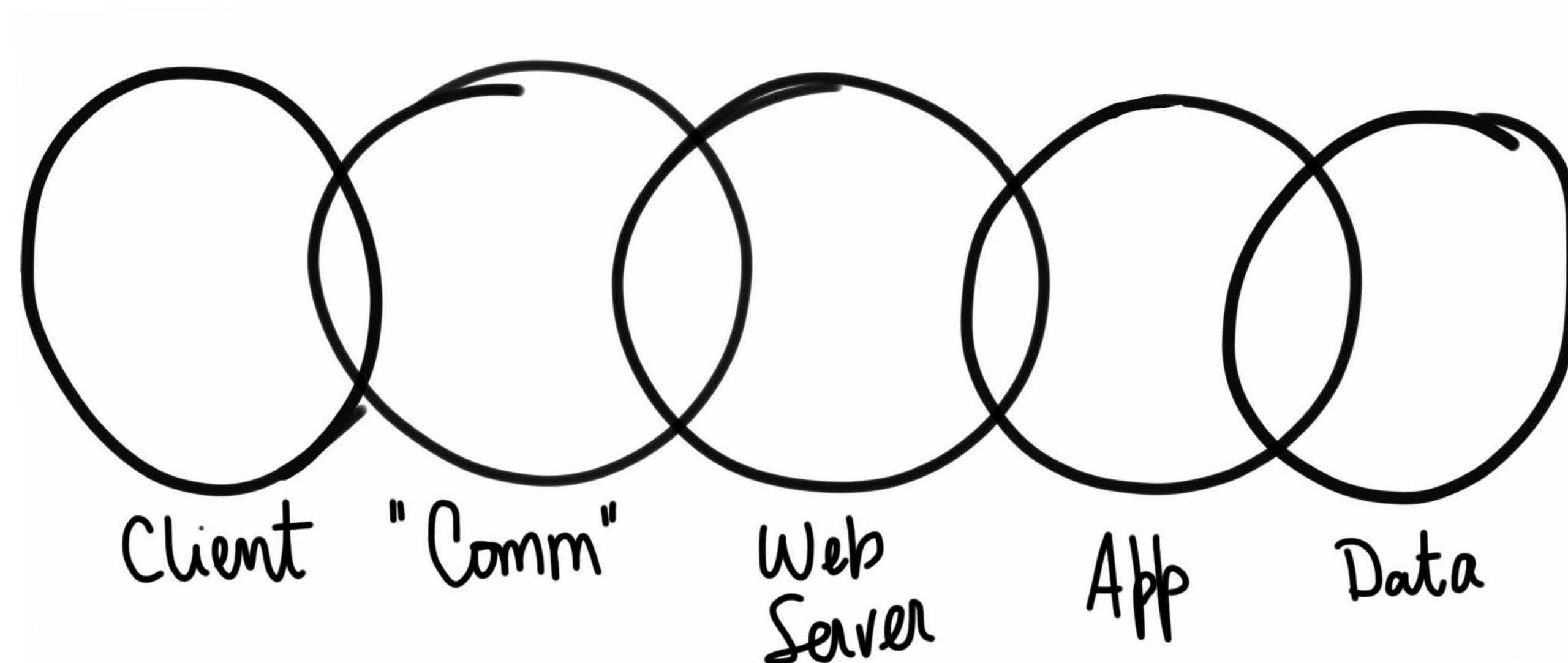
(with previous participations of Jácome Cunha ([jacome@fct.unl.pt](mailto:jacome@fct.unl.pt)) and João Leitão ([jc.leitao@fct.unl.pt](mailto:jc.leitao@fct.unl.pt)))



FACULDADE DE  
CIÊNCIAS E TECNOLOGIA  
UNIVERSIDADE NOVA DE LISBOA

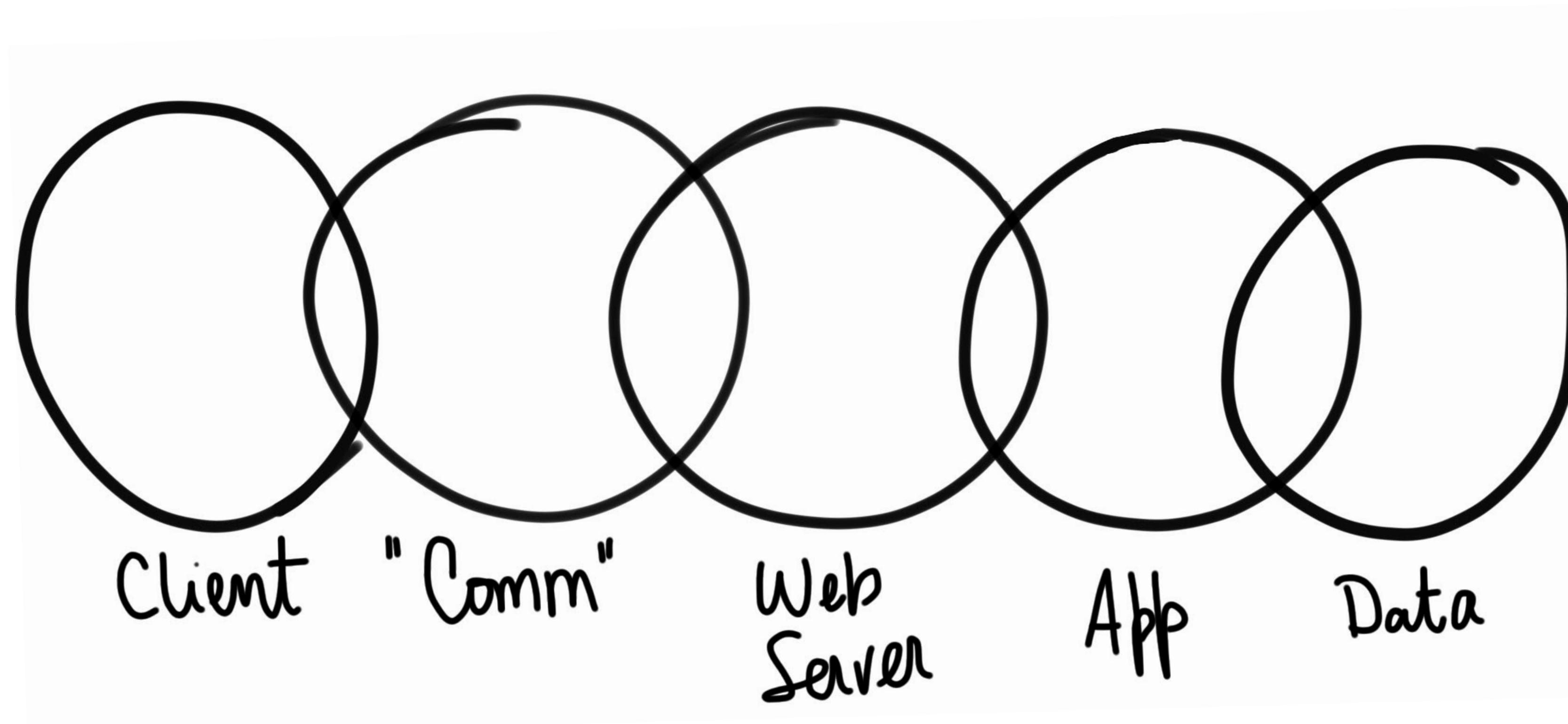
# Web architectures, patterns and styles

- Web applications usually follow a MVC architectural pattern.
  - Model layer - isolate the representation of persistent data and its operations, validations and conditions
  - Controller - contains the core application logic implementing the application interface (e.g. ad-hoc URL mapping, REST convention)
  - View - defines the way in which responses are formed (e.g. HTML, JSON)



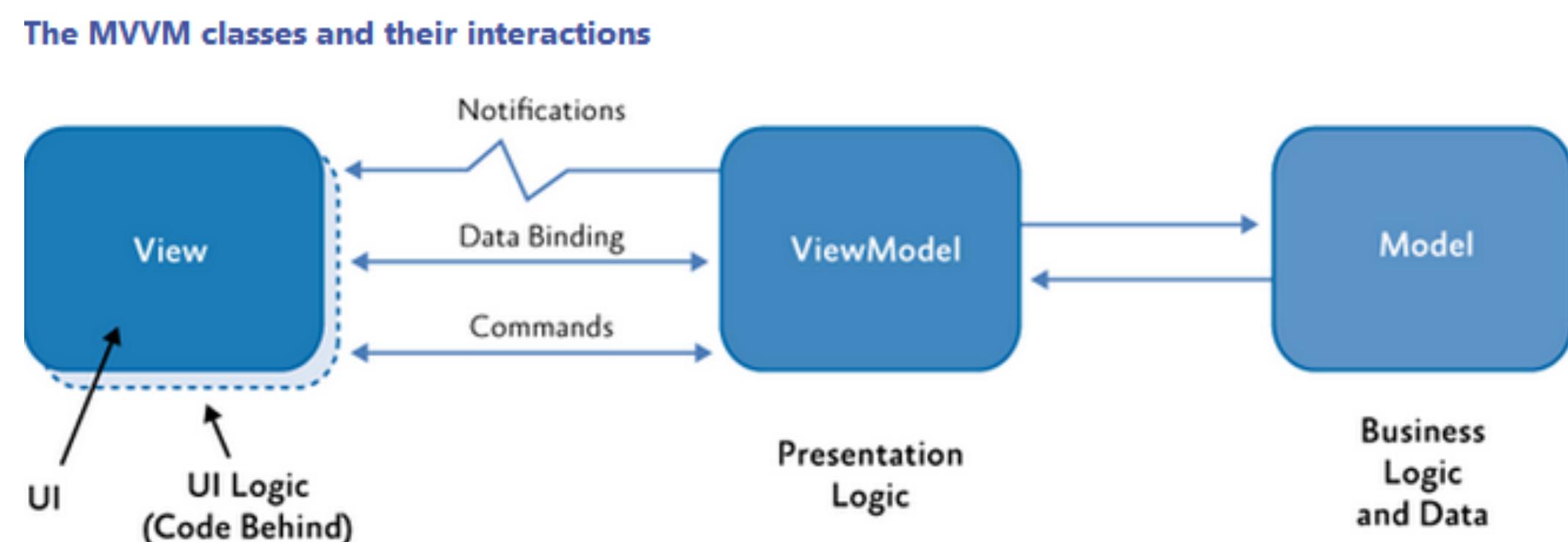
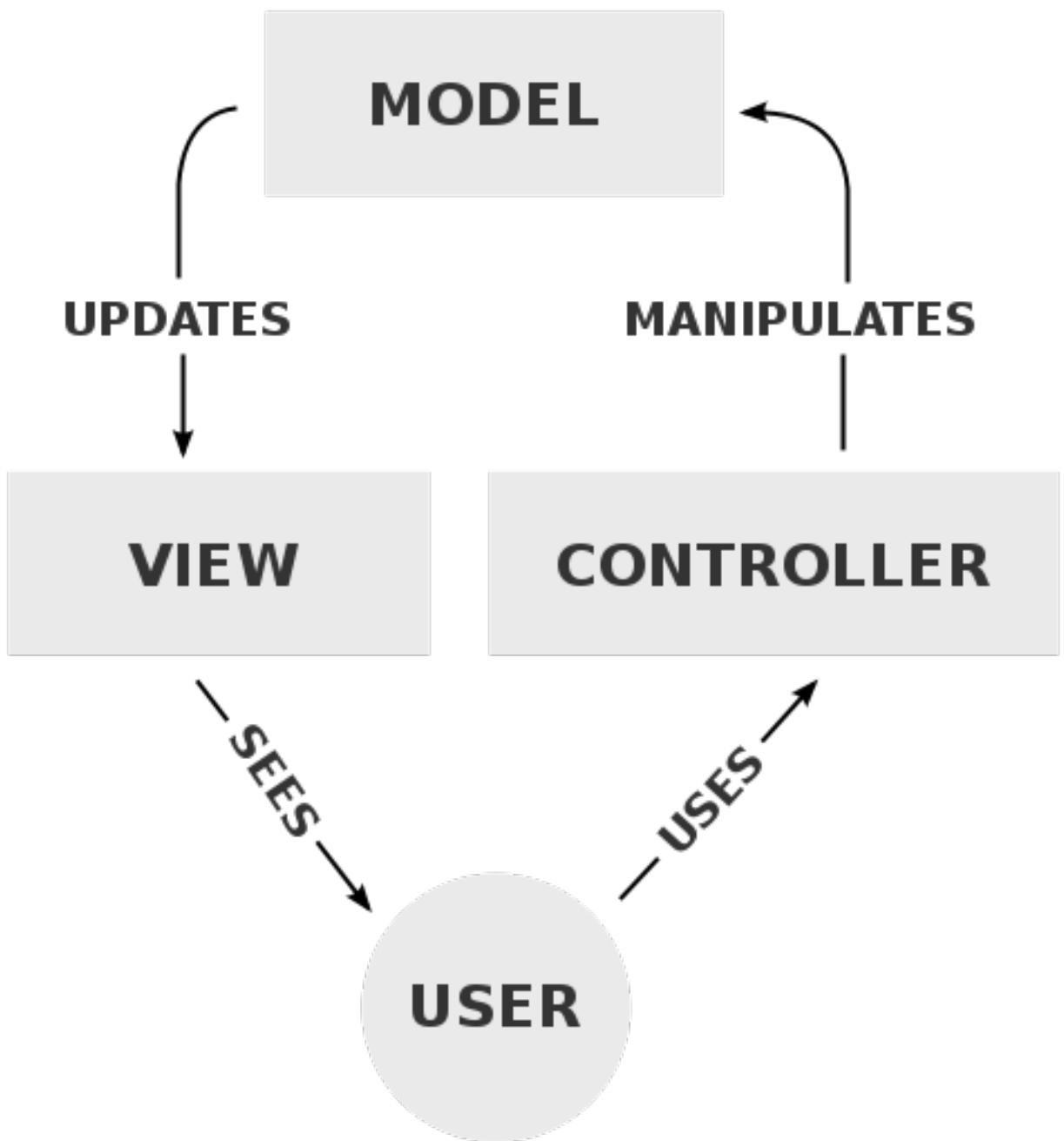
# Summary - Web Frameworks

- Web Frameworks are “languages” that carry libraries and abstractions that get compiled to run on the “web virtual machine”.



# The classic MVC design pattern

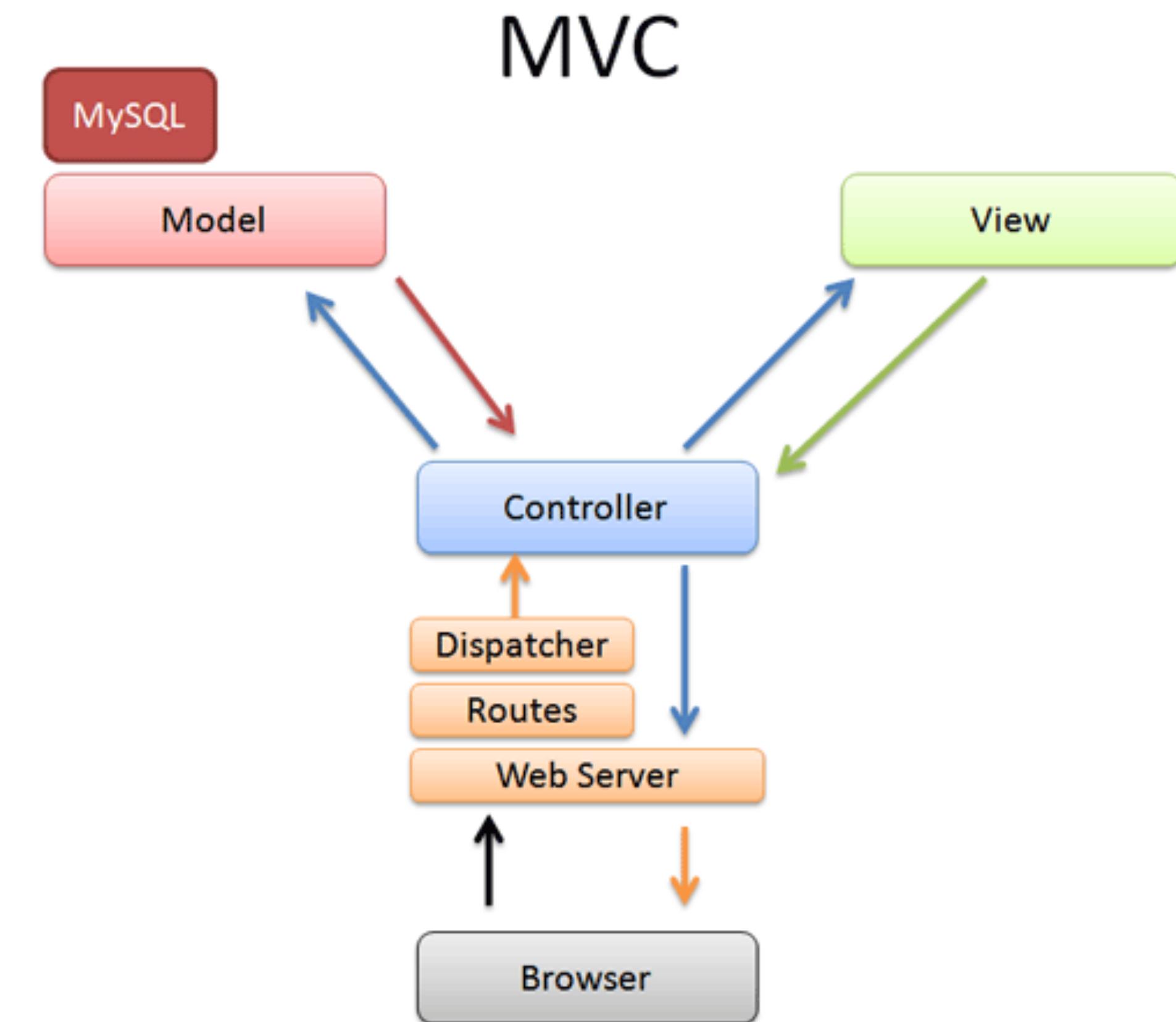
- The Model-View-Controller (Reenskaug'79, JOT'88)
  - designed to develop GUI
  - popular in web applications' context
- Variants of the MVC Architecture (Separation of Concerns)
  - MVP, PM (Fowler), MVVM (Microsoft)



<https://manojjaggavarapu.wordpress.com/2012/05/02/presentation-patterns-mvc-mvp-pm-mvvm/>

# Frameworks and MVC Architecture

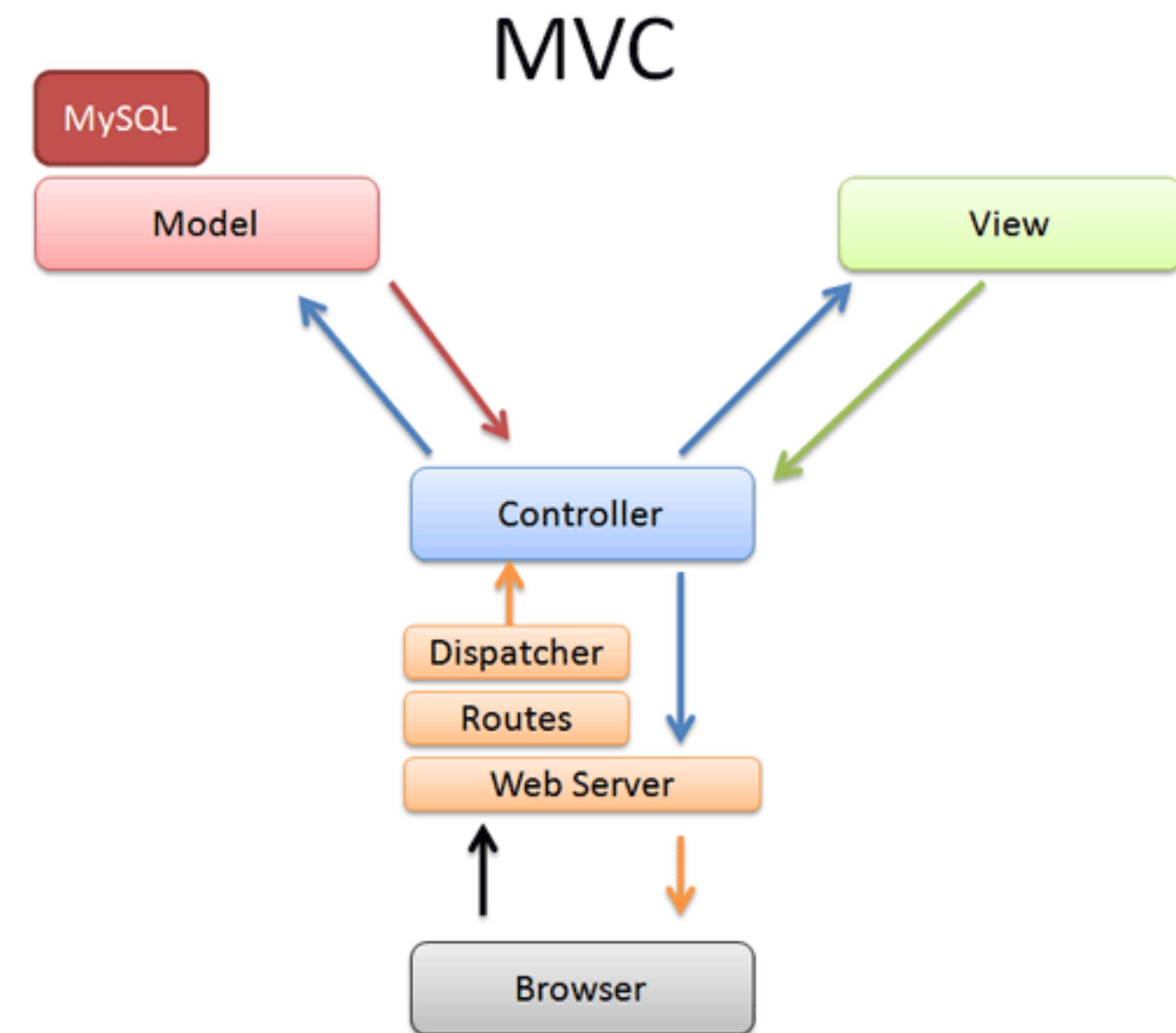
- Frameworks help to implement and maintain architectures.
- Rails (2005):
  - conventions on folder, file, and class names
  - A flexible OO prog language (Ruby) supports data sharing between model, controller, and view objects.



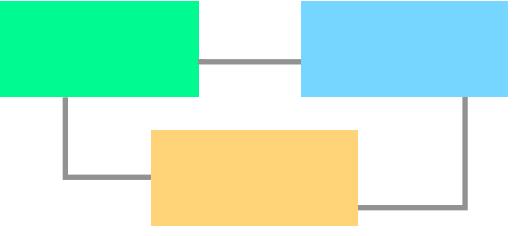
<https://betterexplained.com/articles/intermediate-rails-understanding-models-views-and-controllers/>

# Frameworks and MVC Architecture

- Frameworks help to implement and maintain architectures.
- Django (2005):
  - views are controllers
  - templates are views
  - models are models



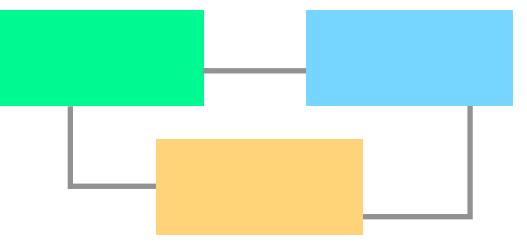
<https://betterexplained.com/articles/intermediate-rails-understanding-models-views-and-controllers/>



# Frameworks and MVC Architecture

- Java Spring is a component-based programming framework (based on configuration).
- It does the “plumbing,” and lets components implement the “logic” of applications.
- How spring implements the MVC
  - Dependency Injection (inversion of control)
  - Aspect-Oriented Programming including Spring's declarative transaction management
  - Spring MVC web application and RESTful web service framework
  - Foundational support for JDBC, JPA, JMS
  - ...

<https://spring.io/guides/>



# Inversion of Control

---

- Design pattern where user-defined code fragment receives the flow of control from a generic framework.
  - Context: object-oriented programming
  - Found in: Frameworks, Event handlers, Callbacks
- Dependency Injection
  - An instance of inversion of control to build object networks
  - Centralised broker that maps types to implementations
  - Java Spring: Pool of beans/components, auto-wiring of object networks

# Without inversion of Control



- Explicit initialisation of references

```
@RestController
@RequestMapping("/")
class EmpController(val employees:EmployeeService) {

    @GetMapping("/api/departments/{id}/employees")
    fun employeesOfDepartment(
        @PathVariable id:String,
        @RequestParam search:String?
    )
    = listOf(
        Employee("John Oliver",40,"New York"),
        Employee("John Gleese", 60, "London")
    )

    @GetMapping( "/api/projects/{id}/team")
    fun teamMembersOfProject(
        @PathVariable id:String
    )
    = employees.teamMembersOfProject(id)

}
```

```
@Service
class EmployeeService(val employees:EmployeeRepository) {
    fun teamMembersOfProject(id:String) = employees.findAll()
}

interface EmployeeRepository : CrudRepository<Employee, Long>

fun someMethod() {
    EmpController(
        EmployeeService(
            EmployeeRepositoryImp(
                DBConnection("..."))
        )
    )
}
```



# Without inversion of Control

- Explicit initialisation of references

```
package pt.unl.fct.demo.controllers;

import org.springframework.web.bind.annotation.*;
import pt.unl.fct.demo.model.Company;
import pt.unl.fct.demo.services.CompaniesService;

@RestController
@RequestMapping(value="/companies")
public class CompaniesController {
    CompaniesService companies;

    public CompaniesController(CompaniesService companies) {
        this.companies = companies;
    }

    @GetMapping("")
    Iterable<Company> getAllCompanies(@RequestParam(required=false) String search) {
        // Do some extra checking on the request, and then...
        return companies.getAllCompanies(search);
    }

    @PostMapping("")
    void addNewCompany(@RequestBody Company company) {
        // Do some extra checking on the request, and then...
        companies.addCompany(company);
    }
}
```

Spring uses annotations to indicate the kind of class, and where to plug it in

# Without inversion of Control

- Explicit initialisation of references

```
package pt.unl.fct.demo.controllers;

import org.springframework.web.bind.annotation.*;
import pt.unl.fct.demo.model.Company;
import pt.unl.fct.demo.services.CompaniesService;

@RestController
@RequestMapping(value="/companies")
public class CompaniesController {
    CompaniesService companies;

    public CompaniesController(CompaniesService companies) {
        this.companies = companies;
    }

    @GetMapping("")
    Iterable<Company> getAllCompanies(@RequestParam(required=false) String search) {
        // Do some extra checking on the request, and then...
        return companies.getAllCompanies(search);
    }

    @PostMapping("")
    void addNewCompany(@RequestBody Company company) {
        // Do some extra checking on the request, and then...
        companies.addCompany(company);
    }
}
```

Instead of doing it explicitly ->>

```
import javax.servlet.http.*;
import javax.servlet.*;
import java.io.*;

public class DemoServ extends HttpServlet{
    public void doGet(HttpServletRequest req,
                      HttpServletResponse res)
        throws ServletException, IOException
    {
        res.setContentType("text/html");
        PrintWriter pw=res.getWriter();

        String name=req.getParameter("name");
        pw.println("Welcome "+name);

        pw.close();
    }
}
```

from: <https://www.javatpoint.com/servletrequest>

# Without inversion of Control

- Explicit initialisation of references

```
package pt.unl.fct.demo.controllers;

import org.springframework.web.bind.annotation.*;
import pt.unl.fct.demo.model.Company;
import pt.unl.fct.demo.services.CompaniesService;

@RestController
@RequestMapping(value="/companies")
public class CompaniesController {

    CompaniesService companies;

    public CompaniesController(CompaniesService companies) {
        this.companies = companies;
    }

    @GetMapping("")
    Iterable<Company> getAllCompanies(@RequestParam(required=false) String search) {
        // Do some extra checking on the request, and then...
        return companies.getAllCompanies(search);
    }

    @PostMapping("")
    void addNewCompany(@RequestBody Company company) {
        // Do some extra checking on the request, and then...
        companies.addCompany(company);
    }
}
```

resources in ruby'nrails  
a whole DSL to define >>  
routes



creates seven different routes in your application, all mapping to the `Photos` controller:

HTTP Verb	Path	Controller#Action	Used for
GET	/photos	photos#index	display a list of all photos
GET	/photos/new	photos#new	return an HTML form for creating a new photo
POST	/photos	photos#create	create a new photo
GET	/photos/:id	photos#show	display a specific photo
GET	/photos/:id/edit	photos#edit	return an HTML form for editing a photo
PATCH/PUT	/photos/:id	photos#update	update a specific photo
DELETE	/photos/:id	photos#destroy	delete a specific photo

<https://guides.rubyonrails.org/routing.html>



# Using Dependency Injection

- Explicitly tell what things are, let spring do the wiring

```
@RestController  
@RequestMapping("/")  
class EmpController {  
  
    @Autowired  
    lateinit var employees:EmployeeService  
  
    @GetMapping("/api/departments/{id}/employees")  
    fun employeesOfDepartment(  
        @PathVariable id:String,  
        @RequestParam search:String?  
    )
```

Declare dependencies explicitly  
to be initialised by Spring



# Using Dependency Injection

- Explicitly tell what things are, let spring do the wiring

```
@RestController  
@RequestMapping("/")  
class EmpController(val employees:EmployeeService) {
```

Declare constructor dependencies  
and let Spring initialise correctly

```
@GetMapping("/api/departments/{id}/employees")  
fun employeesOfDepartment(  
    @PathVariable id:String,  
    @RequestParam search:String?  
)
```

# Frameworks and MVC Architecture

---

- Java Spring is a component-based programming framework (based on configuration).
- It does the “plumbing,” and lets components implement the “logic” of applications.
- How spring implements the MVC:

```
@SpringBootApplication  
class McqApplication  
  
fun main(args: Array<String>) {  
    runApplication<McqApplication>(*args)  
}
```

# Frameworks and MVC Architecture

- Java Spring is a configuration and programming framework.
- It does the “plumbing”, and lets the components implement the “logic” of applications.
- How spring implements the MVC: (in Java)

```
@Configuration  
@EnableAutoConfiguration  
@EnableWebMvc  
@ComponentScan  
public class Application {  
  
    public static void main(String[] args) {  
        SpringApplication.run(Application.class, args);  
    }  
}
```

**@Configuration**

Annotation specifies that the class has Bean definition methods

# Frameworks and MVC Architecture

- Java Spring is a configuration and programming framework.
- It does the “plumbing”, and lets the components implement the “logic” of applications.
- How spring implements the MVC

```
@Configuration  
@EnableAutoConfiguration  
@EnableWebMvc  
@ComponentScan  
public class Application {  
  
    public static void main(String[] args) {  
        SpringApplication.run(Application.class, args);  
    }  
}
```

`@EnableAutoConfiguration`

Attempts to guess and configure beans that you are likely to need ([doc.spring.io](http://doc.spring.io))

# Frameworks and MVC Architecture

- Java Spring is a configuration and programming framework.
- It does the “plumbing”, and lets the components implement the “logic” of applications.
- How spring implements the MVC

```
@Configuration  
@EnableAutoConfiguration  
@EnableWebMvc  
@ComponentScan  
public class Application {  
  
    public static void main(String[] args) {  
        SpringApplication.run(Application.class, args);  
    }  
}
```

## @ComponentScan

Configures component scanning. If specific packages are not defined, scanning will occur from the package of the class that declares this annotation.

# Frameworks and MVC Architecture

- Java Spring is a configuration and programming framework.
- It does the “plumbing”, and lets the components implement the “logic” of applications.
- How spring implements the MVC (Here the view is an HTML (thymeleaf) template)

```
@Controller
public class GreetingController {

    private static final String template = "Hello, %s! %d";
    private final AtomicLong counter = new AtomicLong();

    @RequestMapping("/greeting")
    public String greeting(@RequestParam(value="name", defaultValue="World") String name,
                          Model model) {
        long c = counter.incrementAndGet();
        model.addAttribute("message", String.format(template, name, c));
        return "greeting";
    }
}
```

# Frameworks and MVC Architecture

- Java Spring is a configuration and programming framework.
- It does the “plumbing”, and lets the components implement the “logic” of applications.
- How spring implements the MVC (Here the view is a JSON object formatter)

```
@RestController
public class GreetingController {

    private static final String template = "Hello, %s!";
    private final AtomicLong counter = new AtomicLong();

    @RequestMapping("/greeting")
    public Greeting greeting(@RequestParam(value="name", defaultValue="World") String name) {
        return new Greeting(counter.incrementAndGet(),
                            String.format(template, name));
    }
}
```

# Add-ons to the MVC Framework

- Resource control:  
DB connection &  
transactions

```
@Component
public class BookingService {

    private final static Logger logger = LoggerFactory.getLogger(BookingService.class);

    private final JdbcTemplate jdbcTemplate;

    public BookingService(JdbcTemplate jdbcTemplate) {
        this.jdbcTemplate = jdbcTemplate;
    }

    @Transactional
    public void book(String... persons) {
        for (String person : persons) {
            logger.info("Booking " + person + " in a seat...");
            jdbcTemplate.update("insert into BOOKINGS(FIRST_NAME) values (?)", person);
        }
    }

    public List<String> findAllBookings() {
        return jdbcTemplate.query("select FIRST_NAME from BOOKINGS",
                (rs, rowNum) -> rs.getString("FIRST_NAME"));
    }

}
```

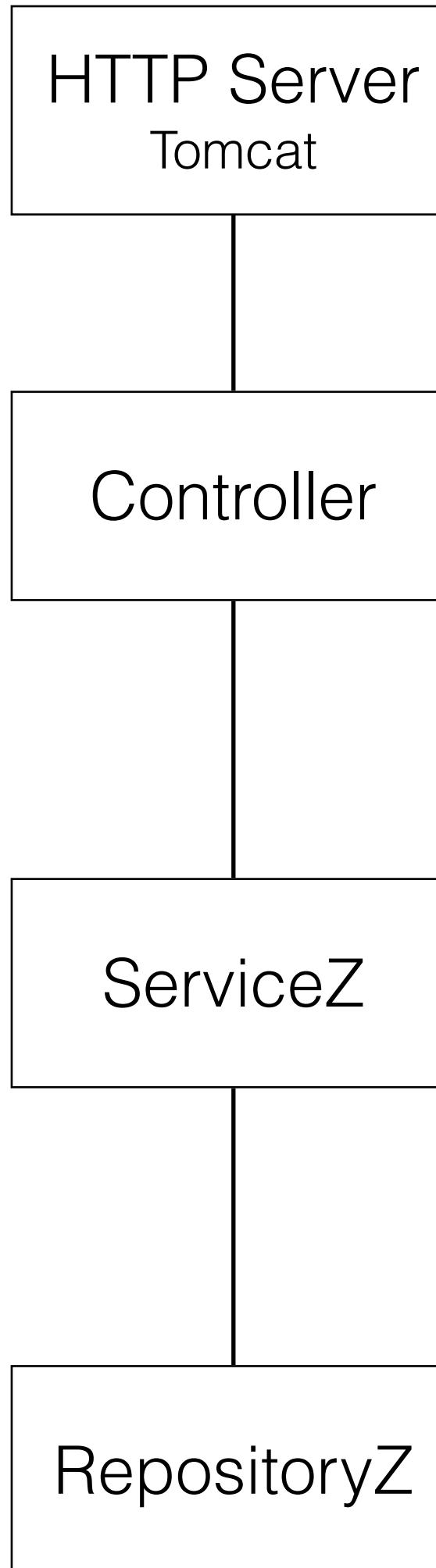
# Add-ons to the MVC Framework

- Across application concerns: security

```
@Configuration  
@EnableWebSecurity  
public class WebSecurityConfig extends WebSecurityConfigurerAdapter {  
    @Override  
    protected void configure(HttpSecurity http) throws Exception {  
        http  
            .authorizeRequests()  
                .antMatchers("/", "/home").permitAll()  
                .anyRequest().authenticated()  
                .and()  
            .formLogin()  
                .loginPage("/login")  
                .permitAll()  
                .and()  
            .logout()  
                .permitAll();  
    }  
}
```

```
@Autowired  
public void configureGlobal(AuthenticationManagerBuilder auth) throws Exception {  
    auth  
        .inMemoryAuthentication()  
            .withUser("user").password("password").roles("USER");  
}
```

# Example of an Architecture built with Spring



- Spring is a component framework
- Resolves component dependencies by dependency injection
- Uses annotations to configure components

```
@RestController  
@RequestMapping("/")  
class EmpController(val employees:EmployeeService) {  
  
    // http GET :8080/api/projects/2/team  
    @GetMapping( "/api/projects/{id}/team")  
    fun teamMembersOfProject(  
        @PathVariable id:String  
    )  
        = employees.teamMembersOfProject(id)  
  
    }  
  
@Service  
class EmployeeService(val employees:EmployeeRepository) {  
    fun teamMembersOfProject(id:String) = employees.findAll()  
}  
  
interface EmployeeRepository : CrudRepository<Employee, Long>
```



# Architecture to the rescue of testers

- Unit tests should test components in isolation
- Defining the context for a component (correctly) is laborious and error prone
- Difficult to do with persistent data (must prepare tests)
- Impossible to do in tightly coupled structures
- Component frameworks allow mocking of dependencies

```
@RunWith(SpringRunner::class)
@SpringBootTest
@AutoConfigureMockMvc
open class RESTApplicationTests() {

    @Autowired lateinit var mvc: MockMvc
    @MockBean lateinit var questions: QuestionRepository

    @Test
    fun `basic REST test`() {
        Mockito.`when`(questions.findAll()).thenReturn(1)

        mvc.perform(get(questionsURL))
            .andExpect(status().isOk)
    }
}
```



# Architecture to the rescue of testers

```
@RunWith(SpringRunner::class)
@SpringBootTest
@AutoConfigureMockMvc
open class RESTApplicationTests() {

    @Autowired lateinit var mvc: MockMvc
    @MockBean lateinit var questions: QuestionRepository

    @Test
    fun `basic REST test`() {
        Mockito.`when`(questions.findAll()).thenReturn(1)

        mvc.perform(get(questionsURL))
            .andExpect(status().isOk)
    }
}
```

Replaces web server

`@Autowired lateinit var mvc: MockMvc`

`@MockBean lateinit var questions: QuestionRepository`

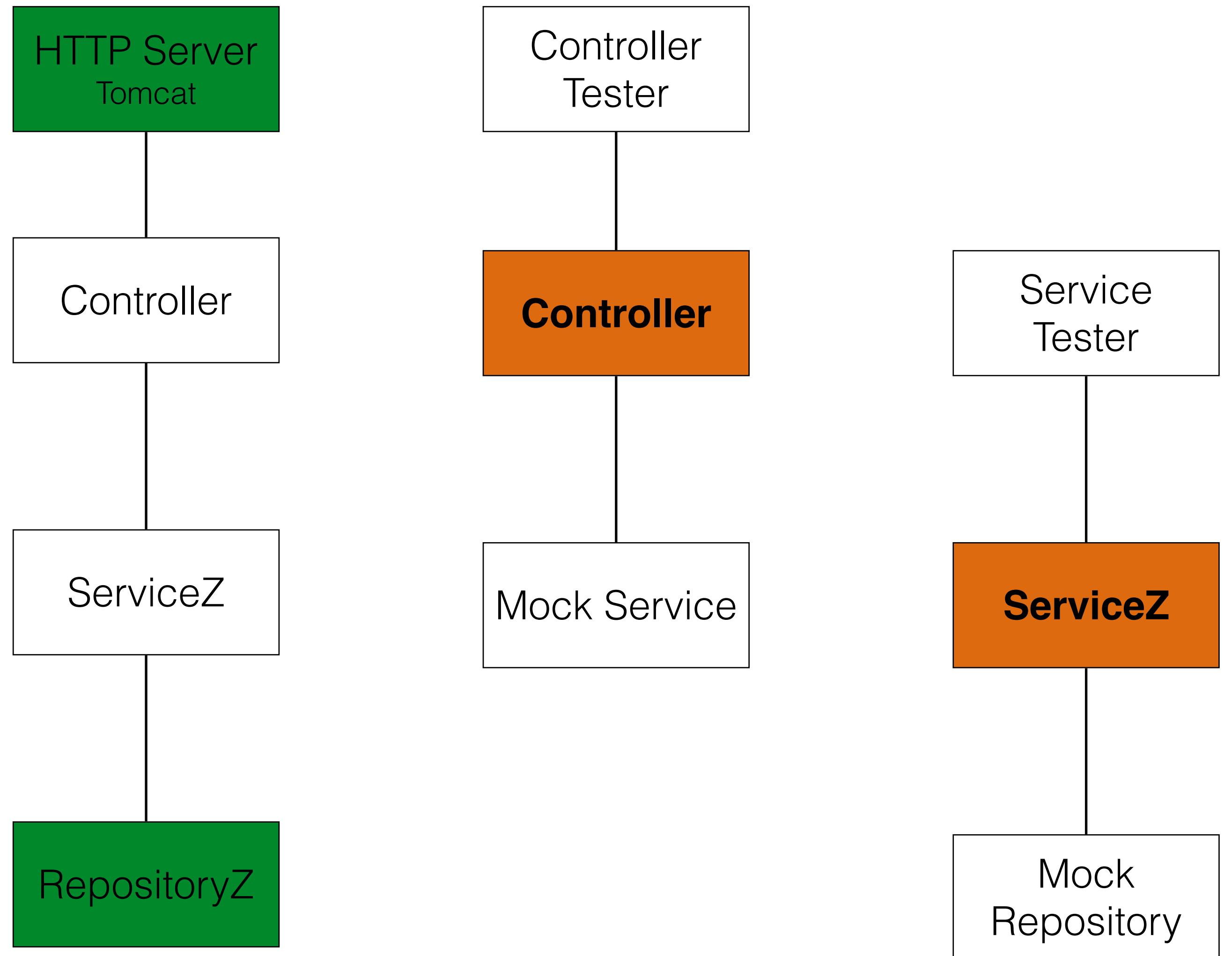
Replaces component with Mock object

Replaces call results with expected values



# Architecture to the rescue of testers

- Unit tests should test components in isolation
- Unit tests simulate inputs and compare outputs
- Mock components create a controlled context for each test or set of tests.



# Internet Applications Design and Implementation

2020 - 2021

(Lecture 3 - Part 3 - Data Sources in MVC)

**MIEI - Integrated Master in Computer Science and Informatics  
Specialization block**

**João Costa Seco ([joao.seco@fct.unl.pt](mailto:joao.seco@fct.unl.pt))**

(with previous participations of Jácome Cunha ([jacome@fct.unl.pt](mailto:jacome@fct.unl.pt)) and João Leitão ([jc.leitao@fct.unl.pt](mailto:jc.leitao@fct.unl.pt)))



FACULDADE DE  
CIÊNCIAS E TECNOLOGIA  
UNIVERSIDADE NOVA DE LISBOA

# Data Abstraction: The M in MVC

---

- An application layer that abstracts how information is stored, related, and protected.
- Examples of database languages, libraries and frameworks
  - JDBC
  - LINQ (in MVC ASP.NET)
  - ORMs (ActiveRecord in Rails, Hibernate in Java\*)
  - NoSQL: MongoDB
  - External Web-services

# JDBC

```
Connection conn = DriverManager.getConnection(
    "jdbc:somejdbcvendor:other data needed by some jdbc vendor",
    "myLogin",
    "myPassword" );
try {
    /* you use the connection here */
} finally {
    //It's important to close the connection when you are done with it
    try { conn.close(); } catch (Throwable ignore) { /* Propagate the original exception
instead of this one that you may want just logged */ }
}

try (Statement stmt = conn.createStatement();
      ResultSet rs = stmt.executeQuery( "SELECT * FROM MyTable" )
) {
    while ( rs.next() ) {
        int numColumns = rs.getMetaData().getColumnCount();
        for ( int i = 1 ; i <= numColumns ; i++ ) {
            // Column numbers start at 1.
            // Also there are many methods on the result set to return
            // the column as a particular type. Refer to the Sun documentation
            // for the list of valid conversions.
            System.out.println( "COLUMN " + i + " = " + rs.getObject(i) );
        }
    }
}
```

- Basic API for Java defining an access to a database
- Does not know the database schema
- Programmer needs to “manually” translate between data formats

```
try (Statement stmt = conn.createStatement();
      ResultSet rs = stmt.executeQuery( "SELECT * FROM MyTable" )
) {
    while ( rs.next() ) {
        int numColumns = rs.getMetaData().getColumnCount();
        for ( int i = 1 ; i <= numColumns ; i++ ) {
            // Column numbers start at 1.
            // Also there are many methods on the result set to return
            // the column as a particular type. Refer to the Sun documentation
            // for the list of valid conversions.
            System.out.println( "COLUMN " + i + " = " + rs.getObject(i) );
        }
    }
}
```

- Language based (integrated)
- Works in memory, xml, databases, etc
  - Based on the notion of **Provider**, it is extensible
- Programmers need to explicitly build objects that matches the database schema

```
var results = from c in SomeCollection
               where c.SomeProperty < 10
               select new {c.SomeProperty, c.OtherProperty};

foreach (var result in results)
{
    Console.WriteLine(result);
}
```

- Language based (integrated)
- Works in memory, xml, databases, etc
  - Based on the notion of **Provider**, it is extensible
- Programmers need to explicitly build objects that matches the database schema

```
[Table(Name="Customers")]
public class Customer
{
    [Column(IsPrimaryKey = true)]
    public int CustID;

    [Column]
    public string CustName;
}
```

- Language based (integrated)
- Allows navigation using associations

```
// Query for customers who have placed orders.  
var custQuery =  
    from cust in Customers  
    where cust.Orders.Any()  
    select cust;  
  
foreach (var custObj in custQuery)  
{  
    Console.WriteLine("ID={0}, Qty={1}", custObj.CustomerID,  
        custObj.Orders.Count);  
}
```

# ActiveRecord in Rails

- Follows the active record pattern to implement an ORM. AR objects link to persistent data and define behaviour.
- Well integrated with the Model in the Rails MVC pattern
- Completely abstracts the database management by:
  - Object-mappings
  - Inheritance
  - Associations
  - Validations
  - Migrations (w/ Rails)

```
def create
  @author = Author.new(author_params)

  respond_to do |format|
    if @author.save
      format.html { redirect_to @author, notice: 'Author was successfully created.' }
      format.json { render action: 'show' }
    else
      format.html { render action: 'new' }
      format.json { render json: @author.errors, status: :unprocessable_entity }
    end
  end
end
```

# NoSQL databases

---

- Not only SQL.
  - Document-based, Chave-Valor, Graph-based
- Desenhadas para escalonamento horizontal (replicação)
- Compromisso na consistência dos dados
- Limited transactional support (real concurrency control)... use of chards
- Very good for querying, harder to get right on “writes”, indexes, etc.
- Queries are written in JavaScript, Java, SPARK, Map reduce algorithms...

# Data abstraction in Internet and Web Apps

---

- Abstraction over the actual data model
  - Hides the actual database engine running beneath
  - Integrates smoothly with the programming model (objects instead of string-based results).
- Independent configuration modes
  - Allows different execution modes with the same code (e.g. in-memory, transactional, replicated, etc.)
- Does not really cover all data models smoothly:
  - SQL model (e.g. Hibernate, ActiveRecord (Rn'R))
  - NoSQL model (e.g. google app engine framework)

# Abstraction levels

---

- Connectivity (e.g. JDBC)
  - abstracts the connectivity and execution of queries.
  - you have to build queries, and parse and translate results
- Data translation (e.g. JPA, ActiveRecord, LINQ)
  - Translates data formats between program and database.
  - Integrates the language values typefully.
- Implementation and execution modes
  - Example: Google Cloud Datastore is a NoSQL document based storage that allows different implementations (cassandra, mongodb)

<https://cloud.google.com/appengine/docs/java/datastore/>

# ORM

# Object-relational impedance mismatch

- Most databases are based on relational algebra
- Applications define object oriented representations (object graphs)

346 systems in ranking, October 2018

Rank			DBMS	Database Model	Score		
Oct 2018	Sep 2018	Oct 2017			Oct 2018	Sep 2018	Oct 2017
1.	1.	1.	Oracle 	Relational DBMS	1319.27	+10.15	-29.54
2.	2.	2.	MySQL 	Relational DBMS	1178.12	-2.36	-120.71
3.	3.	3.	Microsoft SQL Server 	Relational DBMS	1058.33	+7.05	-151.99
4.	4.	4.	PostgreSQL 	Relational DBMS	419.39	+12.97	+46.12
5.	5.	5.	MongoDB 	Document store	363.19	+4.39	+33.79
6.	6.	6.	DB2 	Relational DBMS	179.69	-1.38	-14.90
7.	↑ 8.	↑ 9.	Redis 	Key-value store	145.29	+4.35	+23.24
8.	↓ 7.	↑ 10.	Elasticsearch 	Search engine	142.33	-0.28	+22.09
9.	9.	↓ 7.	Microsoft Access	Relational DBMS	136.80	+3.41	+7.35
10.	10.	↓ 8.	Cassandra 	Wide column store	123.39	+3.83	-1.40

<https://db-engines.com/en/ranking>

# Object-relational impedance mismatch

- Most databases are based on relational algebra
- Applications define object oriented representations (object graphs)

355 systems in ranking, October 2019

Rank	Oct	Sep	Oct	DBMS	Database Model	Score		
	2019	2019	2018			Oct	Sep	Oct
1.	1.	1.	Oracle 	Relational, Multi-model 	1355.88	+9.22	+36.61	
2.	2.	2.	MySQL 	Relational, Multi-model 	1283.06	+3.99	+104.94	
3.	3.	3.	Microsoft SQL Server 	Relational, Multi-model 	1094.72	+9.66	+36.39	
4.	4.	4.	PostgreSQL 	Relational, Multi-model 	483.91	+1.66	+64.52	
5.	5.	5.	MongoDB 	Document	412.09	+2.03	+48.90	
6.	6.	6.	IBM Db2 	Relational, Multi-model 	170.77	-0.79	-8.91	
7.	7.	8.	Elasticsearch 	Search engine, Multi-model 	150.17	+0.90	+7.85	
8.	8.	7.	Redis 	Key-value, Multi-model 	142.91	+1.01	-2.38	
9.	9.	9.	Microsoft Access	Relational	131.18	-1.53	-5.62	
10.	10.	10.	Cassandra 	Wide column	123.22	-0.18	-0.17	

<https://db-engines.com/en/ranking>

# Object-Relational Impedance Mismatch

---

- What's the difference?
  - Encapsulation
  - Interface, class, polymorphism
  - Mapping relational concepts
  - Data type differences
  - Structural and integrity differences
  - Transactional differences

<http://blogs.tedneward.com/post/the-vietnam-of-computer-science/>

<https://dev.to/alagrede/why-i-dont-want-use-jpa-anymore-f1>

# Object-Relational Impedance Mismatch

---

- Identity
  - Object: `a == b` and `a.equals(b)`
  - Relational: primary key based
- Inheritance
  - Object: natural relation
  - Relational: does not exist, idioms are necessary
- Accessing data
  - Object: through the object interface
  - Relational: select queries (with joins)
- Associations/Navigation
  - Object: unidirectional references through objects' interface
  - Relational: through foreign keys
- Granularity
  - In some cases there may be a difference in the granularity level

# Object-Relational Impedance Mismatch

- Identity based on Primary Keys,
- We must define method **equals** (or utils like Lombok).

```
@Entity
public class Person {

    @Id
    @GeneratedValue
    private long id;

    private String name;

    public Person() {}

    public long getId() {
        return id;
    }

    public void setId(long id) {
        this.id = id;
    }

    public String getName() {
        return name;
    }

    public void setName(String name) {
        this.name = name;
    }
}
```

# Object-Relational Impedance Mismatch

- Inheritance: optional support for inheritance is provided by some frameworks

```
@Entity
@Inheritance(strategy= InheritanceType.JOINED)
@JsonSubTypes({
    @JsonSubTypes.Type(value = Professor.class, name = "PROFESSOR"),
    @JsonSubTypes.Type(value = Staff.class, name = "STAFF"),
    @JsonSubTypes.Type(value = Student.class, name = "STUDENT")
})
public class User {

    @Id
    @GeneratedValue
    private Long id_login;

    private String name;
    ...
}
```

```
@Entity
public class Student extends User {

    @Column
    private int number;

    public Student() {
        super();
    }

    public Student(String login,
                   String password,
                   String name,
                   String tel,
                   String email,
                   String address,
                   String type,
                   int number) {
        super( login,
               password,
               name,
               tel,
               email,
               address,
               type);
        this.number = number;
    }

    public int getNumber() {
        return number;
    }
}
```

# Object-Relational Impedance Mismatch

- Inheritance: optional support for inheritance is provided by some frameworks

```
@Entity  
@Inheritance(strategy= InheritanceType.JOINED)  
@JsonSubTypes({  
    @JsonSubTypes.Type(value = Professor.class, name = "PROFESSOR"),  
    @JsonSubTypes.Type(value = Staff.class, name = "STAFF"),  
    @JsonSubTypes.Type(value = Student.class, name = "STUDENT")  
})  
public class User {  
  
    @Id  
    @GeneratedValue  
    private Long id login.  
  
    private ...  
}
```

- *MappedSuperclass* – the parent classes, can't be entities
- Single Table – the entities from different classes with a common ancestor are placed in a single table
- Joined Table – each class has its table and querying a subclass entity requires joining the tables
- Table-Per-Class – all the properties of a class, are in its table, so no join is required

```
@Entity  
public class Student extends User {  
  
    @Column  
    private int number;  
  
    public Student() {  
        super();  
    }  
  
    public Student(String login,  
                  String password,  
                  String name,  
                  String tel,  
                  String email,  
                  String address,  
                  String type,  
                  int number) {  
  
        super( login,  
              password,  
              name,  
              tel,  
              email,  
              address,  
              type,  
              number);  
    }  
}
```

<https://www.baeldung.com/hibernate-inheritance>

# Object-Relational Impedance Mismatch

- Access to data by object navigation
- All fields are retrieved to memory instead of explicitly selected
- May result in navigation queries

```
Organization o = organizationRepository.findById(id).get();
System.out.println(o.getName() + o.getContactInfo());
```

```
@Entity
public class Organization {

    @Id
    @GeneratedValue
    private Long id_entity;

    @Column
    private String name;

    @OneToOne(cascade = CascadeType.ALL)
    @JoinColumn(name = "contact_id")
    private ContactInfo contactInfo;

    public Organization(){ }

    public String getName() {
        return name;
    }

    public void setName(String name) {
        this.name = name;
    }

    public ContactInfo getContactInfo() {
        return contactInfo;
    }

    public void setContactInfo(ContactInfo contactInfo) {
        this.contactInfo = contactInfo;
    }

    ...
}
```

# ActiveRecord Example

```
class Album < ActiveRecord::Base
  has_many :tracks
end

class Track < ActiveRecord::Base
  belongs_to :album
end

album = Album.create(:title => 'Black and Blue', :performer => 'The Rolling Stones')
album.tracks.create(:track_number => 1, :title => 'Hot Stuff')
album.tracks.create(:track_number => 2, :title => 'Hand Of Fate')
album.tracks.create(:track_number => 3, :title => 'Cherry Oh Baby ')
album.tracks.create(:track_number => 4, :title => 'Memory Motel ')
album.tracks.create(:track_number => 5, :title => 'Hey Negrita')
album.tracks.create(:track_number => 6, :title => 'Fool To Cry')
album.tracks.create(:track_number => 7, :title => 'Crazy Mama')
album.tracks.create(:track_number => 8, :title => 'Melody (Inspiration By Billy Preston)')

album = Album.create(:title => 'Sticky Fingers',:performer => 'The Rolling Stones')
album.tracks.create(:track_number => 1, :title => 'Brown Sugar')
album.tracks.create(:track_number => 2, :title => 'Sway')
album.tracks.create(:track_number => 3, :title => 'Wild Horses')
album.tracks.create(:track_number => 4,:title => 'Can\'t You Hear Me Knocking')
album.tracks.create(:track_number => 5, :title => 'You Gotta Move')
album.tracks.create(:track_number => 6, :title => 'Bitch')
album.tracks.create(:track_number => 7, :title => 'I Got The Blues')
album.tracks.create(:track_number => 8, :title => 'Sister Morphine')
album.tracks.create(:track_number => 9, :title => 'Dead Flowers')
album.tracks.create(:track_number => 10, :title => 'Moonlight Mile')
```

<https://dzone.com/articles/simple-ruby-activerecord>

# Object-Relational Mapping

- In Java you navigate the object network.
- Not efficient to retrieve data from a RDBMS.
- Minimize the number of SQL queries by using JOINs and selecting the targeted entities from the start (pre-fetching).

```
from Cat as cat
    inner join cat.mate as mate
    left outer join cat.kittens as kitten
```

<https://docs.jboss.org/hibernate/orm/3.3/reference/en/html/queryhql.html#queryhql-joins>

JPA

# Java Persistence API (JPA)

JPA provides a POJO persistence model for ORM

# Java Persistence API (JPA)

```
@Entity  
@Table(name="ORDER_TABLE")  
public class Order {  
  
    private int id;  
    private String address;  
    private Customer customer;  
  
    @Id  
    @Column(name="ORDER_ID")  
    public int getId() {  
        return id;  
    }  
  
    public void setId(int id){  
        this.id = id;  
    }  
  
    ...  
  
    @Column(name="SHIPPING_ADDRESS")  
    public String getAddress() {  
        return address;  
    }  
    public void setAddress(  
        String address) {  
        this.address = address;  
    }  
  
    @ManyToOne()  
    // foreign key: column used for join  
    @JoinColumn(name="CUSTOMER_ID")  
    public Customer getCustomer() {  
        return customer;  
    }  
  
    ...  
  
    public void setCustomer(  
        Customer customer) {  
        this.customer = customer;  
    }
```

# Internet Applications Design and Implementation

2020 - 2021

(Lecture 4 - Persistence : JPA & Hibernate)

**MIEI - Integrated Master in Computer Science and Informatics  
Specialization block**

**João Costa Seco ([joao.seco@fct.unl.pt](mailto:joao.seco@fct.unl.pt))**

(with previous participations of Jácome Cunha ([jacome@fct.unl.pt](mailto:jacome@fct.unl.pt)) and João Leitão ([jc.leitao@fct.unl.pt](mailto:jc.leitao@fct.unl.pt)))



FACULDADE DE  
CIÊNCIAS E TECNOLOGIA  
UNIVERSIDADE NOVA DE LISBOA

# Outline

---

- Object Relational Mapping Features (JPA & Hibernate)
- Spring and Data Abstraction
- JPA Associations
- Optimization of data fetching

# Internet Applications Design and Implementation

2020 - 2021

(Lecture 4 - Part 1 - Object Relational Mapping)

**MIEI - Integrated Master in Computer Science and Informatics  
Specialization block**

**João Costa Seco ([joao.seco@fct.unl.pt](mailto:joao.seco@fct.unl.pt))**

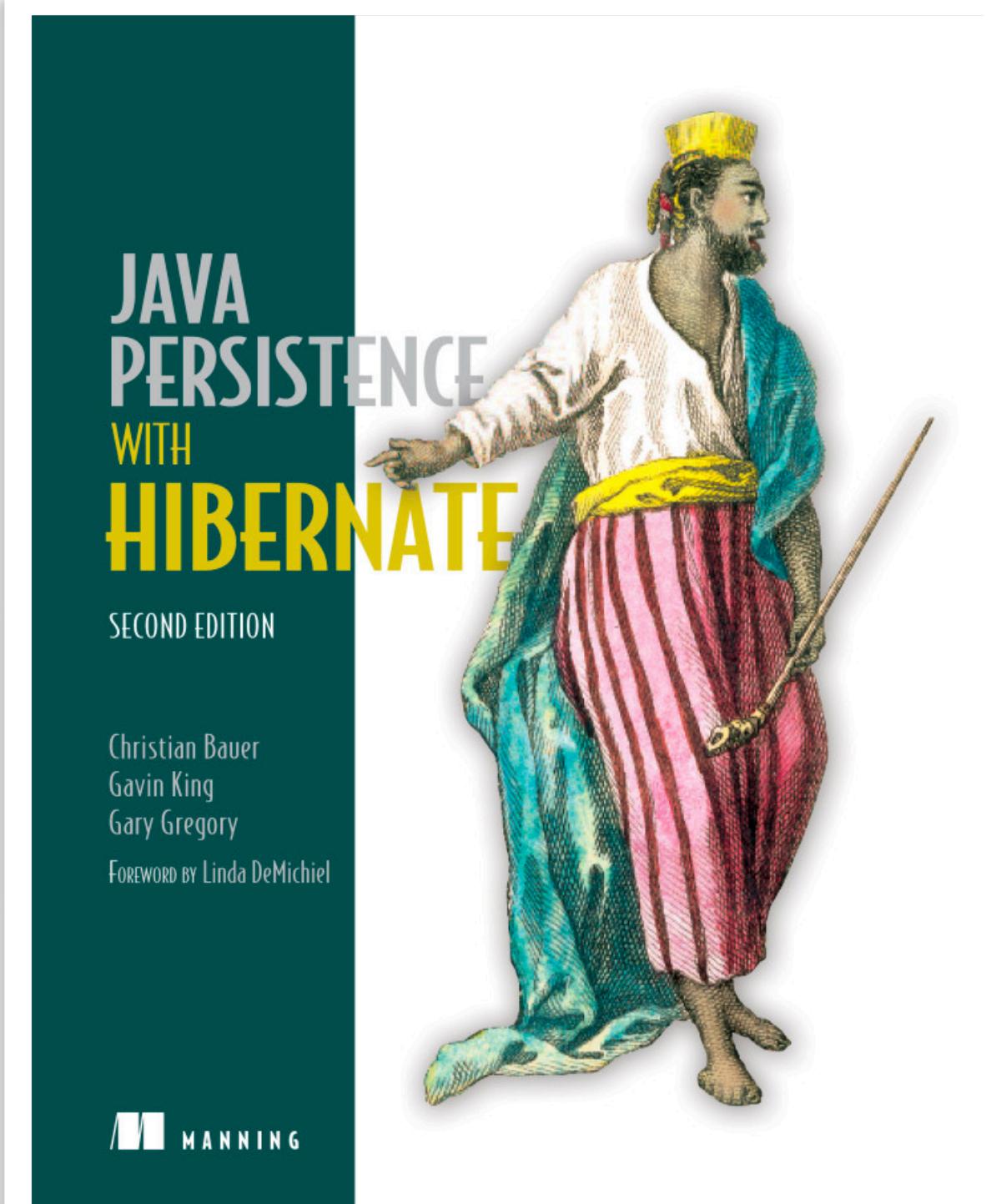
(with previous participations of Jácome Cunha ([jacome@fct.unl.pt](mailto:jacome@fct.unl.pt)) and João Leitão ([jc.leitao@fct.unl.pt](mailto:jc.leitao@fct.unl.pt)))



FACULDADE DE  
CIÊNCIAS E TECNOLOGIA  
UNIVERSIDADE NOVA DE LISBOA

# Object-Relational Mapping

- Manages persistence of data in the OO realm
- Abstracts the use of SQL in connection to RDBMSs
- Covers most injection attacks on queries  
(except with APIs that allow creation with string)
- Specified by a common and standard API (JPA)
- Implementations differ by JPA providers



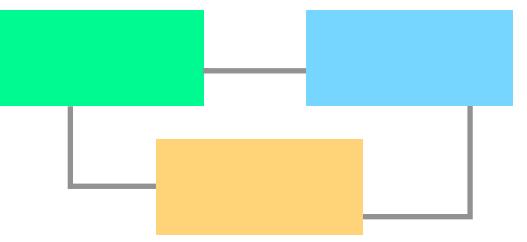
```
public List<AccountDTO> unsafeJpaFindAccountsByCustomerId(String customerId) {  
    String jql = "from Account where customerId = '" + customerId + "'";  
    TypedQuery<Account> q = em.createQuery(jql, Account.class);  
    return q.getResultList()  
        .stream()  
        .map(this::toAccountDTO)  
        .collect(Collectors.toList());  
}
```

# Object-Relational Impedance Mismatch

- Identity
  - Object: `a == b` and `a.equals(b)`
  - Relational: primary key based
- Inheritance
  - Object: natural relation
  - Relational: does not exist, idioms are necessary
- Accessing data
  - Object: through the object interface
  - Relational: select queries (with joins)
- Associations/Navigation
  - Object: unidirectional references through objects' interface
  - Relational: through foreign keys
- Granularity
  - In some cases there may be a difference in the granularity level



<http://hibernate.org/orm/what-is-an-orm/>



# JPA - Java Persistence API

- Java Persistence API (Jakarta Persistence since Set 2019)
- Provides a OO interface to a relational database
- Defines JPQL (Java Persistence Query Language)
- The reference implementation is EclipseLink.
- Hibernate is a JPA provider (extended API and query language HQL)



# Data Abstraction layers

---

- Advantages
  - Hides the complexity of a particular query language
  - Allows the portability of database engines (not really models)
  - Prevents attacks such as SQL injection, or XSS
  - Avoids runtime errors in the construction of queries
  - May isolate efficient implementations (previously, with prepared and compiled parameterised SQL queries)
  - Allows scalability via customised runtime configurations (distribution, transactional behaviour, indexing, ...)
  - Avoids early optimization pitfalls, develop first, configure later.
- Pitfalls
  - Lack of access to proprietary features of providers
  - May lead to inefficient data transmissions: more queries ( $N+1$  queries), more data than needed.

# Internet Applications Design and Implementation

## 2020 - 2021

### (Lecture 4 - Part 2 - Spring & Data Abstraction)

**MIEI - Integrated Master in Computer Science and Informatics  
Specialization block**

**João Costa Seco ([joao.seco@fct.unl.pt](mailto:joao.seco@fct.unl.pt))**

(with previous participations of Jácome Cunha ([jacome@fct.unl.pt](mailto:jacome@fct.unl.pt)) and João Leitão ([jc.leitao@fct.unl.pt](mailto:jc.leitao@fct.unl.pt)))



FACULDADE DE  
CIÊNCIAS E TECNOLOGIA  
UNIVERSIDADE NOVA DE LISBOA

# JDBC & Spring

---

- SpringBoot provides direct support for JDBC
- As in any JDBC setting, it is necessary to define a DataSource (DB, CSV file, etc.)
- SpringBoot offers the JdbcTemplate class to assist programmers
- Spring easily integrates JPA support (later)

# JDBC & Spring & In-memory DBs

---

- JdbcTemplate handles the setup and connection to the DataSource based on the POM dependencies (when possible)
- For instance, for H2 in-memory database (Spring also supports HSQL and Derby):

```
<dependency>
    <groupId>com.h2database</groupId>
    <artifactId>h2</artifactId>
</dependency>
```

- This handles the connection and exceptions

# JDBC & Spring

---

- It also supports “regular” relational databases adding the necessary properties to the `application.properties` file, e.g.:

```
spring.datasource.url=jdbc:mysql://localhost/test  
spring.datasource.username=dbuser  
spring.datasource.password=dbpass
```

# JDBC & Spring

```
@Component
public class Hotels {

    private JdbcTemplate jdbc;

    @Autowired
    public Hotels(JdbcTemplate jdbc) {
        this.jdbc = jdbc;
        createTable();
    }

    public Hotels(){}

    public void createTable() {
        jdbc.execute("drop table tablea if exists");
        jdbc.execute("create table tablea(id SERIAL, attributea VARCHAR(16))");
    }

    public List<Map<String, Object>> select() {
        return jdbc.query("select * from tablea", new ColumnMapRowMapper());
    }

    public int save(String att) {
        return jdbc.update("insert into tablea(attributea) values (?)", att);
    }
}
```



# JPA & Spring

- Spring-boot-starter-data-jpa provides the necessary dependencies:
  - Hibernate — One of the most popular JPA implementations
  - Spring Data JPA — Makes it easy to implement JPA-based repositories
  - Spring ORMs — Core ORM support from the Spring Framework

```
<dependency>
    <groupId>org.springframework.boot</groupId>
    <artifactId>spring-boot-starter-data-jpa</artifactId>
</dependency>
```



# Declare an Entity (in Java)

```
@Entity
public class Customer {
    @Id
    @GeneratedValue(strategy=GenerationType.AUTO)
    private Long id;
    private String firstName;
    private String lastName;

    protected Customer() {}

    public Customer(String firstName, String lastName) {
        this.firstName = firstName;
        this.lastName = lastName;
    }
    @Override
    public String toString() {
        return String.format(
            "Customer[id=%d, firstName='%s', lastName='%s']",
            id, firstName, lastName);
    }
}
```

# Declare a Repository and plug it in... (in Java)



```
public interface CustomerRepository extends CrudRepository<Customer, Long> {  
    List<Customer> findByLastName(String lastName);  
}
```

```
@Controller  
public class CustomerController  
{  
    @Autowired  
    CustomerRepository customers;  
  
    ... findByLastName("Smith");...  
}
```

# Declare an Entity and a Repository and plug it in...



```
@Entity  
data class PetDAO(  
    @Id @GeneratedValue val id: Long,  
    var name: String,  
    var species: String  
)
```

```
interface PetRepository : CrudRepository<PetDAO, Long> {  
    fun findByName(name: String): MutableIterable<PetDAO>  
}
```

```
@Autowired  
lateinit var repo: PetRepository  
  
fun someFunction() {  
    ...repo.findByName("pantufas")...  
}
```

m	findByName(name: String)	MutableIterable<PetDAO>
m	toString()	String
m	save(S)	S
m	count()	Long
m	delete(PetDAO)	Unit
f	to(that: B) for A in kotlin	Pair<PetRepository, B>
m	deleteAll()	Unit
m	deleteAll((Mutable)Iterable<PetDAO!>)	Unit
	.long)	Unit
	.Any?)	Boolean
	.long)	Boolean
	(Mutable)Iterable<PetDAO!>	(Mutable)Iterable<PetDAO!>
	(Mutable)Iterable<Long!>)	(Mutable)Iterable<PetDAO!>
m	findById(Long)	Optional<PetDAO!>
	hashCode()	Int
	saveAll((Mutable)Iterable<S!>)	(Mutable)Iterable<S!>
	let {...} (block: (PetRepository) -> R) for T in kotlin	R
	javaClass for T in kotlin.jvm	Class<PetRepository>
	also {...} (block: (PetRepository) -> Unit) for T in...	PetRepository
	apply {...} (block: PetRepository.() -> Unit) for T ...	PetRepository
	run {...} (block: PetRepository.() -> R) for T in kotlin	R
f	takeIf {...} (predicate: (PetRepository) -> Boolean)	PetRepository?
f	takeUnless {...} (predicate: (PetRepository) -> Boo...	PetRepository?
f	findByIdOrNull(id: Long) for CrudRepository<T, ID> in org...	PetDAO?

^↓ and ^↑ will move caret down and up in the editor [Next Tip](#)

# interface CrudRepository<T , ID extends Serializable>

```
I CrudRepository (org.springframework.data.repository.CrudRepository)
I JpaRepository (org.springframework.data.jpa.repository.JpaRepository)
I JpaRepositoryImplementation (org.springframework.data.jpa.repository.JpaRepositoryImplementation)
I PagingAndSortingRepository (org.springframework.data.repository.PagingAndSortingRepository)
I PetRepository (pt.unl.fct.di.iadi.vetclinic.repositories.PetRepository)
C QuerydslJpaRepository (org.springframework.data.repository.QuerydslJpaRepository)
I ReactiveCrudRepository (org.springframework.data.repository.ReactiveCrudRepository)
I ReactiveSortingRepository (org.springframework.data.repository.ReactiveSortingRepository)
I RevisionRepository (org.springframework.data.repository.RevisionRepository)
I RxJava2CrudRepository (org.springframework.data.repository.RxJava2CrudRepository)
I RxJava2SortingRepository (org.springframework.data.repository.RxJava2SortingRepository)
C SimpleJpaRepository (org.springframework.data.repository.SimpleJpaRepository)
```

m	findByName(name: String)	MutableIterable<PetDAO>
m	toString()	String
m	save(S)	S
m	count()	Long
m	delete(PetDAO)	Unit
f	to(that: B) for A in kotlin	Pair<PetRepository, B>
m	deleteAll()	Unit
m	deleteAll((Mutable)Iterable<PetDAO!>)	Unit
m	deleteById(Long)	Unit
m	equals(other: Any?)	Boolean
m	existsById(Long)	Boolean
m	findAll()	(Mutable)Iterable<PetDAO!>
m	findAllById((Mutable)Iterable<Long!>)	(Mutable)Iterable<PetDAO!>
m	findById(Long)	Optional<PetDAO!>
m	hashCode()	Int
m	saveAll((Mutable)Iterable<S!>)	(Mutable)Iterable<S!>
f	let {...} (block: (PetRepository) -> R) for T in kotlin	R
v	javaClass for T in kotlin.jvm	Class<PetRepository>
f	also {...} (block: (PetRepository) -> Unit) for T in...	PetRepository
f	apply {...} (block: PetRepository.() -> Unit) for T ...	PetRepository
f	run {...} (block: PetRepository.() -> R) for T in kotlin	R
f	takeIf {...} (predicate: (PetRepository) -> Boolean)	PetRepository?
f	takeUnless {...} (predicate: (PetRepository) -> Boolean)	PetRepository?
f	findByIdOrNull(id: Long) for CrudRepository<T, ID> in org...	PetDAO?

# An Example

```
@Entity  
@NamedQuery(name = "User.findByTheUsersName",  
            query = "from User u where u.username = ?1")  
class User(  
    @Column(unique = true)  
    val username:String,  
    val firstname:String,  
    val lastname:String  
)  
  
interface SimpleUserRepository : CrudRepository<User, Long> {  
  
    fun findByTheUsersName(username:String):User  
  
    fun findByLastname(lastname:String):List<User>  
  
    @Query("select u from User u where u.firstname = ?")  
    fun findByFirstname(firstname:String):List<User>  
  
    @Query("select u from User u where u.firstname = :name or u.lastname = :name")  
    fun findByFirstnameOrLastname(@Param("name") name:String):List<User>  
}
```

Keyword	Sample	JPQL snippet
And	findByLastnameAndFirstname	... where x.lastname = ?1 and x.firstname = ?2
Or	findByLastnameOrFirstname	... where x.lastname = ?1 or x.firstname = ?2
Is, Equals	findByFirstname, findByFirstnamels, findByFirstnameEquals	... where x.firstname = ?1
Between	findByStartDateBetween	... where x.startDate between ?1 and ?2
LessThan	findByAgeLessThan	... where x.age < ?1
LessThanEqual	findByAgeLessThanEqual	... where x.age ≤ ?1
Greater Than	findByAgeGreaterThan	... where x.age > ?1
Greater Than Equal	findByAgeGreaterThanEqual	... where x.age ≥ ?1
After	findByStartDateAfter	... where x.startDate > ?1
Before	findByStartDateBefore	... where x.startDate < ?1
IsNull	findByAgeIsNull	... where x.age is null
IsNotNull, NotNull	findByAge(Is)NotNull	... where x.age not null
Like	findByFirstnameLike	... where x.firstname like ?1
NotLike	findByFirstnameNotLike	... where x.firstname not like ?1
StartingWith	findByFirstnameStartingWith	... where x.firstname like ?1 (parameter)
EndingWith	findByFirstnameEndingWith	... where x.firstname like ?1 (parameter)
Containing	findByFirstnameContaining	... where x.firstname like ?1 (parameter)
OrderBy	findByAgeOrderByLastnameDesc	... where x.age = ?1 order by x.lastname
Not	findByLastnameNot	... where x.lastname <> ?1
In	findByAgeIn(Collection<Age> ages)	... where x.age in ?1
NotIn	findByAgeNotIn(Collection<Age> age)	... where x.age not in ?1
TRUE	findByActiveTrue()	... where x.active = true
FALSE	findByActiveFalse()	... where x.active = false
IgnoreCase	findByFirstnameIgnoreCase	... where UPPER(x.firstname) = UPPER(?1)

# Spring Data (and other ORM Implementations)

- Simple declaration of generic queries
- Specific declaration of custom queries (JPQL)
- Richer Behaviour from Repositories (e.g. paged)

```
public interface StudentRepository extends PagingAndSortingRepository<Student, Long> {  
  
    List<Student> findByName(String name);  
  
    @Query("select s from Student s where s.name like CONCAT(?,'%')")  
    List<Student> search(String name);  
  
    Page<Student> findByName(String name, Pageable pageable);  
}
```

- Dependency Injection and component assembly

```
public class StudentController {  
  
    @Autowired  
    StudentRepository students;
```

# Spring Data (and other ORM Implementations)

- Simple declaration of generic queries
- Specific declaration of custom queries (JPQL)
- Richer Behaviour from Repositories (e.g. paged)

```
public interface StudentRepository extends PagingAndSortingRepository<Student, Long> {
```

```
    List<Student> findByName(String name);
```

```
@RequestMapping(value= "/page")
public @ResponseBody Page<Student> getStudentsPaged(
    @RequestParam(required=false, defaultValue = "0") Integer page,
    @RequestParam(required=false, defaultValue = "3") Integer size) {
```

```
    return students.findAll(new PageRequest(page, size));
}
```

```
@Autowired
StudentRepository students;
```

# Spring Data (and other ORM Imp)

- Simple declaration of generic queries
- Specific declaration of custom queries (JPQL)
- Richer Behaviour from Repositories (e.g. Pageable)

```
public interface StudentRepository extends Pageable
```

```
    List<Student> findByName(String name);
```

```
@RequestMapping(value= "/page")
public @ResponseBody Page<Student> getStudents(@RequestParam(required=false, defaultValue="") String name,
                                                 @RequestParam(required=false, defaultValue="") String sort) {
    return students.findAll(new PageRequest(0, 3));
}
```

```
@Autowired
StudentRepository students;
```

```
"content": [
  {
    "id": 1,
    "name": "Ingrid Daubechies",
    "age": 19
  },
  {
    "id": 2,
    "name": "Jacqueline K. Barton",
    "age": 18
  },
  {
    "id": 3,
    "name": "Jane Goodall",
    "age": 20
  }
],
"last": false,
"totalElements": 6,
"totalPages": 2,
"size": 3,
"number": 0,
"sort": null,
"first": true,
"numberOfElements": 3
}
```

# Spring Data - Features

---

- Powerful repository and custom object-mapping abstractions
- Dynamic query derivation from repository method names
- Implementation domain base classes providing basic properties
- Support for transparent auditing (created, last changed)
- Possibility to integrate custom repository code
- Easy Spring integration via JavaConfig and custom XML namespaces
- Advanced integration with Spring MVC controllers
- Experimental support for cross-store persistence

# Spring Data

---

- Spring Data Commons - Core Spring concepts underpinning every Spring Data project.
- Spring Data JPA - Makes it easy to implement JPA-based repositories.
- Spring Data MongoDB - Spring based, object-document support and repositories for MongoDB.
- Spring Data Redis - Provides easy configuration and access to Redis from Spring applications.
- Spring Data Solr - Spring Data module for Apache Solr.
- Spring Data Gemfire - Provides easy configuration and access to GemFire from Spring applications.
- Spring Data REST - Exports Spring Data repositories as hypermedia-driven RESTful resources.

## Community Modules

- Spring Data Cassandra - Spring Data module for Apache Cassandra.
- Spring Data Couchbase - Spring Data module for Couchbase.
- Spring Data DynamoDB - Spring Data module for DynamoDB.
- Spring Data Elasticsearch - Spring Data module for Elasticsearch.
- Spring Data Neo4j - Spring based, object-graph support and repositories for Neo4j.

# MongoDB Example

---

```
public class MongoApp {  
  
    private static final Log log = LogFactory.getLog(MongoApp.class);  
  
    public static void main(String[] args) throws Exception {  
  
        MongoOperations mongoOps = new MongoTemplate(new Mongo(), "database");  
        mongoOps.insert(new Person("Joe", 34));  
  
        log.info(mongoOps.findOne(new Query(where("name").is("Joe")), Person.class));  
  
        mongoOps.dropCollection("person");  
    }  
}
```

# Other database representations

- Objectify: gives easy and full access to the Google Cloud Datastore
- Dynamic / Reflexion based
- Alternative to JPA interface

```
@Entity  
class Car {  
    @Id String vin; // Can be Long, long, or String  
    String color;  
}  
  
ofy().save().entity(new Car("123123", "red")).now();  
Car c = ofy().load().type(Car.class).id("123123").now();  
ofy().delete().entity(c);
```

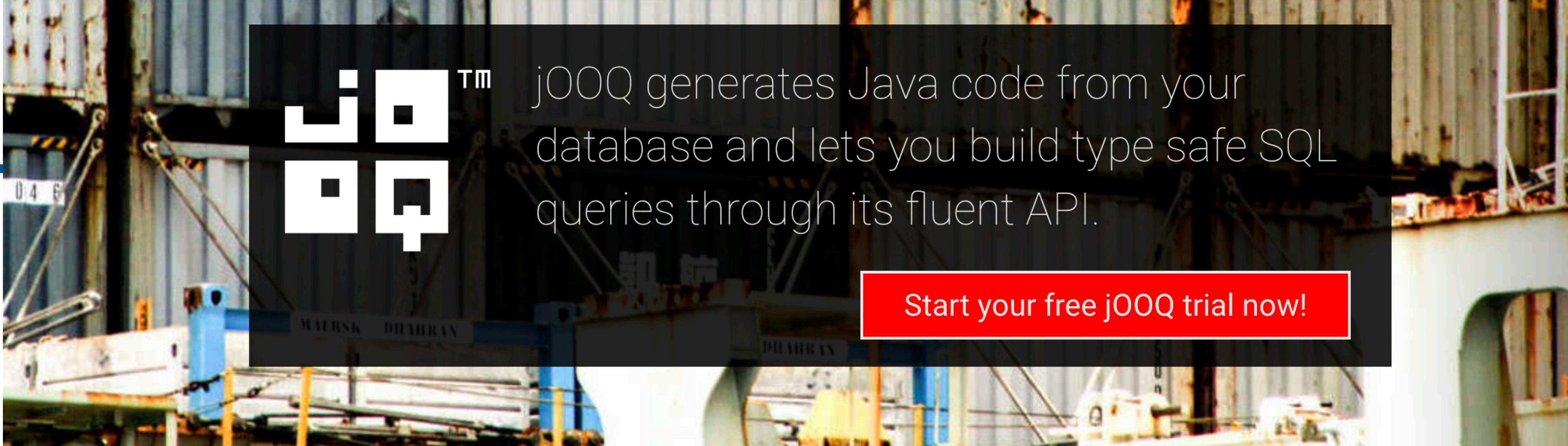
<https://github.com/objectify/objectify>

# Other database representations

- Objectify: gives easy and full access to the Google Cloud Datastore
- Dynamic / Reflexion based
- Alternative to JPA interface

- Objectify surfaces **all native datastore features**, including batch operations, queries, transactions, asynchronous operations, and partial indexes.
- Objectify provides **type-safe key and query classes** using Java generics.
- Objectify provides a **human-friendly query interface**.
- Objectify can automatically **cache your data in memcache** for improved read performance.
- Objectify can store polymorphic entities and perform **true polymorphic queries**.
- Objectify provides a simple, **easy-to-understand transaction model**.
- Objectify provides built-in facilities to **help migrate schema changes** forward.
- Objectify provides **thorough documentation** of concepts as well as use cases.
- Objectify has an **extensive test suite** to prevent regressions.

<https://github.com/objectify/objectify>



jOOQ generates Java code from your database and lets you build type safe SQL queries through its fluent API.

[Start your free jOOQ trial now!](#)

## Great Reasons for Using jOOQ

Our customers spend most time on *their* business-logic.  
Because jOOQ takes care of all their Java/SQL infrastructure problems.

<https://www.jooq.org/>

### Database First

Tired of ORMs driving your database model?

Whether you design a new application or integrate with your legacy, your database holds your most important asset: your data.

jOOQ is SQL-centric. Your database comes "first".

### Typesafe SQL

Fed up with detecting SQL syntax errors in production?

SQL is a highly expressive and type safe language with a rich syntax. jOOQ models SQL as an internal DSL and uses the Java compiler to compile your SQL syntax, metadata and data types.

### Code Generation

Bored with renaming table and column names in your Java code?

jOOQ generates Java classes from your database metadata. Your Java compiler will tell you when your code is out of sync with your schema.

### Active Records

Annoyed by the amount of SQL you write for CRUD?

jOOQ lets you perform CRUD and POJO mapping directly on Active Records, which are also generated from the code generator.

# Internet Applications Design and Implementation

## 2020 - 2021

### (Lecture 4 - Part 3 - JPA Associations)

**MIEI - Integrated Master in Computer Science and Informatics  
Specialization block**

**João Costa Seco ([joao.seco@fct.unl.pt](mailto:joao.seco@fct.unl.pt))**

(with previous participations of Jácome Cunha ([jacome@fct.unl.pt](mailto:jacome@fct.unl.pt)) and João Leitão ([jc.leitao@fct.unl.pt](mailto:jc.leitao@fct.unl.pt)))



FACULDADE DE  
CIÊNCIAS E TECNOLOGIA  
UNIVERSIDADE NOVA DE LISBOA

# JPA Associations



```
@Entity  
data class Book(  
    @Id  
    @GeneratedValue  
    val id: Long,  
    val name: String,  
    @ManyToOne  
    val kind: Category  
)  
  
@Entity  
data class Category(  
    @Id  
    @GeneratedValue  
    val id: Long,  
    val name: String,  
    @OneToMany  
    val books: Set<Book>  
)
```

```
interface BookRepository : CrudRepository<Book, Long>  
interface CategoryRepository: CrudRepository<Category, Long>  
...  
val fantasy = Category(0, "Fantasy", emptySet<Book>())  
categories.save(fantasy)  
val lor = Book(0, "Lord of the Rings", fantasy)  
books.save(lor)
```

```
call next value for hibernate_sequence  
insert into category (name, id) values (?, ?)  
binding parameter [1] as [VARCHAR] - [Fantasy]  
binding parameter [2] as [BIGINT] - [1]  
call next value for hibernate_sequence  
insert into book (kind_id, name, id) values (?, ?, ?)  
binding parameter [1] as [BIGINT] - [1]  
binding parameter [2] as [VARCHAR] - [Lord of the Rings]  
binding parameter [3] as [BIGINT] - [2]
```



# JPA Associations

```
@Entity  
@Table(name = "book_category")  
public class BookCategory {  
    private int id;  
    private String name;  
    private Set<Book> books;  
  
    public BookCategory(){ ... }  
  
    public BookCategory(String name) {...}  
  
    @Id  
    @GeneratedValue(strategy = GenerationType.AUTO)  
    public int getId() { ... }  
  
    public void setId(int id) { ... }  
  
    public String getName() {...}  
  
    public void setName(String name) {...}  
  
    @OneToMany(mappedBy = "bookCategory",  
               cascade = CascadeType.ALL)  
    public Set<Book> getBooks() { ... }  
  
    public void setBooks(Set<Book> books) { ... }  
}
```

```
@Entity  
public class Book{  
    private int id;  
    private String name;  
    private BookCategory bookCategory;  
  
    public Book() {}  
  
    public Book(String name) { this.name = name;}  
  
    public Book(String name, BookCategory bookCategory) { ... }  
  
    @Id  
    @GeneratedValue(strategy = GenerationType.AUTO)  
    public int getId() { ... }  
  
    public void setId(int id) { ... }  
  
    public String getName() { ... }  
  
    public void setName(String name) { ... }  
  
    @ManyToOne  
    @JoinColumn(name = "book_category_id")  
    public BookCategory getBookCategory() { ... }  
  
    public void setBookCategory(BookCategory bookCategory) {...}  
}
```

# JPA Associations



```
@Entity  
data class Book(  
    @Id  
    @GeneratedValue  
    val id: Long,  
    val name: String,  
    @ManyToOne  
    val kind: Category  
)
```

```
@Entity  
data class Category(  
    @Id  
    @GeneratedValue  
    val id: Long,  
    val name: String,  
    @OneToMany  
    val books: Set<Book>  
)
```

```
interface BookRepository : CrudRepository<Book, Long>  
interface CategoryRepository: CrudRepository<Category, Long>  
...  
val book = books.findById(lor.id)  
logger.info(book.get().kind.toString())
```

```
select book0_.id as id1_0_0_,  
       book0_.kind_id as kind_id3_0_0_,  
       book0_.name as name2_0_0_,  
       category1_.id as id1_1_1_,  
       category1_.name as name2_1_1_  
  from book book0_  
 left outer join category category1_ on  
       book0_.kind_id=category1_.id where book0_.id=?
```

# JPA Associations



```
@Entity  
data class Book(  
    @Id  
    @GeneratedValue  
    val id:Long,  
    val name:String,  
    @ManyToOne  
    val kind:Category  
)  
  
@Entity  
data class Category(  
    @Id  
    @GeneratedValue  
    val id:Long,  
    val name:String,  
    @OneToMany  
    val books:Set<Book>  
)
```

```
interface BookRepository : CrudRepository<Book, Long>  
interface CategoryRepository: CrudRepository<Category, Long>  
...  
val kind = categories.findById(fantasy.id)
```

```
select  
    category0_.id as id1_1_0_,  
    category0_.name as name2_1_0_  
from category category0_  
where category0_.id=?
```

# JPA Associations



```
@Entity  
data class Book(  
    @Id  
    @GeneratedValue  
    val id:Long,  
    val name:String,  
  
    @OneToMany  
    val kind:Category  
)  
  
@Entity  
data class Category(  
    @Id  
    @GeneratedValue  
    val id:Long,  
    val name:String,  
    @ManyToOne  
    val books:Set<Book>  
)
```

```
interface BookRepository : CrudRepository<Book, Long>  
interface CategoryRepository: CrudRepository<Category, Long>  
...  
val kind = categories.findById(fantasy.id)  
logger.info(kind.toString())
```

failed to lazily initialize a collection of role:  
com.demo.Category.books

# JPA Associations



```
@Entity  
data class Book(  
    @Id  
    @GeneratedValue  
    val id: Long,  
    val name: String,  
    @ManyToOne  
    val kind: Category  
)  
  
@Entity  
data class Category(  
    @Id  
    @GeneratedValue  
    val id: Long,  
    val name: String,  
    @OneToMany(fetch = FetchType.EAGER)  
    val books: Set<Book>  
)  
  
Optional[Category(id=1, name=Fantastic, books=[])]
```

```
interface BookRepository : CrudRepository<Book, Long>  
interface CategoryRepository: CrudRepository<Category, Long>  
...  
val kind = categories.findById(fantasy.id)  
logger.info(kind.toString())
```

```
select  
category0_.id as id1_1_0_,  
category0_.name as name2_1_0_,  
books1_.category_id as category1_2_1_,  
book2_.id as books_id2_2_1_,  
book2_.id as id1_0_2_,  
book2_.kind_id as kind_id3_0_2_,  
book2_.name as name2_0_2_,  
category3_.id as id1_1_3_,  
category3_.name as name2_1_3_  
from category category0_  
left outer join category_books books1_ on category0_.id=books1_.category_0_id  
left outer join book book2_ on books1_.books_id=book2_.id  
left outer join category category3_ on book2_.kind_id=category3_.id  
where category0_.id=?
```

# JPA Associations



```
@Entity
data class Book(
    @Id
    @GeneratedValue
    val id:Long,
    @Column(nullable = false)
    val name:String,
    @ManyToOne
    val kind:Category
)
@Entity
data class Category(
    @Id
    @GeneratedValue
    val id:Long,
    @Column(nullable = false)
    val name:String,
    @OneToMany(cascade = arrayOf(CascadeType.ALL), mappedBy = "kind", fetch = FetchType.EAGER)
    var books:List<Book>
)

val fantasy = Category(0, "Fantasy", emptyList<Book>())
val lor = Book(0,"Lord of the Rings", fantasy)
val silm = Book(0,"Silmarillion", fantasy)
fantasy.books = listOf(lor,silm)
categories.save(fantasy)

binding parameter [1] as [VARCHAR] - [Fantasy]
binding parameter [2] as [BIGINT] - [1]
insert into book (kind_id, name, id) values (?, ?, ?)
binding parameter [1] as [BIGINT] - [1]
binding parameter [2] as [VARCHAR] - [Lord of the Rings]
binding parameter [3] as [BIGINT] - [2]
insert into book (kind_id, name, id) values (?, ?, ?)
binding parameter [1] as [BIGINT] - [1]
binding parameter [2] as [VARCHAR] - [Silmarillion]
binding parameter [3] as [BIGINT] - [3]

Category(id=1, name=Fantasy, books=[{ Lord of the Rings, Fantasy }, { Silmarillion, Fantasy }])
```

# JPA Associations



```
@Entity  
data class Book(  
    @Id  
    @GeneratedValue  
    val id:Long,  
    @Column(nullable = false)  
    val name:String,  
    @ManyToOne  
    val kind:Category  
)  
  
@Entity  
data class Category(  
    @Id  
    @GeneratedValue  
    val id:Long,  
    @Column(nullable = false)  
    val name:String,  
    @OneToMany(cascade = arrayOf(CascadeType.ALL), mappedBy = "kind", fetch = FetchType.EAGER)  
    var books:List<Book>  
)
```

```
Category(id=1, name=Fantasy, books=[{ Lord of the Rings, Fantasy }, { Silmarillion, Fantasy }])
```

```
val kind = categories.findById(fantasy.id)  
logger.info(kind.toString())  
logger.info(kind.get().books.size.toString())  
for (b in kind.get().books) {  
    logger.info(b.toString())  
    logger.info(b.kind.toString())  
}
```

```
select  
    category0_.id as id1_1_0_,  
    category0_.name as name2_1_0_,  
    books1_.kind_id as kind_id3_0_1_,  
    books1_.id as id1_0_1_,  
    books1_.id as id1_0_2_,  
    books1_.kind_id as kind_id3_0_2_,  
    books1_.name as name2_0_2_  
from category category0_  
left outer join book books1_ on  
    category0_.id=books1_.kind_id where category0_.id=?
```



# Eager and Lazy

- Evaluation modes - transferring objects to memory

```
@OneToMany(mappedBy = "course", cascade = CascadeType.ALL, fetch = FetchType.EAGER)  
private Set<Enrollment> enrollments;
```

- Eager: transfers all objects related to the root

```
@OneToMany(mappedBy = "course", cascade = CascadeType.ALL, fetch = FetchType.LAZY)  
private Set<Enrollment> enrollments;
```

- Lazy: transfers object when needed

- Needs a transactional environment

```
@Component  
public class ProfessorService {  
  
    @Autowired  
    CourseRepository courseRepository;  
  
    @Autowired  
    ProfessorRepository professors;  
  
    @Transactional  
    public void addCourses(String name, String... courses) {  
        Professor p = professors.findByName(name);  
  
        Set<Course> cs = p.getCourses();  
        for(String c: courses)  
            cs.add(courseRepository.findByName(c).get(0));  
        professors.save(p);  
    }  
}
```



# Many To Many

```
@Entity  
public class Course {  
  
    @Id  
    @GeneratedValue(strategy=GenerationType.AUTO)  
    private long id;  
  
    private String name;  
  
    private int credits;  
  
    @OneToMany(mappedBy = "course",  
              cascade = CascadeType.ALL,  
              fetch = FetchType.EAGER)  
    private Set<Enrollment> enrollments;  
  
    @ManyToMany(mappedBy = "courses")  
    private Set<Professor> professors;  
}
```

```
@Entity  
public class Professor {  
  
    public Professor(String name) {  
        this.setName(name);  
    }  
  
    public Professor() {}  
  
    @javax.persistence.Id  
    @GeneratedValue(strategy=GenerationType.AUTO)  
    private long id;  
  
    private String name;  
  
    @ManyToMany  
    private Set<Course> courses;  
}
```

creates *professor\_courses* table in a bidirectional relation

[https://en.wikibooks.org/wiki/Java\\_Persistence/ManyToMany](https://en.wikibooks.org/wiki/Java_Persistence/ManyToMany)

<http://www.objectdb.com/java/jpa/gettingstarted>

<https://hellokoding.com/jpa-many-to-many-extra-columns-relationship-mapping-example-with-spring-boot-maven-and-mysql/>

# Internet Applications Design and Implementation

2020 - 2021

(Lecture 4 - Part 4 -Optimization of data fetching)

**MIEI - Integrated Master in Computer Science and Informatics  
Specialization block**

**João Costa Seco ([joao.seco@fct.unl.pt](mailto:joao.seco@fct.unl.pt))**

(with previous participations of Jácome Cunha ([jacome@fct.unl.pt](mailto:jacome@fct.unl.pt)) and João Leitão ([jc.leitao@fct.unl.pt](mailto:jc.leitao@fct.unl.pt)))



FACULDADE DE  
CIÊNCIAS E TECNOLOGIA  
UNIVERSIDADE NOVA DE LISBOA

# N+1 query problem

```
@Entity  
@Table(name = "book_category")  
public class BookCategory {  
    private int id;  
    private String name;  
    private Set<Book> books;  
  
    public BookCategory(){ ... }  
  
    public BookCategory(String name) {...}  
  
    @Id  
    @GeneratedValue(strategy = GenerationType.AUTO)  
    public int getId() { ... }  
  
    public void setId(int id) { ... }  
  
    public String getName() {...}  
  
    public void setName(String name) { ... }  
  
    @Repository  
    @OneToMany(mappedBy = "bookCategory", cascade = CascadeType.ALL)  
    public interface BookCategoryRepository extends JpaRepository<BookCategory, Integer>{}  
  
    public Set<Book> getBooks() { ... }  
  
    public void setBooks(Set<Book> books) { ... }  
    for( BookCategory c: categoryRepo.findAll() )  
        for( Book b: c.books )  
            ...  
}
```

```
@Entity  
public class Book{  
    private int id;  
    private String name;  
    private BookCategory bookCategory;  
  
    public Book() {}  
  
    public Book(String name) { this.name = name;}  
  
    public Book(String name, BookCategory bookCategory) { ... }  
  
    @Id  
    @GeneratedValue(strategy = GenerationType.AUTO)  
    public int getId() { ... }  
  
    public void setId(int id) { ... }  
  
    public String getName() { ... }  
  
    @JoinColumn(name = "book_category_id")  
    public BookCategory getBookCategory() { ... }  
  
    select * from book_category;  
    select * from book where bookCategory = ?  
    ...  
    select * from book where bookCategory = ?
```

# N+1 query problem

```
@Entity  
@Table(name = "book_category")  
public class BookCategory {  
    private int id;  
    private String name;  
    private Set<Book> books;  
  
    public BookCategory(){ ... }  
  
    public BookCategory(String name) {...}  
  
    @Id  
    @GeneratedValue(strategy = GenerationType.AUTO)  
    public int getId() { ... }  
  
    public void setId(int id) { ... }  
  
    public String getName() {...}  
  
    public void setName(String name) { ... }  
  
    @Repository  
    public interface BookCategoryRepository extends JpaRepository<BookCategory, Integer>{  
        public Set<Book> getBooks() { ... }  
        ...  
    }  
    for( Book b : BookRepo.findAll() )  
        System.out.println( b.toString() + b.bookCategory.toString() )  
  
    @Entity  
    public class Book{  
        private int id;  
        private String name;  
        private BookCategory bookCategory;  
  
        public Book() {}  
  
        public Book(String name) { this.name = name;}  
  
        public Book(String name, BookCategory bookCategory) { ... }  
  
        @Id  
        @GeneratedValue(strategy = GenerationType.AUTO)  
        public int getId() { ... }  
  
        public void setId(int id) { ... }  
  
        public String getName() { ... }  
  
        @JoinColumn(name = "book_category_id")  
        public BookCategory getBookCategory() { ... }  
  
        setBookCategory(BookCategory bookCategory) {...}  
  
        select * from book;  
        select * from bookCategory where bookCategory = ?  
        ...  
        select * from bookCategory where bookCategory = ?
```

# Prefetching

- Instead of using global fetching strategies, one can define how objects/collections related to one particular entity are loaded to memory

```
fun appointmentsOfPet(id: Long): List<AppointmentDAO> {  
    val pet = pets.findById(id)  
        .orElseThrow { NotFoundException("There is no Pet with Id $id") }  
    return pet.appointments  
}
```

Two queries

```
interface PetRepository : JpaRepository<PetDAO, Long> {  
    @Query("select p from PetDAO p inner join fetch p.appointments where p.id = :id")  
    fun findByIdWithAppointment(id:Long) : Optional<PetDAO>  
}
```

```
fun appointmentsOfPet(id: Long): List<AppointmentDAO> {  
    val pet = pets.findByIdWithAppointment(id)  
        .orElseThrow { NotFoundException("There is no Pet with Id $id") }  
    return pet.appointments  
}
```

Appointment's collections is fetched and loaded in one single query

# Custom queries for efficient execution

---

- ORM relations can produce a large number of queries... which can be optimized by means of a single query being dispatched to the DB

```
@Query(" select s from Student s "+  
       "   inner fetch join s.courses en "+  
       "   inner join en.course c "+  
       " where c.name = :name")  
List<Student> searchByCourse(@Param("name") String name);
```

- Optimization may work by summarising data

```
@Query("select new ciai.model.StudentSummary(s.name,s.age) from Student s")  
List<StudentSummary> summaryStudents();
```

# Java Persistence Query Language (JPQL ⊂ HQL)

---

- Simple custom queries

```
@Query("select s from Student s where s.name like CONCAT(?:, '%')")  
List<Student> search(String name);
```

- Complex custom queries

```
@Query(" select s from Student s "+  
        "   inner join s.courses en "+  
        "   inner join en.course c "+  
        " where c.name = :name")  
List<Student> searchByCourse(@Param("name") String name);
```

Now it's time for you to  
research and experiment...

# Internet Applications Design and Implementation

## 2020 - 2021

### (Lab class 4)

**MIEI - Integrated Master in Computer Science and Informatics  
Specialization block**

**João Costa Seco ([joao.seco@fct.unl.pt](mailto:joao.seco@fct.unl.pt))  
Eduardo Geraldo ([e.gerald@campus.fct.unl.pt](mailto:e.gerald@campus.fct.unl.pt))**

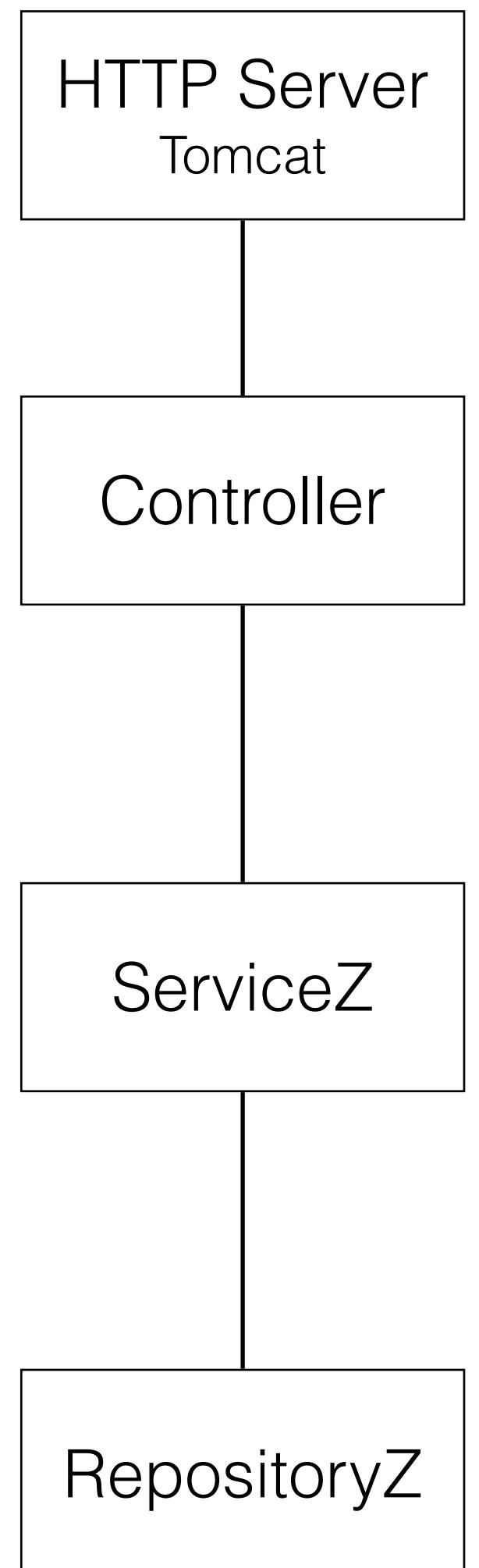


FACULDADE DE  
CIÊNCIAS E TECNOLOGIA  
UNIVERSIDADE NOVA DE LISBOA

# Lab class 4 - Software Architecture using Spring

- Lab Objectives:

1. Check your group status in the spreadsheet with the link below:  
<https://docs.google.com/spreadsheets/d/1CUIXcvIXmU4tH71L2Ox-sGSLuXSDw73AHmorznQNS44/edit?usp=sharing>
2. Create an Architecture with internal services and repositories
3. Test the architecture for at least one entity using Mock components
4. Define the data model for resource Application (no relations yet)
5. Implement the functionality of one resource (Application)



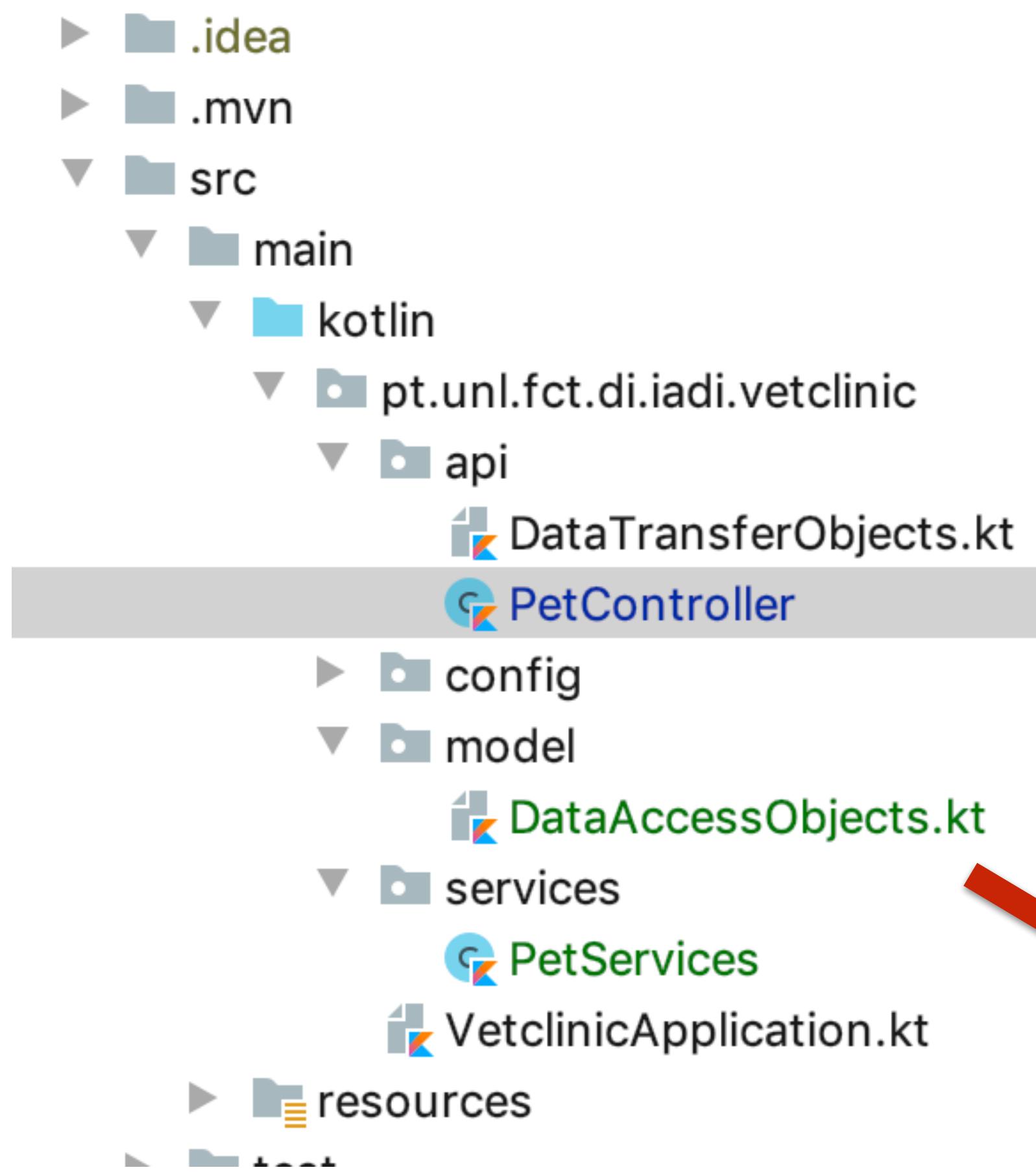
# Lab class 4 - Introduction to Spring and Swagger

---

- Lab Protocol:
  1. Check your group status in the spreadsheet with the link
  2. Make sure that you have the whole API defined and documented with Swagger
  3. Create an internal service class for each top-level resource and wire the calls from controller to service
  4. Create Exceptions for NotFound errors that are thrown by the service
  5. Add JPA Entities for resource Application (ApplicationDAO)
  6. Create tests that separately test the controller and the service for resource Application
  7. Create a repository for Application using database h2 (in memory)
  8. You may want to also create tests for the repository to understand better the data operations
  9. Implement the service using the repository's basic functions.
  10. Create a Repository for Applications and Students
  11. Insert seed data into the database
  12. Produce efficient queries to search Applications by date
  13. Produce a search filter in the “List all applications” endpoint

# Lab class 4 - Create internal services

- Create and wire a Service Class, redirect the calls, Make DAO-DTO transformation

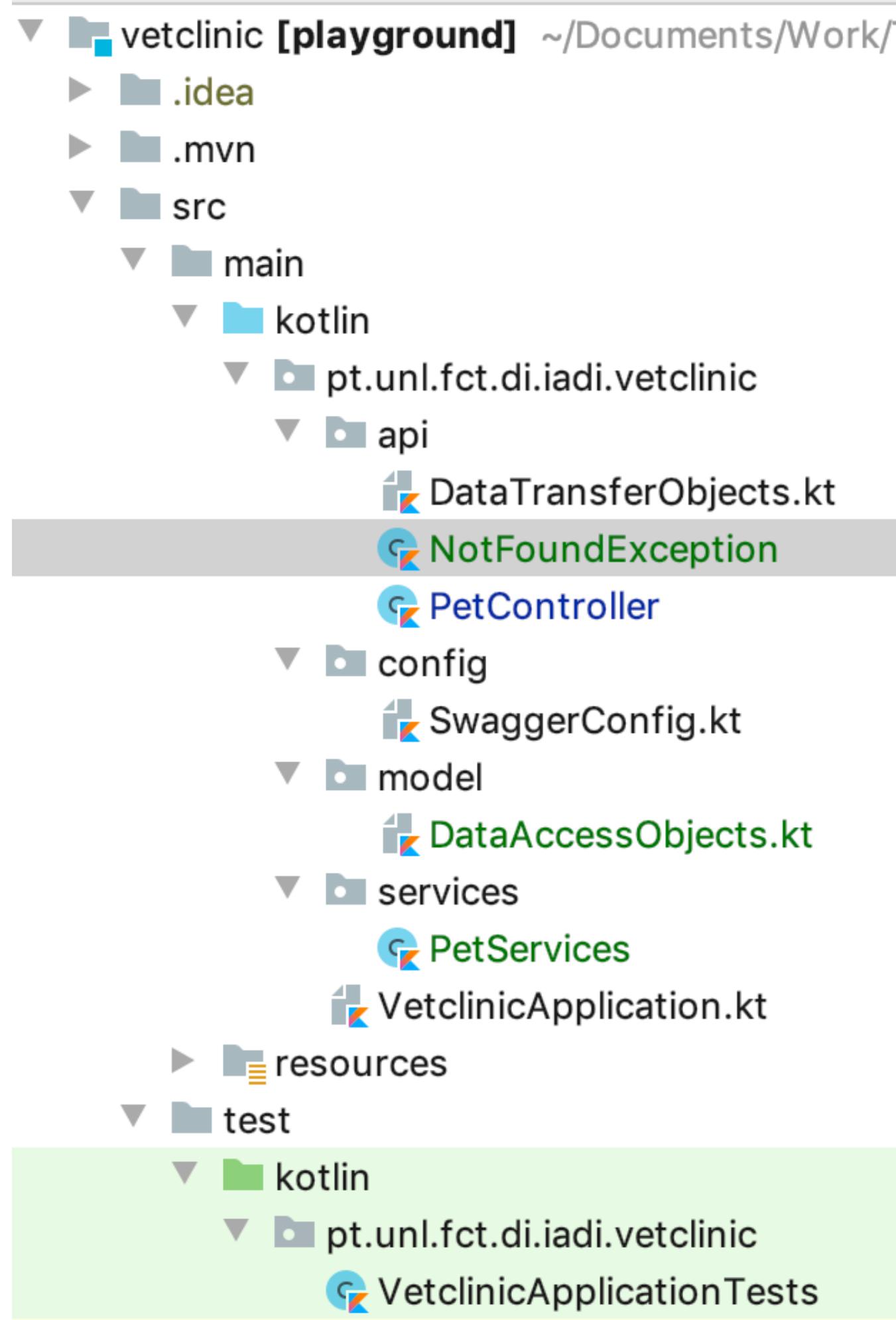


```
@RestController  
@RequestMapping( ...value: "/pets")  
class PetController(val pets:PetServices) {  
  
    @GetMapping( ...value: "")  
    fun getAllPets() =  
        pets.getAllPets().map { PetDTO(it.id, it.name, it.species) }  
  
    @PostMapping( ...value: "")  
    fun addNewPet(@RequestBody pet:PetDTO) =  
        pets.addOnePet(PetDAO(pet.id,pet.name,pet.species))  
  
    data class PetDAO(val id:Long, val name: String, val species: String)
```

Red arrows point from the code snippets to the corresponding parts of the project structure. One arrow points from the first code snippet to the PetController file in the api folder. Another arrow points from the second code snippet to the PetDAO definition at the bottom. A third arrow points from the third code snippet to the PetServices file in the services folder.

# Lab class 4 - Exceptions

- Create Exceptions should be used to represent REST Errors



```
package pt.unl.fct.di.iadi.vetclinic.api

class NotNotFoundException(msg:String) : RuntimeException(msg)

@Service
class PetServices {

    fun getAllPets(): List<PetDAO> = emptyList()

    fun getOnePet(id:Long) =
        if (id == 1L)
            PetDAO(id, name: "Pantufas", species: "Dog")
        else
            throw NotNotFoundException("Pet $id not found")

    fun addOnePet(pet:PetDAO) {}

}
```

# Lab class 4 - Tests with mock objects

- Create a basic test for the service PetServices

The screenshot shows the IntelliJ IDEA interface with the following components:

- Project Structure:** On the left, the project tree shows the `vetclinic [playground]` project with its modules (`.idea`, `.mvn`, `src`, `test`) and source files (`DataTransferObjects.kt`, `NotFoundException.kt`, `PetController.kt`, `SwaggerConfig.kt`, `DataAccessObjects.kt`, `PetServices.kt`, `VetclinicApplication.kt`, etc.). The `PetServiceTester.kt` file is selected in the `test/kotlin` directory.
- Code Editor:** The main window displays the `PetServiceTester.kt` file content:import org.hamcrest.CoreMatchers.equalTo
import org.junit.Assert
import org.junit.Test
import org.junit.runner.RunWith
import org.springframework.beans.factory.annotation.Autowired
import org.springframework.boot.test.context.SpringBootTest
import org.springframework.test.context.junit4.SpringRunner
import pt.unl.fct.di.iadi.vetclinic.services.PetServices

@RunWith(SpringRunner::class)
@SpringBootTest
class PetServiceTester {

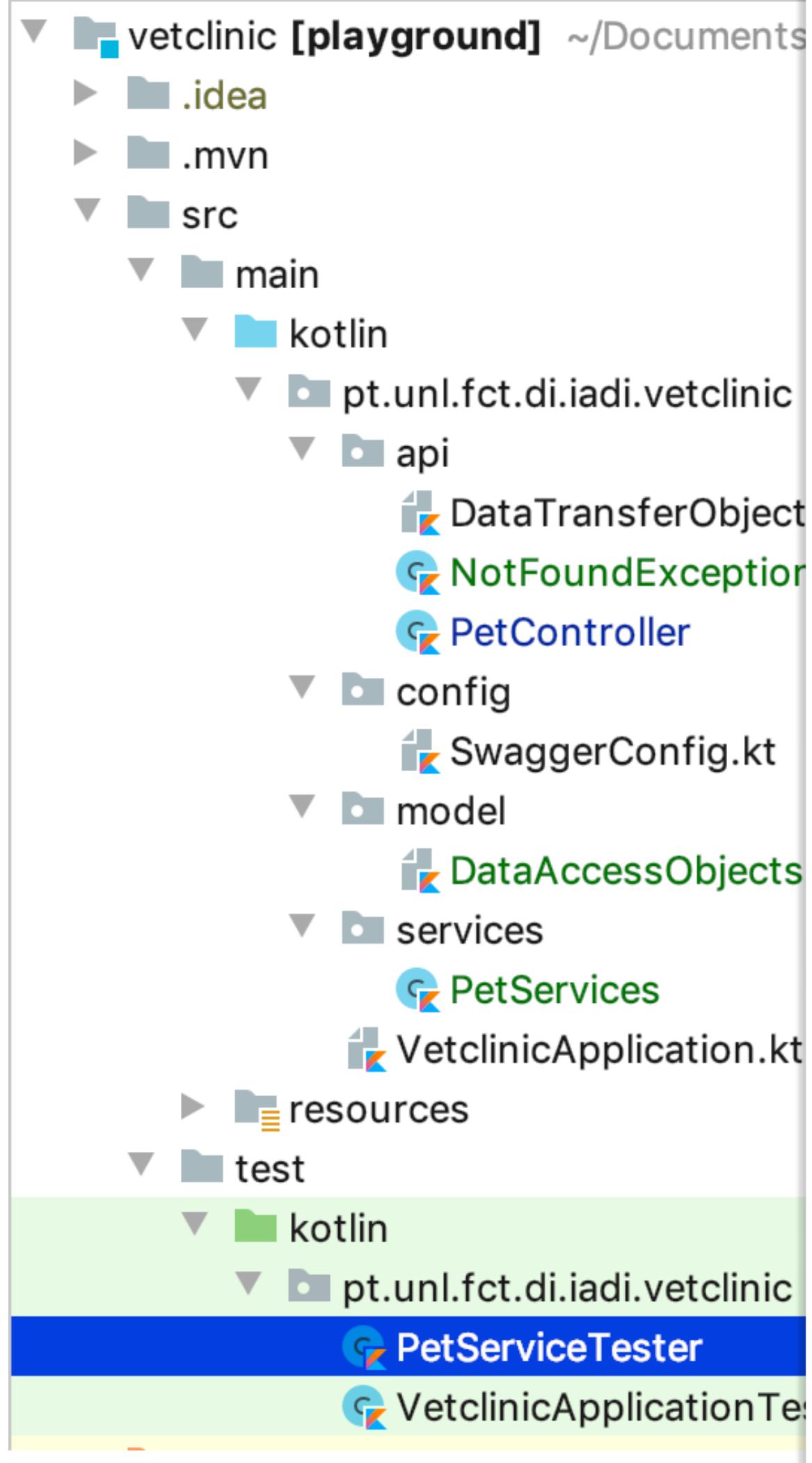
 @Autowired
 lateinit var pets:PetServices

 @Test
 fun `basic test on getAll`() {
 Assert.assertThat(pets.getAllPets(), equalTo(emptyList()))
 }
}
- Run Results:** On the right, the `Run` tool window shows the test results for `PetServiceTester`:

Test	Time
PetServiceTester (pt.unl.fct.di.iadi.vetclinic.services.PetServiceTester)	326 ms
basic test on getAll	326 ms

# Lab class 4 - Test

- Test all methods



```
@RunWith(SpringRunner::class)
@SpringBootTest
class PetServiceTester {

    @Autowired
    lateinit var pets:PetServices

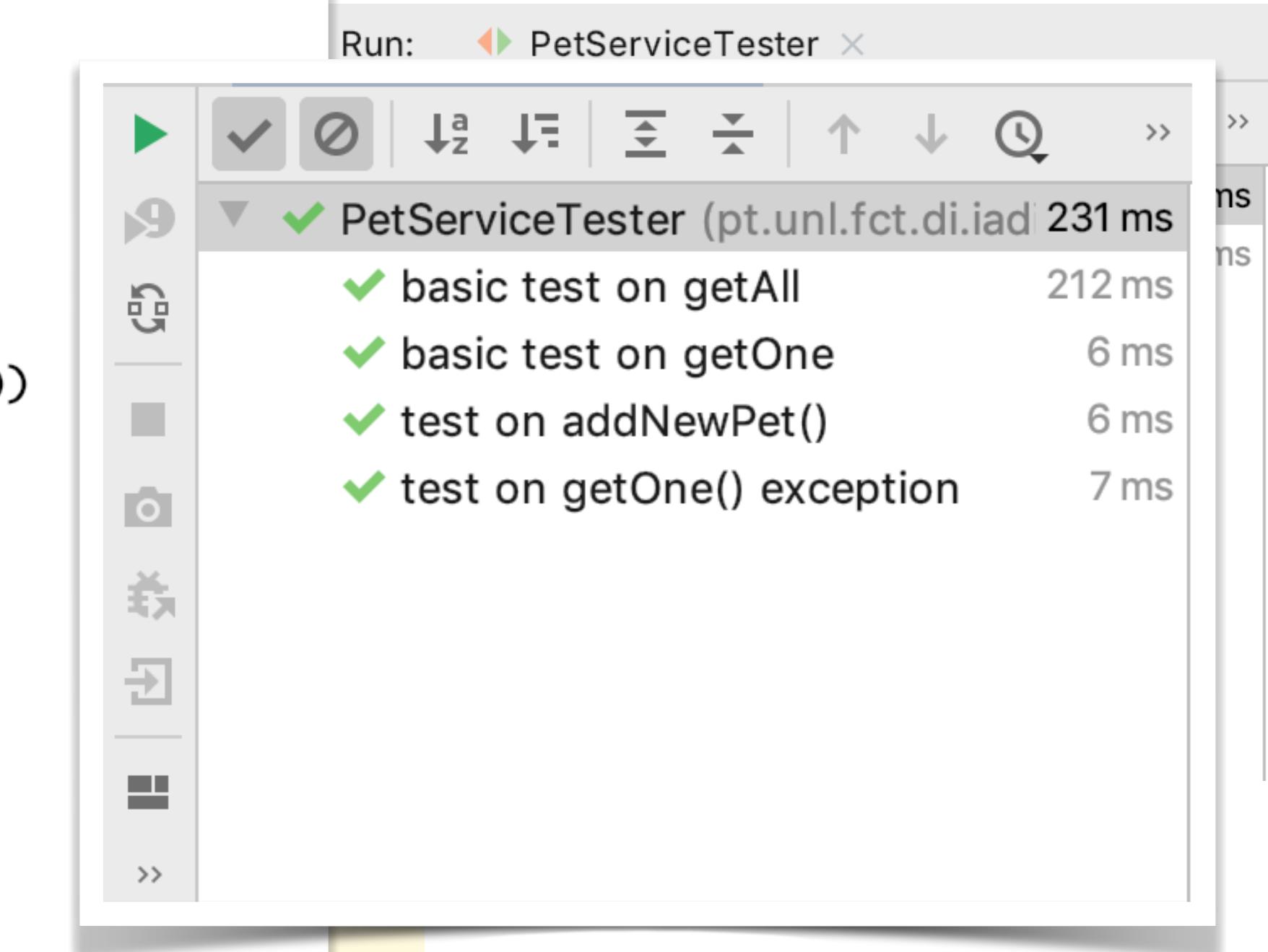
    companion object Contants {
        val pantufas = PetDAO(id: 1L, name: "Pantufas", species: "Dog")
    }

    @Test fun `basic test on getAll`() {
        assertThat(pets.getAllPets(), equalTo(emptyList()))
    }

    @Test fun `basic test on getOne`() {
        assertThat(pets.getOnePet(id: 1L), equalTo(pantufas))
    }

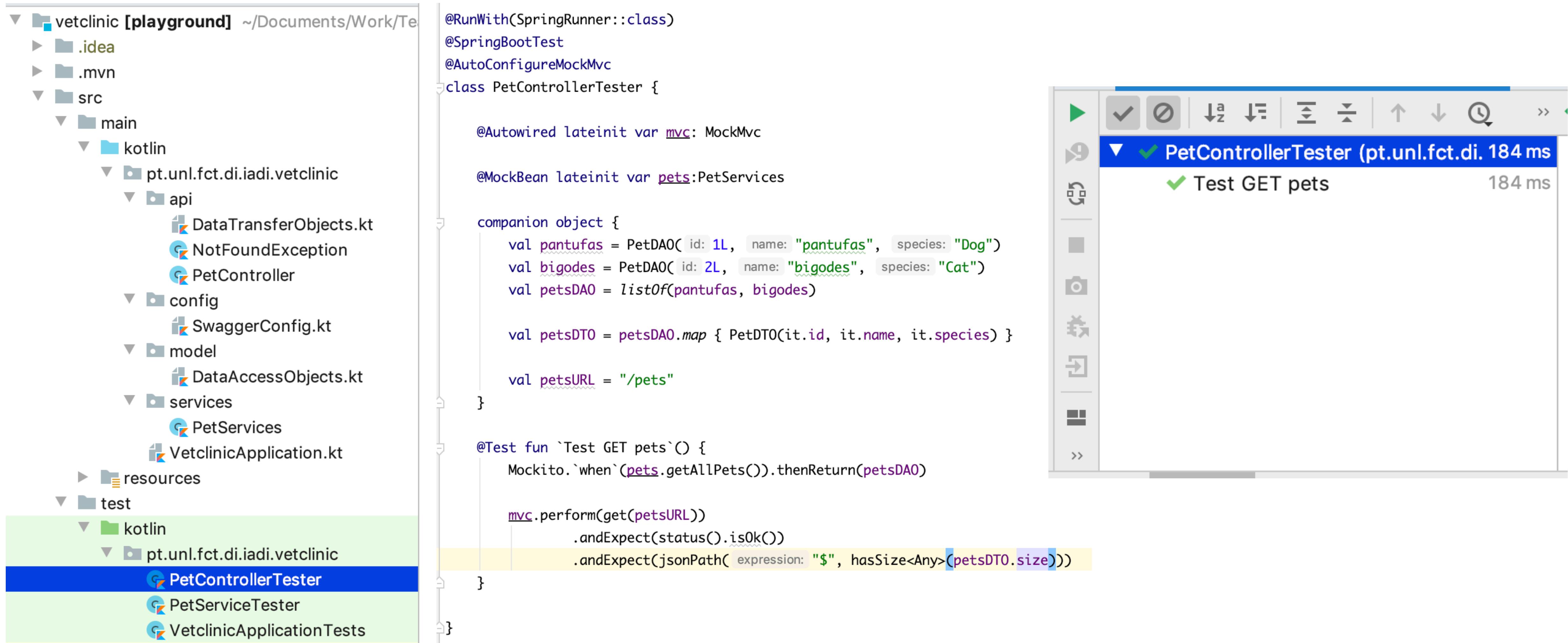
    @Test(expected = NotFoundException::class)
    fun `test on getOne() exception`() {
        pets.getOnePet(id: 0L)
    }

    @Test
    fun `test on addNewPet`() {
        pets.addOnePet(pantufas)
        assertThat(pets.getOnePet(pantufas.id), equalTo(pantufas))
    }
}
```



# Lab class 4 - Tests with mock objects

- Create a test for controllers mocking the corresponding service



The image shows a screenshot of an IDE interface. On the left, there is a file tree for a project named "vetclinic [playground]". The "test" directory contains three files: "PetControllerTester", "PetServiceTester", and "VetclinicApplicationTests". The "PetControllerTester" file is currently selected and shown in the code editor. The code in the editor is a Kotlin test class for a PetController. It uses annotations like @RunWith, @SpringBootTest, and @AutoConfigureMockMvc. It defines a companion object with two pet DAO instances and their corresponding DTOs. It then tests the GET /pets endpoint using Mockito's when() thenReturn() method to return the mocked DAO, and performs an expectation on the MockMvc's perform() method to check the status and JSON path of the response. On the right, there is a test results panel showing a single test named "PetControllerTester (pt.unl.fct.di. 184 ms)" which has passed, indicated by a green checkmark. The test name "Test GET pets" and its duration "184 ms" are also displayed.

```
@RunWith(SpringRunner::class)
@SpringBootTest
@AutoConfigureMockMvc
class PetControllerTester {

    @Autowired lateinit var mvc: MockMvc
    @MockBean lateinit var pets: PetServices

    companion object {
        val pantufas = PetDAO(id: 1L, name: "pantufas", species: "Dog")
        val bigodes = PetDAO(id: 2L, name: "bigodes", species: "Cat")
        val petsDAO = listOf(pantufas, bigodes)

        val petsDTO = petsDAO.map { PetDTO(it.id, it.name, it.species) }
    }

    @Test fun `Test GET pets`() {
        Mockito.`when`(pets.getAllPets()).thenReturn(petsDAO)

        mvc.perform(get(petsURL))
            .andExpect(status().isOk())
            .andExpect(jsonPath( expression: "$", hasSize<Any>(petsDTO.size())))
    }
}
```

# Lab class 4 - Tests with mock objects

- Create a test for controllers mocking the corresponding service

The screenshot shows an IDE interface with a file tree on the left and a code editor on the right.

**File Tree:**

- vetclinic [play]
- .idea
- .mvn
- src
- main
- kotlin
- pt.
- resources
- test
- kotlin
- pt.

**Code Editor (Kotlin Test Code):**

```
@Test fun `Test Get One Pet`() {  
    Mockito.`when`(pets.getOnePet(id: 1)).thenReturn(pantufas)  
  
    val result = mvc.perform(get(urlTemplate: "$petsURL/1"))  
        .andExpect(status().isOk)  
        .andReturn()  
  
    val responseString = result.response.contentAsString  
    val responseDTO = mapper.readValue<PetDTO>(responseString)  
    assertThat(responseDTO, equalTo(petsDTO[0]))  
}  
  
@Test fun `Test GET One Pet (Not Found)`() {  
    Mockito.`when`(pets.getOnePet(id: 2)).thenThrow(NotFoundException("not found"))  
  
    val result = mvc.perform(get(urlTemplate: "$petsURL/2"))  
        .andExpect(status().is4xxClientError)  
}
```

**Run Configuration:**

- ControllerTester (pt.unl.fct.di. 184 ms)
- ET pets 184 ms

**Page Footer:**

Internet Applications Design 272

# Lab class 4

- Import new Components (Spring-Data & H2)
- Declare DAO @Entity classes
- Declare repositories and implement services

```
<dependency>
    <groupId>org.springframework.boot</groupId>
    <artifactId>spring-boot-starter-data-jpa</artifactId>
</dependency>
<dependency>
    <groupId>com.h2database</groupId>
    <artifactId>h2</artifactId>
    <scope>runtime</scope>
</dependency>
```

```
@Service
class PetServices {
    @Autowired
    lateinit var pets: PetRepository

    fun getAllPets(): MutableIterable<PetDAO> = pets.findAll()

    fun getOnePet(id: Long): PetDAO {
        val pet = pets.findById(id)
        if (pet.isPresent)
            return pet.get()
        else
            throw NotFoundException("There is no pet with Id ${id}")
    }
}
```

```
import javax.persistence.*

@Entity
data class PetDAO(
    @Id @GeneratedValue val id: Long,
    val name: String,
    val species: String)
```

# Lab class 4 - Mock the repository, test the service

---

# Internet Applications Design and Implementation

## 2020 - 2021

### (Lecture 5 - on Security)

**MIEI - Integrated Master in Computer Science and Informatics  
Specialization block**

**João Costa Seco ([joao.seco@fct.unl.pt](mailto:joao.seco@fct.unl.pt))**

(with previous participations of Jácome Cunha ([jacome@fct.unl.pt](mailto:jacome@fct.unl.pt)) and João Leitão ([jc.leitao@fct.unl.pt](mailto:jc.leitao@fct.unl.pt)),  
contributions from Beatriz Moreira, APDC-INV 2017/2018)



**FACULDADE DE  
CIÊNCIAS E TECNOLOGIA  
UNIVERSIDADE NOVA DE LISBOA**

# Security of Applications (Overview)

---

- Security is one of the most hot topics in CS in present days!
- Cryptography can only protect data outside of systems, when properly applied and if there are no “internal” information leaks.
- Security breaches are often caused by crashes, erroneous behaviour due to unexpected inputs, or errors in the code.

# Security of Applications (Overview)

---

- Good engineering practices and correct usage of methods and tools ensures that the specified data confidentiality rules are enforced.
- There are two elective courses in MIEI only about this topic.
  - Software Security: fundamental concepts and technologies
  - Network and Computer Systems Security: system-level security
- This lecture is about models and frameworks that implement software security.

# Outline

---

- Security Concepts Review
- Foundations of Computer Security
- Security Models
- Kotlin and Spring Security
- Model-Based Access Control in Spring

# Internet Applications Design and Implementation

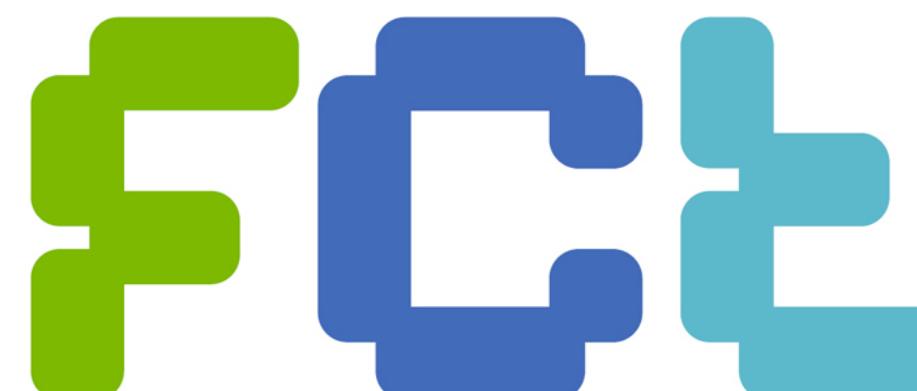
## 2020 - 2021

### (Lecture 5 - Part 1 - Security Concepts)

**MIEI - Integrated Master in Computer Science and Informatics  
Specialization block**

**João Costa Seco ([joao.seco@fct.unl.pt](mailto:joao.seco@fct.unl.pt))**

(with previous participations of Jácome Cunha ([jacome@fct.unl.pt](mailto:jacome@fct.unl.pt)) and João Leitão ([jc.leitao@fct.unl.pt](mailto:jc.leitao@fct.unl.pt)))



FACULDADE DE  
CIÊNCIAS E TECNOLOGIA  
UNIVERSIDADE NOVA DE LISBOA

# Security of Internet Applications

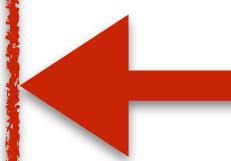
- Layers of internet application security
  - Network Level (network security and system identification)
  - System Level (firewalls, VPNs, SSL, DMZ)
  - Application Level (our focus)
    - Authentication
    - Access control
    - Information flow



# Big Picture - Organisation Industry Standards (ISO 27002)

- Definition of General Security policies
- Organization of information security
- Asset management
- Human resources security
- Physical and environmental security
- Communications and operations management
- Access control (data, operations, and other resources)
- Acquisition, development, and maintenance of Software Systems
- Incident management
- Compliance with regulations

**About software**



# Security Policies in Software Systems

---

- within an software system:
  - “The set of restrictions and properties that specify how a computing system prevents information and computing resources from being used to violate an organizational security policy” in Computer Security, Dieter Gollmann 2011
- define who has permission to access or operate on, a given resource.
  - Access control lists,
  - firewall settings,
  - services that may be run on user devices,
  - security protocols for protecting network traffic,
  - ...

# Attacks and Attackers

- Security can be defined and challenged based on the definition of attacks and attackers. What does an attacker knows and what operations can they perform on a system.
- The correct functioning of a system is based on assumptions on the environment.
- Attacks are designed to challenge system assumptions with illegal inputs, causing illegal states, erroneous behaviour or crashes.

## Firefox Bug Bounty Rewards

On behalf of the Mozilla and the millions of people who visit our sites, use Firefox and our other products we would like to thank them for their hard work in helping to make us more secure.

As of this date, we have paid out almost **\$1,000,000** across all of our bounties. Congratulations to everybody who has participated!

### – 2018

#### 1st Quarter 2018

- Tadj Youssouf
- James Grant
- xisigr
- Root Object
- Jun Kokatsu
- mozillabugs
- Abdulrahman Alqabandi
- Jordi Chancel
- Konark Modi
- Francisco Alonso of NowSecure Research Team
- Zhang Hanming from 360 Vulcan team
- Nils
- Omair
- Rob Wu [:robwu]
- David Dworken

[Mozilla Security](#)

[Advisories](#)

[Known Vulnerabilities](#)

[Mozilla Security Blog](#)

[Security Bug Bounty](#)

[Client Bug Bounty](#)

[Frequently Asked Questions](#)

Hall of Fame

[Web Bug Bounty](#)

[Eligible Websites](#)

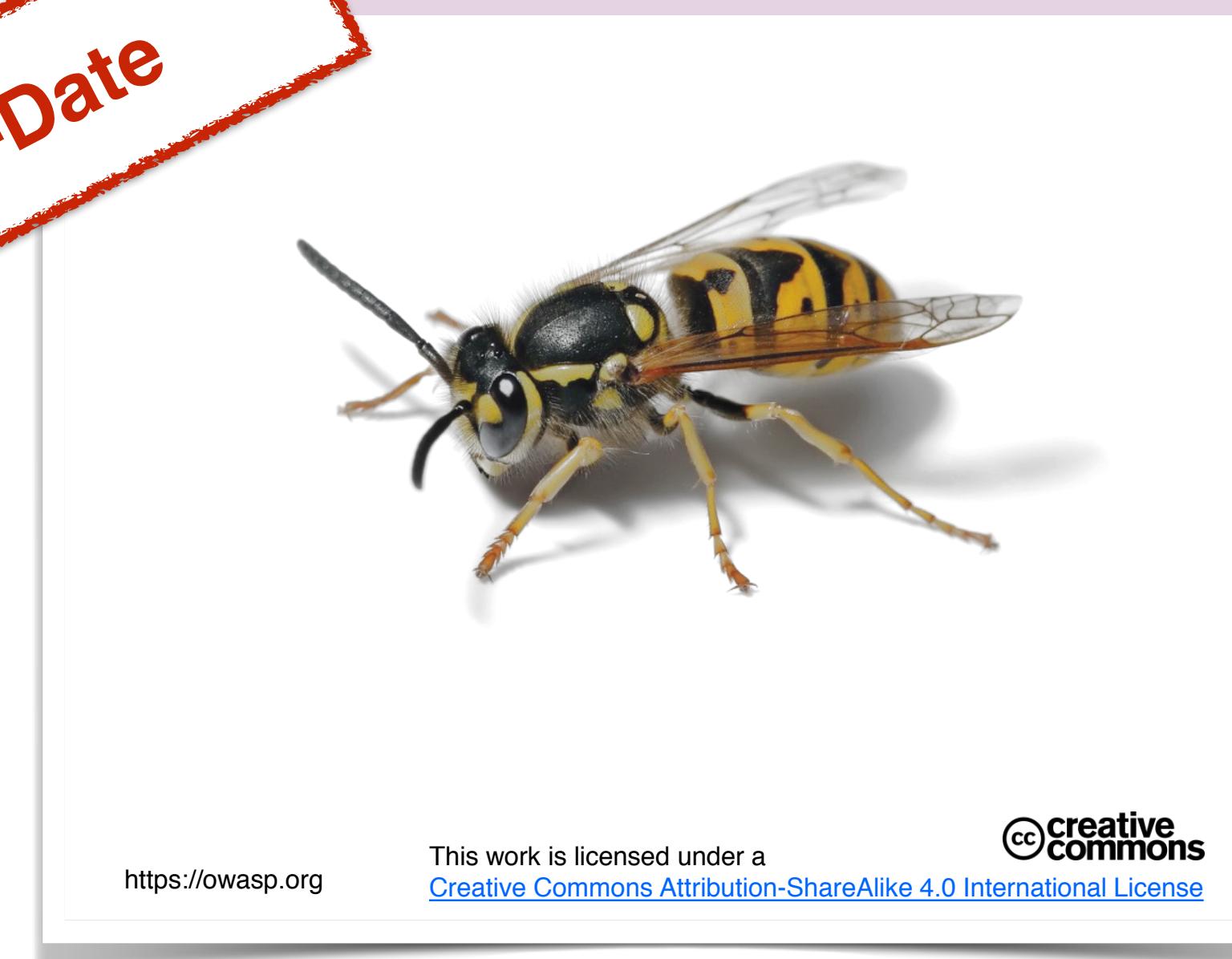
[Frequently Asked Questions](#)

Hall of Fame

# Security flaws in software



**Still Up-to-Date**



<https://owasp.org> This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License

© creative commons

## OWASP Top 10 - 2017

A1:2017-Injection

A2:2017-Broken Authentication

A3:2017-Sensitive Data Exposure

A4:2017-XML External Entities (XXE) [NEW]

A5:2017-Broken Access Control [Merged]

A6:2017-Security Misconfiguration

A7:2017-Cross-Site Scripting (XSS)

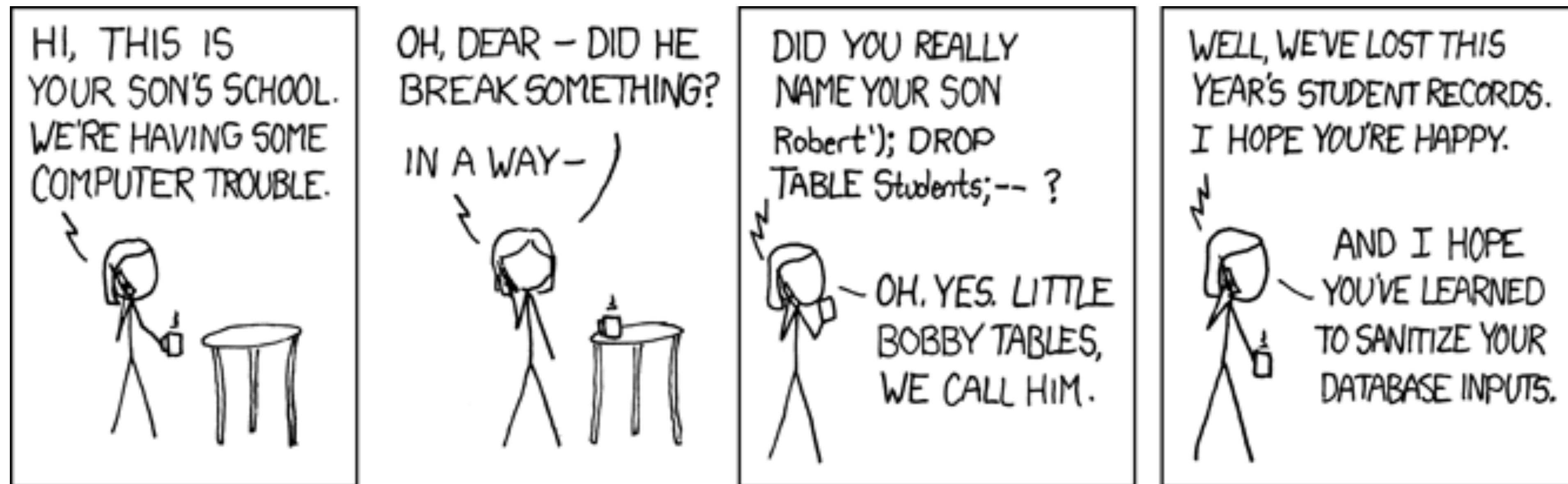
A8:2017-Insecure Deserialization [NEW, Community]

A9:2017-Using Components with Known Vulnerabilities

A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

<https://www.owasp.org/>

# Classic Example: SQL injection



# Classic Example: SQL injection

User Name:	<input "="" \"="" or="" type="text" value="\"/>
Password:	<input "="" \"="" or="" type="text" value="\"/>

```
uName = getRequestString("username");
uPass = getRequestString("userpassword");

sql = 'SELECT * FROM Users WHERE Name ='
+ uName + '\" AND Pass =\"' + uPass + '\"'
```

## Result

```
SELECT * FROM Users WHERE Name ="" or ""="" AND Pass ="" or ""=""
```

[https://www.w3schools.com/sql/sql\\_injection.asp](https://www.w3schools.com/sql/sql_injection.asp)

# In a nutshell

---

Most common attacks are at the application level and can be avoided by properly using well tested and tested frameworks and well established methods.

# Internet Applications Design and Implementation

## 2020 - 2021

### (Lecture 5 - Part 2 - Foundations)

**MIEI - Integrated Master in Computer Science and Informatics  
Specialization block**

**João Costa Seco ([joao.seco@fct.unl.pt](mailto:joao.seco@fct.unl.pt))**

(with previous participations of Jácome Cunha ([jacome@fct.unl.pt](mailto:jacome@fct.unl.pt)) and João Leitão ([jc.leitao@fct.unl.pt](mailto:jc.leitao@fct.unl.pt)))



**FACULDADE DE  
CIÊNCIAS E TECNOLOGIA  
UNIVERSIDADE NOVA DE LISBOA**

# Foundations of Computer Security

---

- Fundamental Properties:
  - **confidentiality** - prevention of unauthorised disclosure of information,
  - **integrity** - prevention of unauthorised modification of information,
  - **availability** - prevention of unauthorised withholding of information or resources
  - ... more... accountability; non-repudiation; reliability/dependability; ...

“Computer security deals with the prevention and detection of unauthorized actions by users of a computer system” - Dieter Gollmann,

# Foundations of Software Security

---

- Main concepts used in software security
  - **Principal** (the active subject)
  - **Resource** (the passive object)
  - **Authentication** - the principal provides proof that they are who they say they are
  - **Authorisation** - the principal is trusted to access or perform an operation on a resource
  - **Delegation** - can you operate on behalf of other principal?
- Declassification operations in confidentiality analysis
- Endorsement operations in integrity analysis

# Principal/Authentication

---

- An authenticated entity (or group) that uses the system
- The active subject on system operations
- **Authentication:**
  - The certification process of determining the identity of an external entity that uses the system, invokes actions, produces and consumes data.

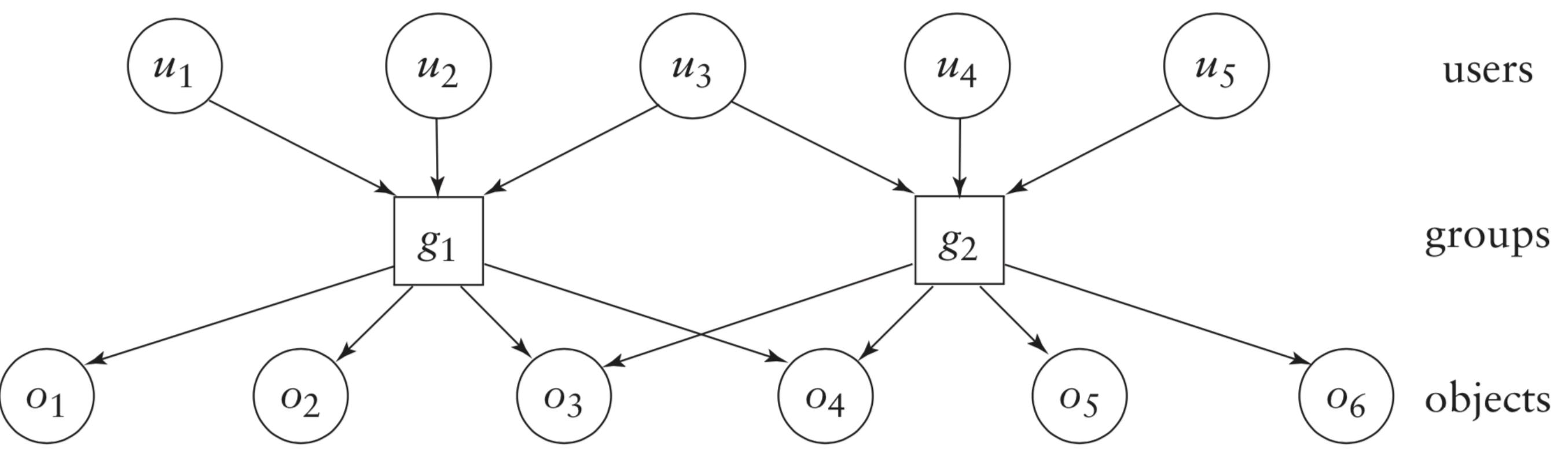
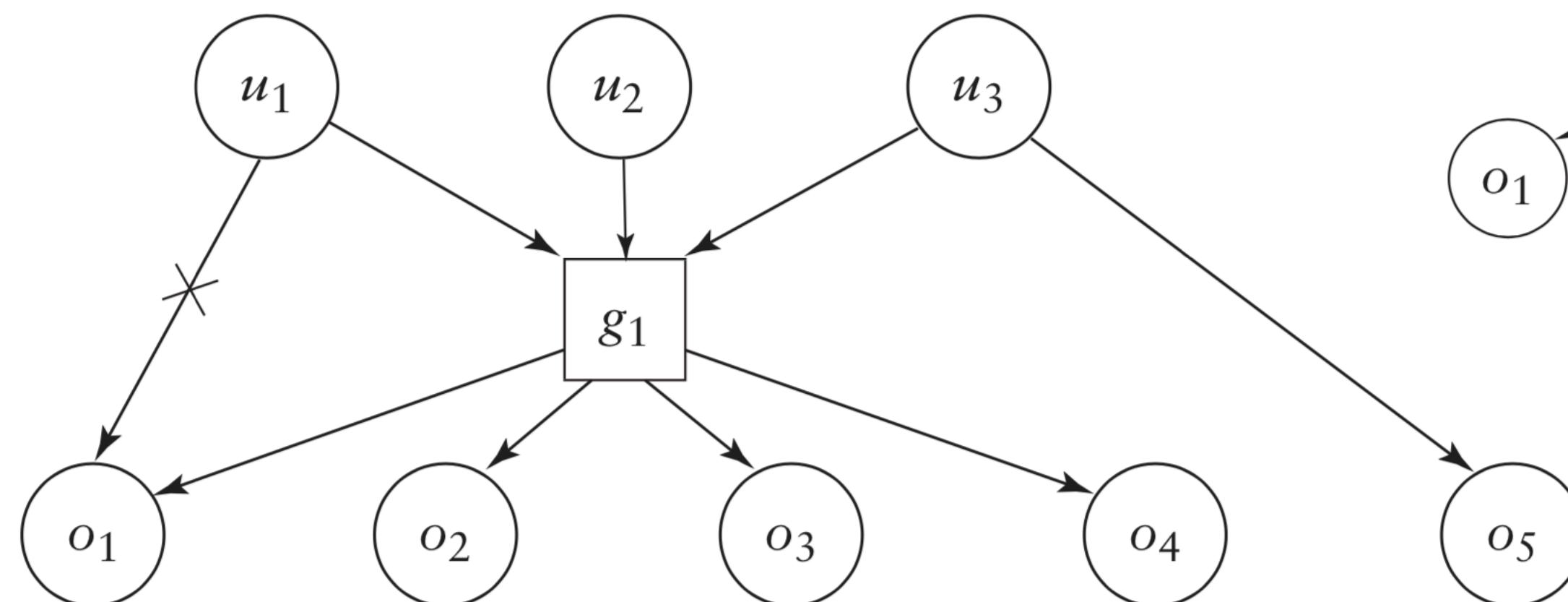
# Resource/Authorisation

---

- The process of checking what resources a principal is allowed to access and manipulate, and what operations is it allowed to execute at a given time and system state (data, parameters, context, etc.).
- **Authorisation** (to observe or change)
  - read, execute, write, append, delete, change access, change ownership, ...
  - Classic access control models
    - Access Control Matrix
    - Capabilities
    - Access Control Lists

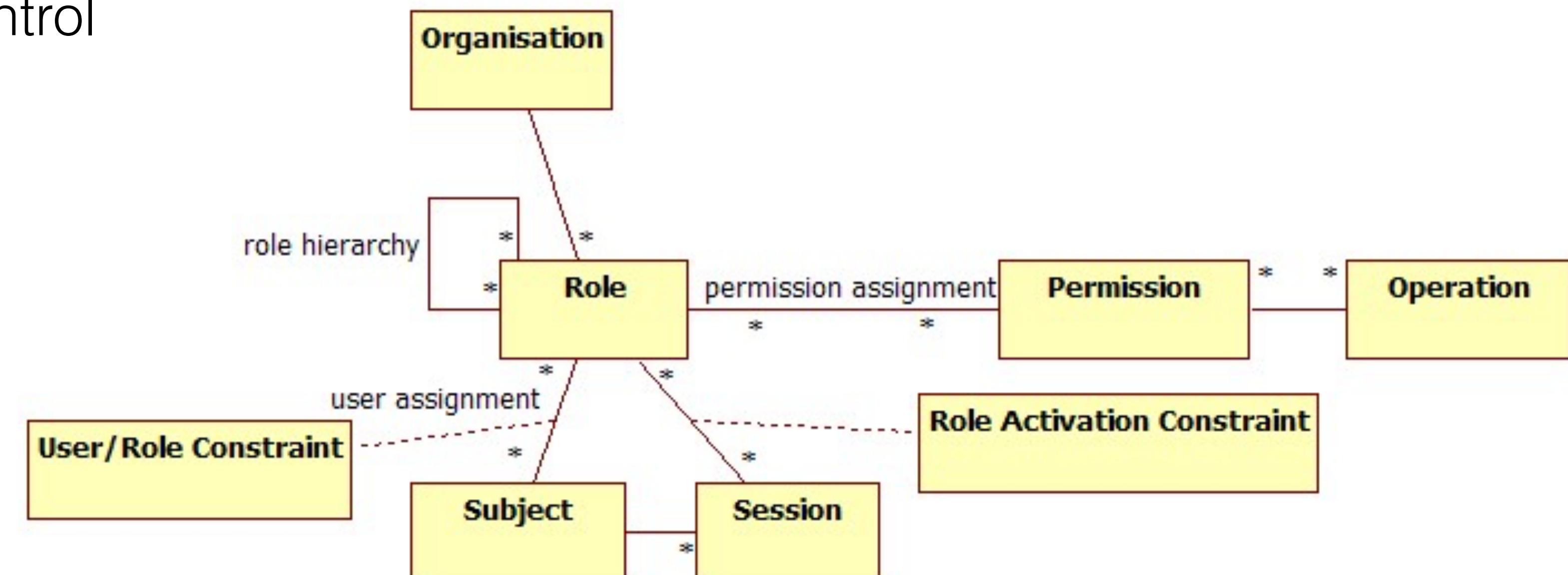
# Authorisation and access control models

- Base models
  - Access Control Matrix; Capabilities; Access Control Lists
- Intermediate control structures
  - Groups and negative permissions



# Authorisation and access control models

- Base models
  - Access Control Matrix; Capabilities; Access Control Lists
- Intermediate control structures
  - Role-based access control
    - Principal
    - Roles
    - Permissions
    - Operations
    - Resources



# Internet Applications Design and Implementation

## 2020 - 2021

### (Lecture 5 - Part 3 - Security Models)

**MIEI - Integrated Master in Computer Science and Informatics  
Specialization block**

**João Costa Seco ([joao.seco@fct.unl.pt](mailto:joao.seco@fct.unl.pt))**

(with previous participations of Jácome Cunha ([jacome@fct.unl.pt](mailto:jacome@fct.unl.pt)) and João Leitão ([jc.leitao@fct.unl.pt](mailto:jc.leitao@fct.unl.pt)))



FACULDADE DE  
CIÊNCIAS E TECNOLOGIA  
UNIVERSIDADE NOVA DE LISBOA

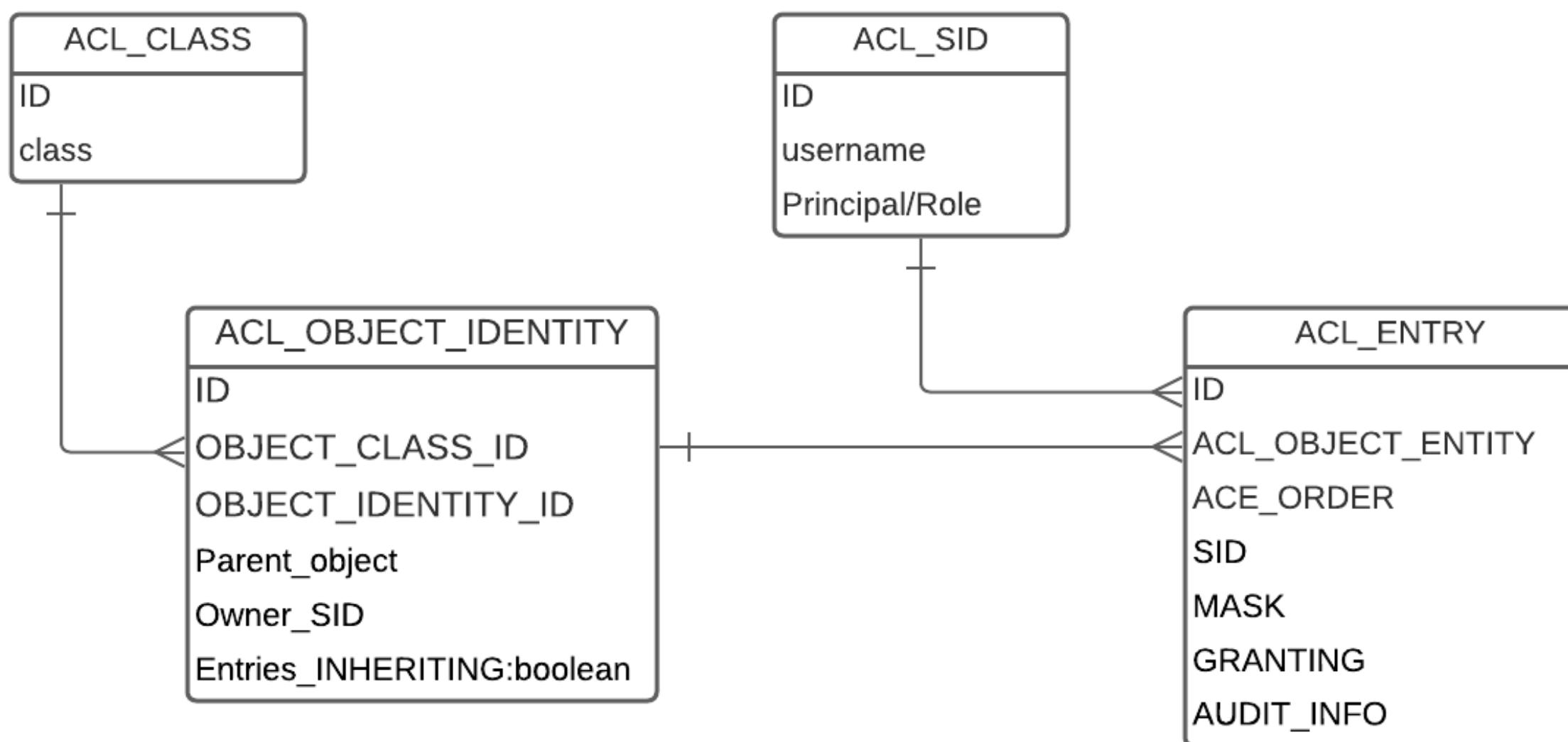
# Security Models

---

- Access Control List
- Capability-based access control
- Role-based access control
- Bell–LaPadula model for confidentiality
- Biba Integrity model for data integrity
- Model-based access control

# Access Control Lists

- ACLs are lists of permissions (identity, operation) attached to objects stored within the system.
- It must explicitly assign individual identities to operations on resources.
- Spring Security ACL implements ACL on top of explicitly managed database tables



```
@PostFilter("hasPermission(filterObject, 'READ')")
List<NoticeMessage> findAll();

@PostAuthorize("hasPermission(returnObject, 'READ')")
NoticeMessage findById(Integer id);

@PreAuthorize("hasPermission(#noticeMessage, 'WRITE')")
NoticeMessage save(@Param("noticeMessage")NoticeMessage noticeMessage);
```

<https://www.baeldung.com/spring-security-acl>

# Capability-based access control

---

- A decentralised method that provides a scalable approach to access control
  - No need for centralised access control lists and mechanisms;
  - A capability refers to an object and a set of rights, the user that owns it can perform the operation described in the capability
  - Example: a pair (“/etc/pass”, O\_RDWR) gives readwrite access
  - Common in micro-service based architectures and IoT scenarios

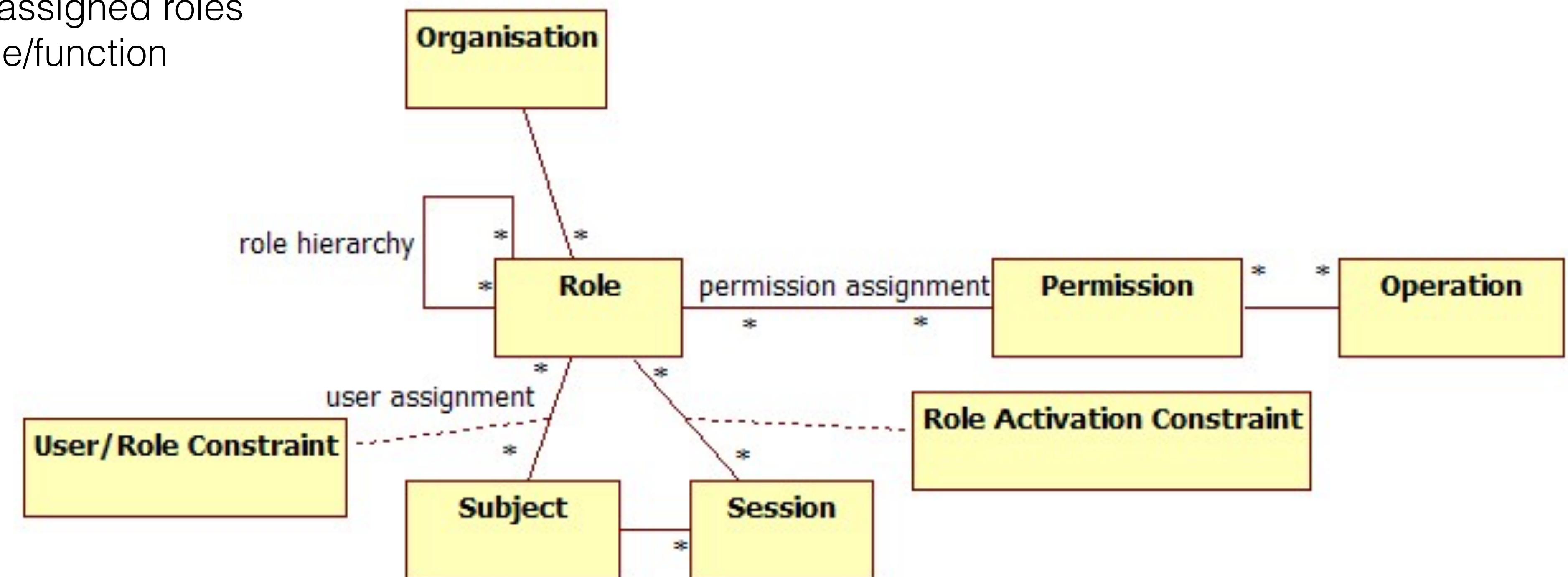
# Capability-based access control

---

- A capability is transmitted through unforgeable (and ephemeral) tokens
- Capabilities can be explicitly and dynamically managed
  - Good support for authorisation and delegation
- To perform an operation on a particular object, the principal has first to acquire the associated capability via some dynamic authorisation method.

# Role-Base Access Control

- Standard approach to authorise users to perform operations in software systems.
  - Roles are specified for system related tasks
  - Permissions are assigned to specific roles
  - Users are dynamically assigned roles according to their profile/function



<https://upload.wikimedia.org/wikipedia/en/c/c3/RBAC.jpg>

# Role-Base Access Control

- Standard approach to authorise users to perform operations in software systems.
  - Roles are specified for system related tasks
  - Permissions are assigned to specific roles
  - Users are dynamically assigned to roles according to their needs
- **Roles can also be combined in hierarchies or lattices**
- **Delegation can be integrated in the general model**
- **RBAC provides a framework for a verification based on interceptors and filters**
- **Roles can also be parameterised and depend on actual data.**

Operation

<https://upload.wikimedia.org/wikipedia/en/c/c3/RBAC.jpg>

# Bell–LaPadula model - Confidentiality

- Formalises the U.S. Department of Defense multilevel security policies.
- The security level of a subject is compared to the classification of the object (and the security compartment where it is stored)
- The access control rules state that:
  - A subject cannot read up
  - A subject cannot write down
  - + an access control matrix

TOP SECRET

SECRET

CONFIDENTIAL

PUBLIC

No Write Down

No Read Up

# Information Flow Control - Confidentiality

- The process of ensuring that data is only seen by trusted principals. This involves assigning a level of trust to data and principals.
- General technique to check it is called **information flow control**
- **Declassification:** The process of lowering the level of trust needed to access a given data item.

```
var high = 1  
var low = ... 10 + high ...
```

```
var low = 2  
if ( high > 0 ) low else 3
```

Operating  
Systems

R.S. Gaines  
Editor

## A Lattice Model of Secure Information Flow

Dorothy E. Denning  
Purdue University

# Biba Integrity model - Data Integrity

- Data integrity has three goals:
  - Prevent data modification by unauthorised principals
  - Prevent unauthorised data modification by authorised principals
  - Maintain internal and external data consistency
- The access control rules state that:
  - A subject cannot read up
  - A subject cannot write down
  - + an access control matrix

TOP SECRET

SECRET

CONFIDENTIAL

PUBLIC

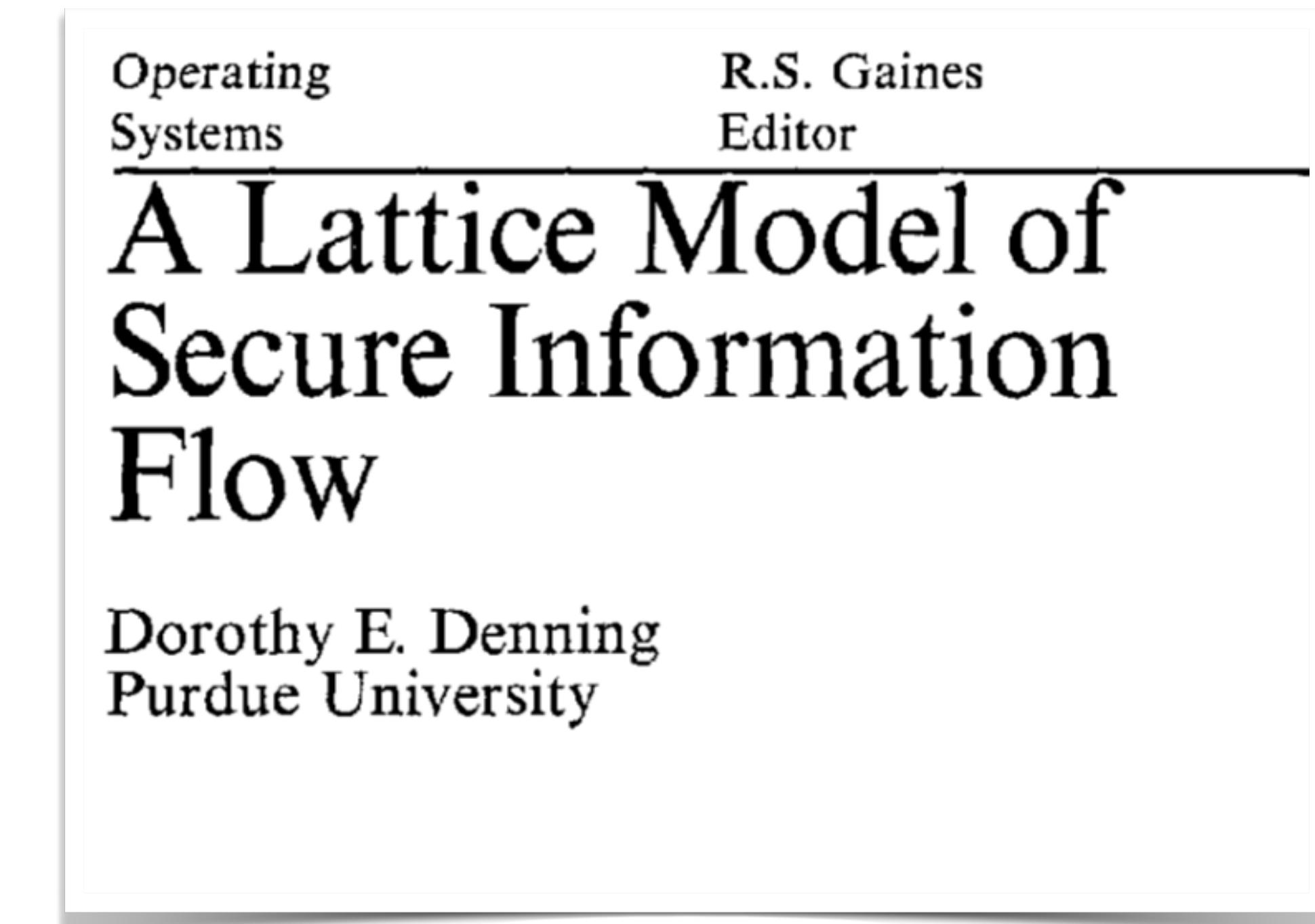
No Read Down

No Write Up

# Information Flow Control - Data Integrity

- The process of ensuring that data is only provided by trusted principals.
- Also an information flow control property (dual of confidentiality)
- **Endorsement:** the process of increasing the level of trust o a given data item.

```
var untrusted = 1  
var trusted = ... 10 + untrusted ...  
  
var trusted = 2  
if ( untrusted > 0 ) trusted else 3
```



# Model-Based Access Control

- Security conditions are many times hidden in query filters and program conditions. These policies are very difficult to get right, maintain, and modify.
- Developer-defined roles usually depend on the current state of the application. (e.g. ModeratorOf(...)). Role-based models usually ignore this and require the application logic to validate it.
- Example: authorisations usually depend on the state of the target entity (status == “submitted”)
- Capabilities defined by the developer can extend the standard read/write/delete (not hardwired to the basic programming elements)

## Type-based Access Control in Data-Centric Systems

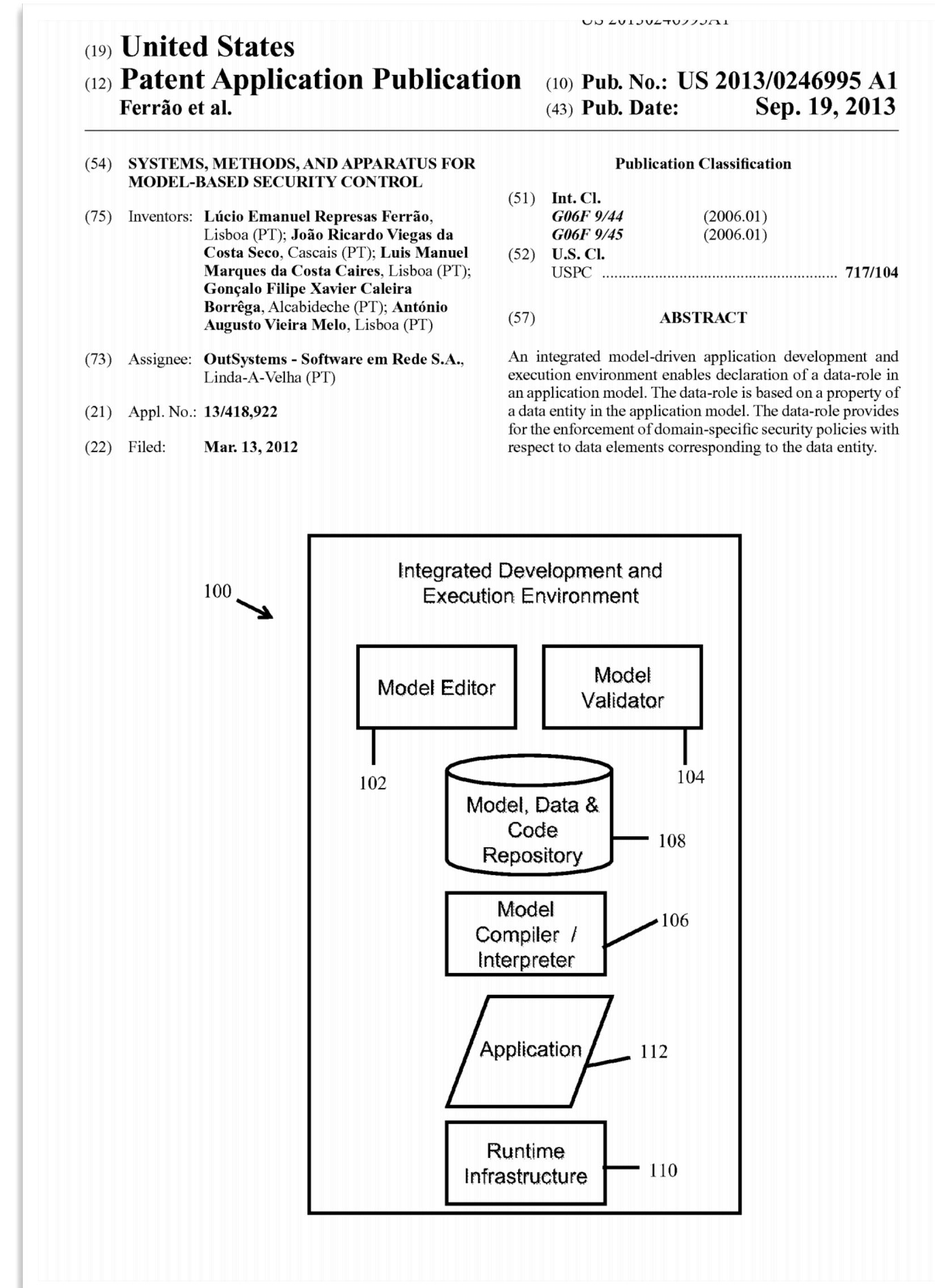
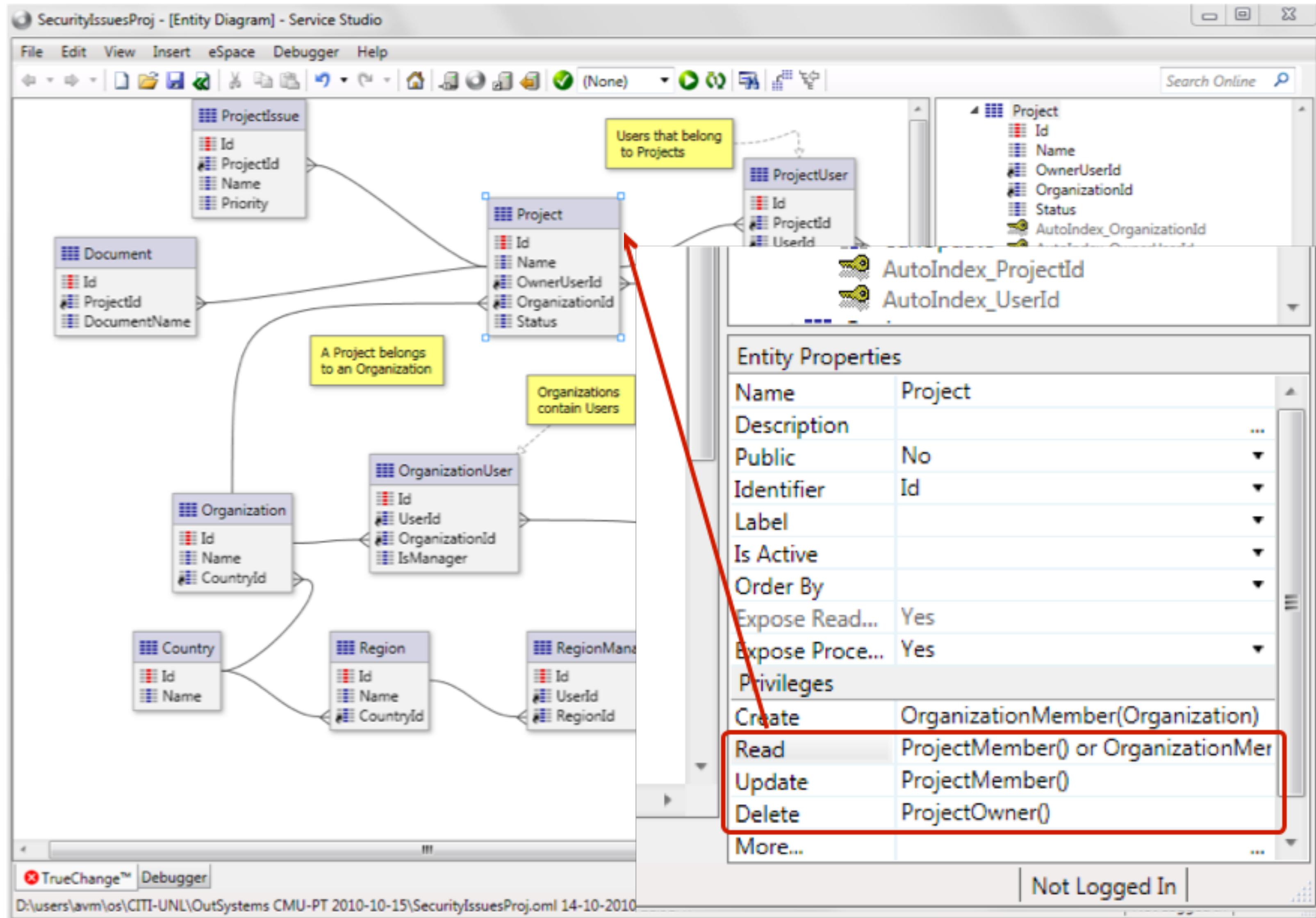
Luís Caires<sup>1</sup>, Jorge A. Pérez<sup>1</sup>, João C. Seco<sup>1</sup>, Hugo T. Vieira<sup>1</sup>, and Lúcio Ferrão<sup>2</sup>

<sup>1</sup> CITI and Departamento de Informática, Faculdade de Ciências e Tecnologia,  
Universidade Nova de Lisboa

<sup>2</sup> OutSystems SA

Data-centric multi-user systems, such as web applications, require flexible yet fine-grained data security mechanisms. Such mechanisms are usually enforced by a specially crafted security layer, which adds extra complexity and often leads to error prone coding, easily causing severe security breaches. In this paper, we introduce a programming language approach for enforcing access control policies to data in data-centric programs by static typing. Our development is based on the general concept of refinement type, but extended so as to address realistic and challenging scenarios of permission-based data security, in which policies dynamically depend on the database state, and flexible

# Model-Based Access Control

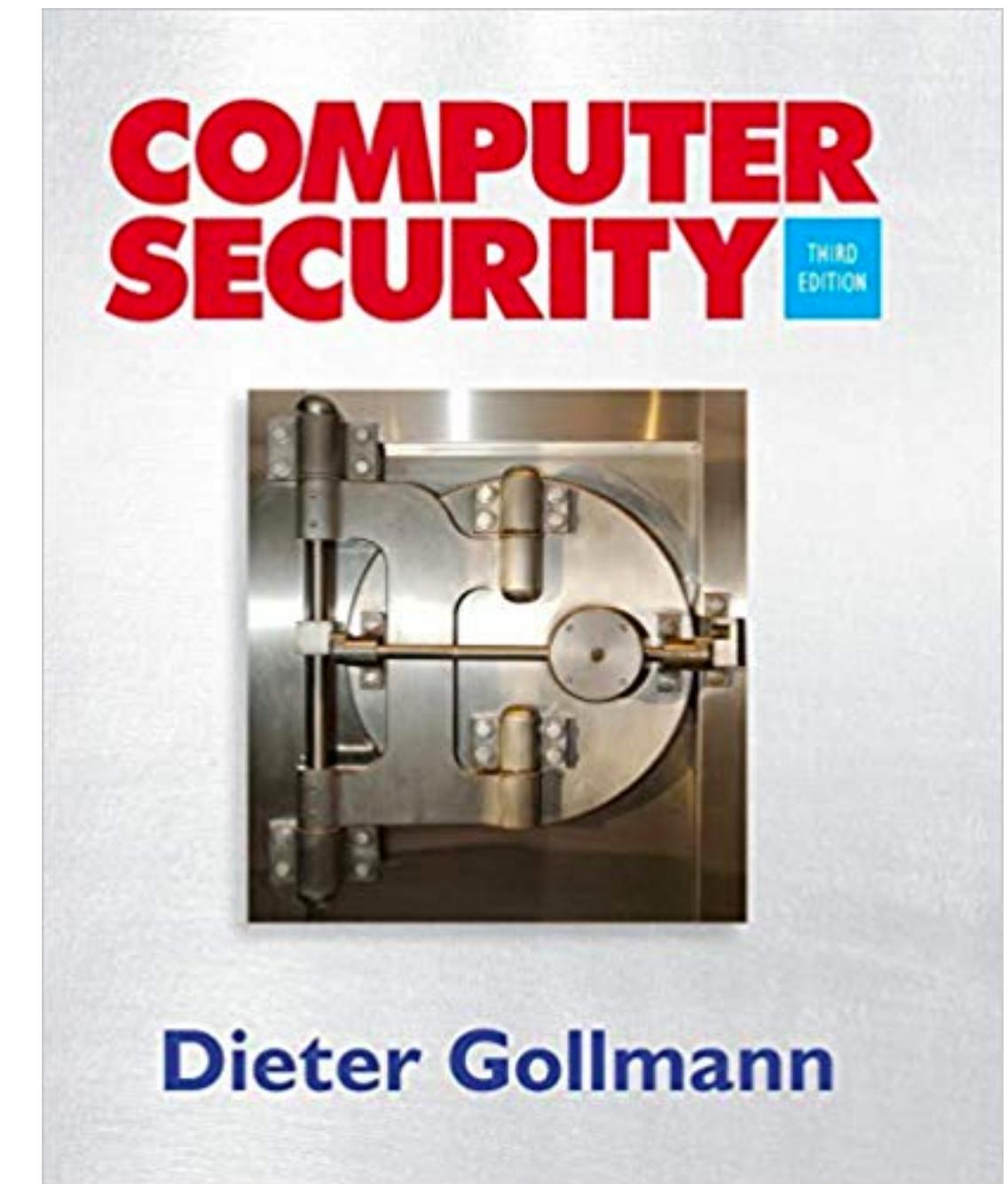


# Further Reading

Computer Security. Dieter Gollmann. 3rd edition. Wiley, 2011.

OWASP Testing Guide V4. Owasp foundation, 2016. <https://www.owasp.org/images/1/19/OTGv4.pdf>

- CIA triad: confidentiality, integrity, and availability (A1, A6)
- Authentication, authorization, non-repudiation (A1, A2, A6)
- Risk, threats, vulnerabilities, and attack vectors (A3, A6)
- Concept of trust and trustworthiness (A4)
- Threat and attacker modelling (A3, A5, B1)
  
- Identification and authentication (A2, B3)
- Authorization and access control models (B2, B4, B5)
- Defensive programming (C2, D1)
- Software security testing (A5, C2, D2)
  
- Secure design basic principles (B2, B4, C1)
- Security best practices and standards (B3, B4, B5, B6, C2)
- Techniques for preserving security across modules and trust maintenance (A4, B1, B6, D1, D2, D3)
  
- Web security model (B6)
- Session management, authentication (B3, C3)
- Web application vulnerabilities and defenses (A5, B1, C3, C4)
- Client-side security (C4, D3, D4)
- Server-side security tools (C4, D3, D5)



**Dieter Gollmann**

# Internet Applications Design and Implementation

## 2020 - 2021

### (Lecture 5 - Part 4 - Using Kotlin & Spring)

**MIEI - Integrated Master in Computer Science and Informatics  
Specialization block**

**João Costa Seco ([joao.seco@fct.unl.pt](mailto:joao.seco@fct.unl.pt))**

(with previous participations of Jácome Cunha ([jacome@fct.unl.pt](mailto:jacome@fct.unl.pt)) and João Leitão ([jc.leitao@fct.unl.pt](mailto:jc.leitao@fct.unl.pt)))



**FACULDADE DE  
CIÊNCIAS E TECNOLOGIA  
UNIVERSIDADE NOVA DE LISBOA**

# Using frameworks for security

- Frameworks such as Spring, with Spring Security project promote the reuse of (correct) code, good practices, and great number of base features.

## Spring Security 5.4.1



OVERVIEW

LEARN

Spring Security is a powerful and highly customizable authentication and access-control framework. It is the de-facto standard for securing Spring-based applications.

Spring Security is a framework that focuses on providing both authentication and authorization to Java applications. Like all Spring projects, the real power of Spring Security is found in how easily it can be extended to meet custom requirements

<https://spring.io/projects/spring-security>

# Using frameworks for security

---

- Frameworks such as Spring Security promote the reuse of (correct) code, good practices, and great number of base features.
  - HTTP BASIC authentication headers (an IETF RFC-based standard)
  - HTTP Digest authentication headers (an IETF RFC-based standard)
  - HTTP X.509 client certificate exchange (an IETF RFC-based standard)
  - LDAP (a very common approach to cross-platform authentication needs, especially in large environments)
  - Form-based authentication (for simple user interface needs)
  - OpenID authentication
  - Authentication based on pre-established request headers (such as Computer Associates Siteminder)
  - JA-SIG Central Authentication Service (otherwise known as CAS, which is a popular open source single sign-on system)
  - Transparent authentication context propagation for Remote Method Invocation (RMI) and HttpInvoker (a Spring remoting protocol)
  - Automatic “remember me” authentication (so you can tick a box to avoid re-authentication for a predetermined period of time)
  - Anonymous authentication (allowing every unauthenticated call to automatically assume a particular security identity)
  - Run-as authentication (which is useful if one call should proceed with a different security identity)
  - Java Authentication and Authorization Service (JAAS)
  - JEE container authentication (so you can still use Container Managed Authentication if desired)
  - Kerberos

# Including Spring Security



- By just including the dependency in the application, security is automatically enabled.

```
<dependency>
  <groupId>org.springframework.boot</groupId>
  <artifactId>spring-boot-starter-security</artifactId>
</dependency>
```

```
<dependency>
  <groupId>org.springframework.security</groupId>
  <artifactId>spring-security-test</artifactId>
  <scope>test</scope>
</dependency>
```

- Configuration is then possible by declaring basic access properties and basic user information.

<https://spring.io/guides/gs/securing-web/>

# Including Spring Security

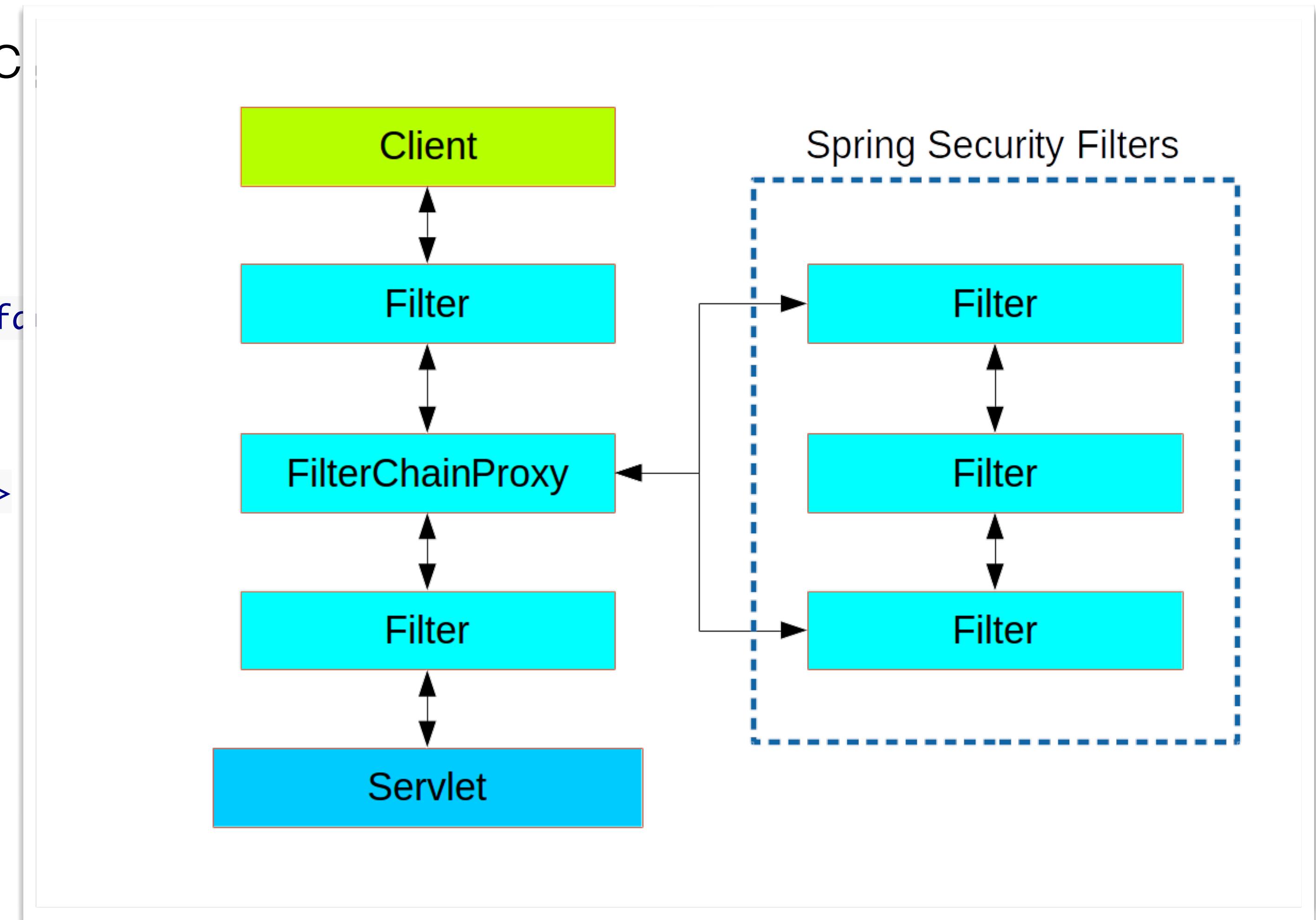


- By just including the dependency, everything is enabled.

```
<dependency>
  <groupId>org.springframework.boot</groupId>
  <artifactId>spring-boot-starter-security</artifactId>
</dependency>
```

```
<dependency>
  <groupId>org.springframework.security</groupId>
  <artifactId>spring-security-test</artifactId>
  <scope>test</scope>
</dependency>
```

- Configuration is then possible by declaring basic access properties and basic user information.



<https://spring.io/guides/gs/securing-web/>

<https://spring.io/guides/topics/spring-security-architecture>

# Including Spring Security



- By just including the dependency it is enabled.

```
<dependency>
    <groupId>org.springframework.boot</groupId>
    <artifactId>spring-boot-starter-security</artifactId>
</dependency>
```

```
<dependency>
    <groupId>org.springframework.security</groupId>
    <artifactId>spring-security-test</artifactId>
    <scope>test</scope>
</dependency>
```

- Configuration is then possible by declaring basic access properties and basic user information.

```
@Configuration
@EnableWebSecurity
class WebSecurityConfig : WebSecurityConfigurerAdapter() {
    @Throws(Exception::class)
    override fun configure(http: HttpSecurity) {
        http
            .authorizeRequests()
                .antMatchers("/").permitAll()
                .anyRequest().authenticated()
                .and()
            .formLogin()
                .permitAll()
                .and()
            .logout()
                .permitAll()
    }

    @Bean
    public override fun userDetailsService(): UserDetailsService {
        val user: UserDetails = User.withDefaultPasswordEncoder()
            .username("user")
            .password("password")
            .roles("USER")
            .build()
        return InMemoryUserDetailsManager(user)
    }
}
```

# Including Spring Security



- By just including the dependency it is enabled.

```
<dependency>
  <groupId>org.springframework.boot</groupId>
  <artifactId>spring-boot-starter-security</artifactId>
</dependency>
```

```
<dependency>
  <groupId>org.springframework.security</groupId>
  <artifactId>spring-security-test</artifactId>
  <scope>test</scope>
</dependency>
```

- Configuration is there by declaring basic application properties and basic user information.

```
@Configuration
@EnableWebSecurity
class WebSecurityConfig : WebSecurityConfigurerAdapter() {
    override fun configure(http: HttpSecurity) {
        http
            .authorizeRequests()
            .anyRequest().authenticated()
            .and()
            .formLogin()
            .username("user")
            .password("password")
            .and()
            .logout()
            .logoutUrl("/logout")
            .and()
            .rememberMe()
            .key("myapp")
    }

    override fun userDetailsService(): UserDetailsService {
        return InMemoryUserDetailsManager(
            listOf(
                User.builder()
                    .username("user")
                    .password(passwordEncoder.encode("password"))
                    .authorities("ROLE_USER")
                    .build()
            )
        )
    }

    private val passwordEncoder: PasswordEncoder = BCryptPasswordEncoder()
}
```

# Including Spring Security



- By just including the dependency, security is enabled.

```
<dependency>
  <groupId>org.springframework.boot</groupId>
  <artifactId>spring-boot-starter-security</artifactId>
</dependency>
```

```
<dependency>
  <groupId>org.springframework.security</groupId>
  <artifactId>spring-security-test</artifactId>
  <scope>test</scope>
</dependency>
```

- Configuration is then possible by declaring basic access properties and basic user information.

```
@Configuration
@EnableWebSecurity
class WebSecurityConfig : WebSecurityConfigurerAdapter() {
    override fun configure(http: HttpSecurity) {
        http
            .csrf().disable()
            .authorizeRequests()
                .antMatchers("/*").permitAll()
                .anyRequest().authenticated()
            .and().httpBasic()
    }

    override fun configure(auth: AuthenticationManagerBuilder) {
        auth.inMemoryAuthentication()
            .withUser("user")
            .password(BCryptPasswordEncoder().encode("password"))
            .authorities(emptyList())
        .and()
            .passwordEncoder(BCryptPasswordEncoder())
    }
}
```

<https://spring.io/guides/gs/securing-web/>

# Including Spring Security



- By just including the dependency, security is enabled.

```
<dependency>
    <groupId>org.springframework.boot</groupId>
    <artifactId>spring-boot-starter-security</artifactId>
    <version>2.3.2.RELEASE</version>
</dependency>
```

```
<dependency>
    <groupId>org.springframework.boot</groupId>
    <artifactId>spring-boot-starter-test</artifactId>
    <scope>test</scope>
</dependency>
```

- Configuration is done by declaring beans, properties and Java annotations, and security information.

The screenshot shows a terminal window titled "jcs — zsh — 80x24". The command entered was "http :8080/applications". The response is as follows:

```
jcs@Joaos-iMac ~ % http :8080/applications
HTTP/1.1 403
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Connection: keep-alive
Content-Type: application/json
Date: Mon, 19 Oct 2020 14:30:34 GMT
Expires: 0
Keep-Alive: timeout=60
Pragma: no-cache
Set-Cookie: JSESSIONID=2454FD5814FB3EEBF80E07CF1737C10D; Path=/; HttpOnly
Transfer-Encoding: chunked
X-Content-Type-Options: nosniff
X-Frame-Options: DENY
X-XSS-Protection: 1; mode=block

{
    "error": "Forbidden",
    "message": "",
    "path": "/applications",
    "status": 403,
    "timestamp": "2020-10-19T14:30:34.051+00:00"
}
```

<https://spring.io/guides/gs/securing-web/>

# Including Spring Security



- By just including `spring-boot-starter-security` the security is enabled.

```
<dependency>
    <groupId>org.springframework.boot</groupId>
    <artifactId>spring-boot-starter-security</artifactId>
    <version>2.3.3.RELEASE</version>
</dependency>

<dependency>
    <groupId>org.springframework.boot</groupId>
    <artifactId>spring-boot-starter-test</artifactId>
    <scope>test</scope>
</dependency>
```

- Configuration is done by declaring basic security properties and basic authentication information.

```
jcs@Joaos-iMac ~ % http :8080/applications --auth user:password
HTTP/1.1 200
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Connection: keep-alive
Content-Type: application/json
Date: Mon, 19 Oct 2020 14:57:40 GMT
Expires: 0
Keep-Alive: timeout=60
Pragma: no-cache
Set-Cookie: JSESSIONID=2361CEB5951A39C2967863030D2EBA48; Path=/; HttpOnly
Transfer-Encoding: chunked
X-Content-Type-Options: nosniff
X-Frame-Options: DENY
X-XSS-Protection: 1; mode=block
[]

jcs@Joaos-iMac ~ %
```

```
    ter() {
        gerBuilder) {
            ncode("password"))
        der()))
    }
}
```

<https://spring.io/guides/gs/securing-web/>



# Authentication - Simple starter code

- The default security setting provides that all requests are protected, a login form is created, RESTful interface for login/logout...

```
@Configuration  
@EnableWebSecurity  
public class SecurityConfig extends WebSecurityConfigurerAdapter {  
  
    @Autowired  
    public void configureGlobal(AuthenticationManagerBuilder auth) throws Exception {  
        auth  
            .inMemoryAuthentication()  
                .withUser("user").password("password").roles("USER");  
    }  
}
```

**Look into the documentation for the up-to-date API!!**

# Fundamental Concepts mapped to Spring Context



- Principal - Who is the entity behind a particular request

```
@RequestMapping("/messages/inbox")
public ModelAndView findMessagesForUser(@AuthenticationPrincipal CustomUser user) {

    // .. find messages for this user and return them ...
}
```

- Authentication: Certify that a given set of credentials identify one principal

```
@Autowired
public void configureGlobal(AuthenticationManagerBuilder auth) throws Exception {
    auth
        .jdbcAuthentication()
        .dataSource(dataSource)
        .withDefaultSchema()
        .withUser("user").password("password").roles("USER").and()
        .withUser("admin").password("password").roles("USER", "ADMIN");
}
```

**Look into the documentation for the up-to-date API!!**



# Linking to the application model

- Dynamic verification of user credentials is part of the application model

```
override fun configure(auth: AuthenticationManagerBuilder) {  
    auth.inMemoryAuthentication()  
        .withUser( username: "user")  
        .password(BCryptPasswordEncoder().encode( rawPassword: "password"))  
        .authorities(emptyList())  
        .and()  
        .passwordEncoder(BCryptPasswordEncoder())  
        .and()  
        .userDetailsService(customUserDetails)  
}
```

**Look into the documentation for the up-to-date API!!**

# Linking to the application model



- Dynamic verification of user credentials is part of the application model

```
override fun configure(auth: AuthenticationManagerBuilder) {
    auth.inMemoryAuthentication()
        .withUser("user")
            .password("password")
            .authorities(emptyList())
        .and()
        .passwordEncoder(BCryptPasswordEncoder())
        .and()
    .userDetailsService(customUserDetailsService)
}

@Service
class CustomUserDetailsService(
    val users: UserService
) : UserDetailsService {
    override fun loadUserByUsername(username: String?): UserDetails {
        username?.let { it: String ->
            val userDAO = users.findUser(it)
            if( userDAO.isPresent ) {
                return CustomUserDetails(userDAO.get().username, userDAO.get().password, mutableListOf())
            } else {
                throw UsernameNotFoundException(username)
            }
        }
        throw UsernameNotFoundException(username)
    }
}
```

**Look into the documentation for the up-to-date API!!**



# Security of Internet Applications

- Authorisation - Check if a given principal has rights to access a given piece of information

```
protected void configure(HttpSecurity http) throws Exception {  
    http  
        .authorizeRequests()  
            .antMatchers("/resources/**", "/signup", "/about").permitAll()  
            .antMatchers("/admin/**").hasRole("ADMIN")  
            .antMatchers("/db/**").access("hasRole('ROLE_ADMIN') and hasRole('ROLE_DBA')")  
            .anyRequest().authenticated()  
        .and()  
        // ...  
        .formLogin();  
}
```

org.springframework.security.web.authentication.switchuser

## Class SwitchUserFilter

java.lang.Object

org.springframework.web.filter.GenericFilterBean

org.springframework.security.web.authentication.switchuser.SwitchUserFilter

### All Implemented Interfaces:

javax.servlet.Filter, Aware, BeanNameAware, DisposableBean, InitializingBean, Ap

[http://docs.spring.io/autorepo/docs/spring-security/3.2.1.RELEASE/apidocs/  
org/springframework/security/web/authentication/switchuser/SwitchUserFilter.html](http://docs.spring.io/autorepo/docs/spring-security/3.2.1.RELEASE/apidocs/org/springframework/security/web/authentication/switchuser/SwitchUserFilter.html)

# Basic Spring Security Guarantees

There really isn't much to this configuration, but it does a lot. You can find a summary of the features below:

- Require authentication to every URL in your application
- Generate a login form for you
- Allow the user with the **Username** user and the **Password** password to authenticate with form based authentication
- Allow the user to logout
- [CSRF attack](#) prevention
- [Session Fixation](#) protection
- Security Header integration
  - [HTTP Strict Transport Security](#) for secure requests
  - [X-Content-Type-Options](#) integration
  - Cache Control (can be overridden later by your application to allow caching of your static resources)

**From Spring Security docs**

# Basic Spring Security Guarantees

- Security Header integration
  - [HTTP Strict Transport Security](#) for secure requests
  - [X-Content-Type-Options](#) integration
  - Cache Control (can be overridden later by your application to allow caching of your static resources)
  - [X-XSS-Protection](#) integration
  - X-Frame-Options integration to help prevent [Clickjacking](#)
- Integrate with the following Servlet API methods
  - [HttpServletRequest#getRemoteUser\(\)](#)
  - [HttpServletRequest.html#getUserPrincipal\(\)](#)
  - [HttpServletRequest.html#isUserInRole\(java.lang.String\)](#)
  - [HttpServletRequest.html#login\(java.lang.String, java.lang.String\)](#)
  - [HttpServletRequest.html#logout\(\)](#)

**From Spring Security docs**

## 6. Cross Site Request Forgery (CSRF)

This section discusses Spring Security's [Cross Site Request Forgery \(CSRF\)](#) support.

### 6.1. CSRF Attacks

Before we discuss how Spring Security can protect applications from CSRF attacks, we will explain what a CSRF attack is. Let's take a look at a concrete example to get a better understanding.

Assume that your bank's website provides a form that allows transferring money from the currently logged in user to another bank account. For example, the HTTP request might look like:

```
POST /transfer HTTP/1.1
Host: bank.example.com
Cookie: JSESSIONID=randomid; Domain=bank.example.com; Secure; HttpOnly
Content-Type: application/x-www-form-urlencoded

amount=100.00&routingNumber=1234&account=9876
```

**From Spring Security docs**

# CSRF - token issued by the server / recognised by the same server

---

- Template example...

```
<div th:if="#{httpServletRequest.remoteUser}!=null">
    <label>User:&nbsp;</label><span th:text="#{httpServletRequest.remoteUser}"></span>
    <form style="display:inline-block" th:action="@{/logout}" method="post">
        <input type="submit" value="Sign Out"/>
    </form>
</div>

<div th:if="#{httpServletRequest.remoteUser} == null" >
    <form th:action="@{/}" method="post">
        <label> User : <input type="text" name="username"/> </label>
        <label> Password: <input type="password" name="password"/> </label>
        <input type="hidden" name="${_csrf.parameterName}" value="${_csrf.token}"/>
        <input type="submit" value="Sign In"/>
    </form>
</div>
```

# CSRF - token issued by the server / recognised by the same server

- Actual page example

```
---  
  ▼ <div class="container">  
    ▼ <div>  
      ▼ <form method="post" action="/">  
        ▼ <label>  
          " User : "  
          ▶ <input type="text" name="username">  
        </label>  
        ▼ <label>  
          " Password: "  
          ▶ <input type="password" name="password">  
        </label>  
          ▶ <input type="hidden" name="${_csrf.parameterName}" value="${_csrf.token}">  
          ▶ <input type="submit" value="Sign In">  
          ▶ <input type="hidden" name="_csrf" value="f067a25f-c6f5-4de0-b6ad-ea7416986b22">  
        </form>  
      </div>  
    </div>  
  </div>
```

# Internet Applications Design and Implementation

2020 - 2021

(Lecture 5 - Part 5 - Model-based Authorisation in Spring)

**MIEI - Integrated Master in Computer Science and Informatics  
Specialization block**

**João Costa Seco ([joao.seco@fct.unl.pt](mailto:joao.seco@fct.unl.pt))**

(with previous participations of Jácome Cunha ([jacome@fct.unl.pt](mailto:jacome@fct.unl.pt)) and João Leitão ([jc.leitao@fct.unl.pt](mailto:jc.leitao@fct.unl.pt)))



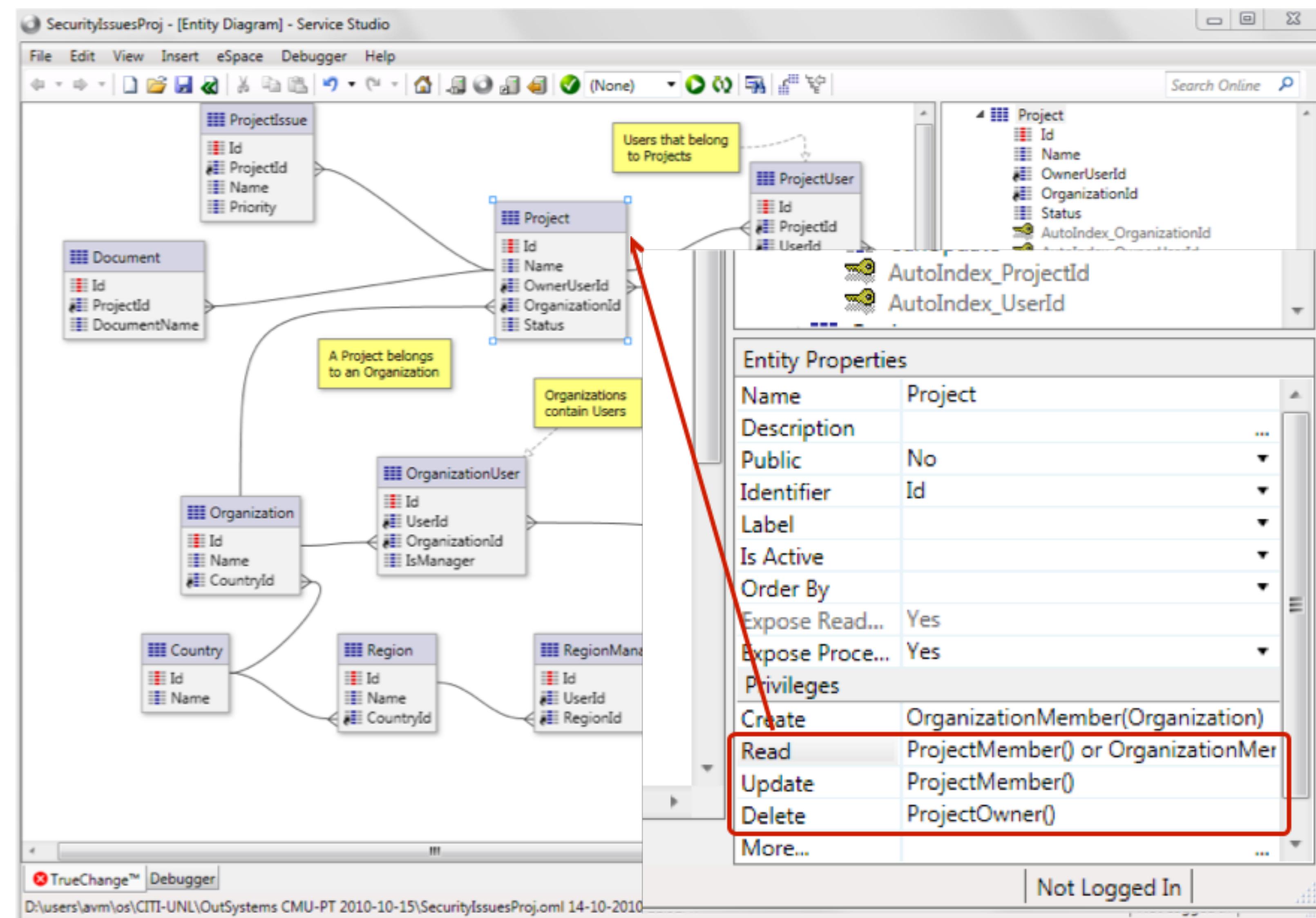
FACULDADE DE  
CIÊNCIAS E TECNOLOGIA  
UNIVERSIDADE NOVA DE LISBOA

# Model Based Access Control

---

- Security conditions are many times hidden in query filters and program conditions. They are very difficult to maintain/modify/get right.
- Developer defined roles usually depend on the state of the application. (e.g. ModeratorOf(...)). Role-based models ignore this.
- Authorisations usually depend on the state of the target entity (status == submitted)
- Capabilities defined by the developer extend read/write/delete (not hardwired to the basic programming elements)

# Model Based Access Control



# Model Based Access Control - Spring?

```
protected void configure(HttpSecurity http) throws Exception {  
    http  
        .authorizeRequests()  
            .anyRequest().authenticated()  
            .and()  
            .antMatchers("/admin/hotels/{id}")  
            .access(id => managerOfHotel(id))  
            .access(id => hotels.findOne(id).isApproved())  
        //...  
}
```

**Not really Spring... how could we do this?**

# Security and Frameworks (Spring)

---

- Web Development Frameworks provide basic mechanisms like:
  - Authentication
    - username, password, authorities (roles)
  - Authorization
    - hasRole, hasPermission

# Role Based Access Control

---

- Application level pattern implemented on top of basic authentication mechanisms
  - Principal (The authenticated user)
  - Role (Job functions a user may have)
  - Capabilities (Systems operations a role may be associated with)
- Allows the dynamic assignment of capabilities to users
- Allows sophisticated assignment and delegation mechanisms (e.g. roles assigned in name of another principal, or by a limited time).

# Model based security

- Security conditions are part of the application level
- Authentication and authorisation are system level

```
// POST /hotels/{id}          - update the hotel with identifier {id}
@RequestMapping(value="{id}", method=RequestMethod.POST)
@PreAuthorize("hasRole('{ROLE_ADMIN,ROLE_MANAGER}')")
public String editSave(@PathVariable("id") long id, Hotel hotel,
                      Model model, Principal principal) {
    if( principal.getName().equals(hotel.getManager().getName()) ) {
        hotel.setTimestamp(new Date());
        hotels.save(hotel);
        return "redirect:/hotels/"+id;
    } else
        throw new AccessDeniedException("Cannot edit hotel "+hotel.getName());
}
```

- Security conditions are many times encoded into application logic (if-else-throw statements) and where conditions in queries.

# Spring Security implementation

- Basic spring security is based on SPEL expressions using principal information and parameters...

```
// POST /hotels/{id}      - update the hotel with identifier {id}
@RequestMapping(value="{id}", method=RequestMethod.POST)
@PreAuthorize("hasRole('ROLE_ADMIN', 'ROLE_MANAGER') "
    + "and principal.name == #hotel.manager.name")
public String editSave(@PathVariable("id") long id, Hotel hotel,
    Model model, Principal principal) {
    hotel.setTimestamp(new Date());
    hotels.save(hotel);
    return "redirect:/hotels/" + id;
}
```

- Rule: “a hotel can be edited by its manager or an administrator”
  - Problem: `#hotel.manager.name` is not loaded !!

# Pros & Cons

---

- + May use model information
- + Provides row-level authorisation on resources
- - Has limited access to the model (database)
- - Bad reuse of condition expressions
- - Runtime parsing and execution of security expressions

# Policies or security rules

---

- Isolate the implementation of security rules in services with full access to the model.

```
@Component("mySecurityService")
public class MySecurityService {

    @Autowired
    HotelRepository hotels;

    public boolean canEditHotel(User user, long hotelId) {
        Hotel hotel = hotels.findOne(hotelId);

        return hotel != null && hotel.getManager() != null &&
               user.getUsername().equals(hotel.getManager().getName());
    }
}
```

- Model access, Good reuse, auditing of rules.

# Policies or security rules in “services”

---

- Isolate the implementation of security rules in services with full access to the model.

```
// POST /hotels/{id}      - update the hotel with identifier {id}
@RequestMapping(value="{id}", method=RequestMethod.POST)
@PreAuthorize("hasRole({'ROLE_ADMIN'}) or "
              + "@mySecurityService.canEditHotel(principal,#id)")
public String editSave(@PathVariable("id") long id, Hotel hotel,
                      Model model, Principal principal) {
    hotel.setTimestamp(new Date());
    hotels.save(hotel);
    return "redirect:/hotels/"+id;
}
```

- Model access, Good reuse, auditing of rules.

# Capabilities encoded in “annotations”

---

- Statically identify capabilities and associated rules in annotations, associated to controllers...

```
// POST /hotels/{id}          - update the hotel with identifier {id}
@RequestMapping(value="{id}", method=RequestMethod.POST)
@AllowedForEditHotel
public String editSave(@PathVariable("id") long id, Hotel hotel, Model model) {
    hotel.setTimestamp(new Date());
    hotels.save(hotel);
    return "redirect:/hotels/"+id;
}
```

# Capabilities encoded in “annotations”

```
@Target({ElementType.METHOD, ElementType.TYPE})
@Retention(RetentionPolicy.RUNTIME)
@Inherited
@Documented
@PreAuthorize(AllowedForHotelCreation.Condition)
public @interface AllowedForHotelCreation {
    String Condition = "hasRole('ROLE_ADMIN')";
}

@Target({ElementType.METHOD, ElementType.TYPE})
@Retention(RetentionPolicy.RUNTIME)
@Inherited
@Documented
@PreAuthorize(AllowedForEditHotel.Condition)
public @interface AllowedForEditHotel {
    String Condition = "@mySecurityService.canEditHotel(principal,#id) or "
                      + AllowedForHotelCreation.Condition;
}
```

<http://blog.novoj.net/2012/03/27/combining-custom-annotations-for-secluding-methods-with-spring-security/>

# View authorisations

- Authorization expressions can be also used in views (with an awkward syntax, yes...)

```
<div class="container">
    <h1>Hotel <span th:text="${hotel.name}"></span></h1>
    <p th:text="${hotel.timestamp}"></p>

    <h2>Rooms</h2>
    <ul th:each="room : ${rooms}">
        <li th:text="${room.name} + ' ' + ${room.type.description}"></li>
    </ul>

    <div sec:authorize="#${authorization.expression(T(booking.security.AllowedForEditHotel).Condition2)}">
        <p><a th:href="@{/hotels/${hotel.id}/edit}">Edit</a></p>
    </div>
    <div sec:authorize="#${authorization.expression(T(booking.security.AllowedForHotelCreation).Condition)}">
        <p><a href="/hotels/new">Add a new hotel</a></p>
    </div>
    <p><a href="/hotels">List all hotels</a></p>
</div>
```

- Binding is sometimes different and has to be adapted :(

```
String Condition = "@mySecurityService.canEditHotel(principal,#id) or "
                + AllowedForHotelCreation.Condition;
String Condition2 = "@mySecurityService.canEditHotel(principal,#vars.hotel.id) or "
                + AllowedForHotelCreation.Condition;
```

# Pros & Cons

---

- + May use model information
- + Provides row-level authorisation on resources
- + Has full access to the model (database)
- + Good reuse of condition expressions (in services)
- - Runtime parsing and execution of security expressions  
(only better using static verification of code)

# Further Reading

---

Computer Security. Dieter Gollmann. 3rd edition. Wiley, 2011.

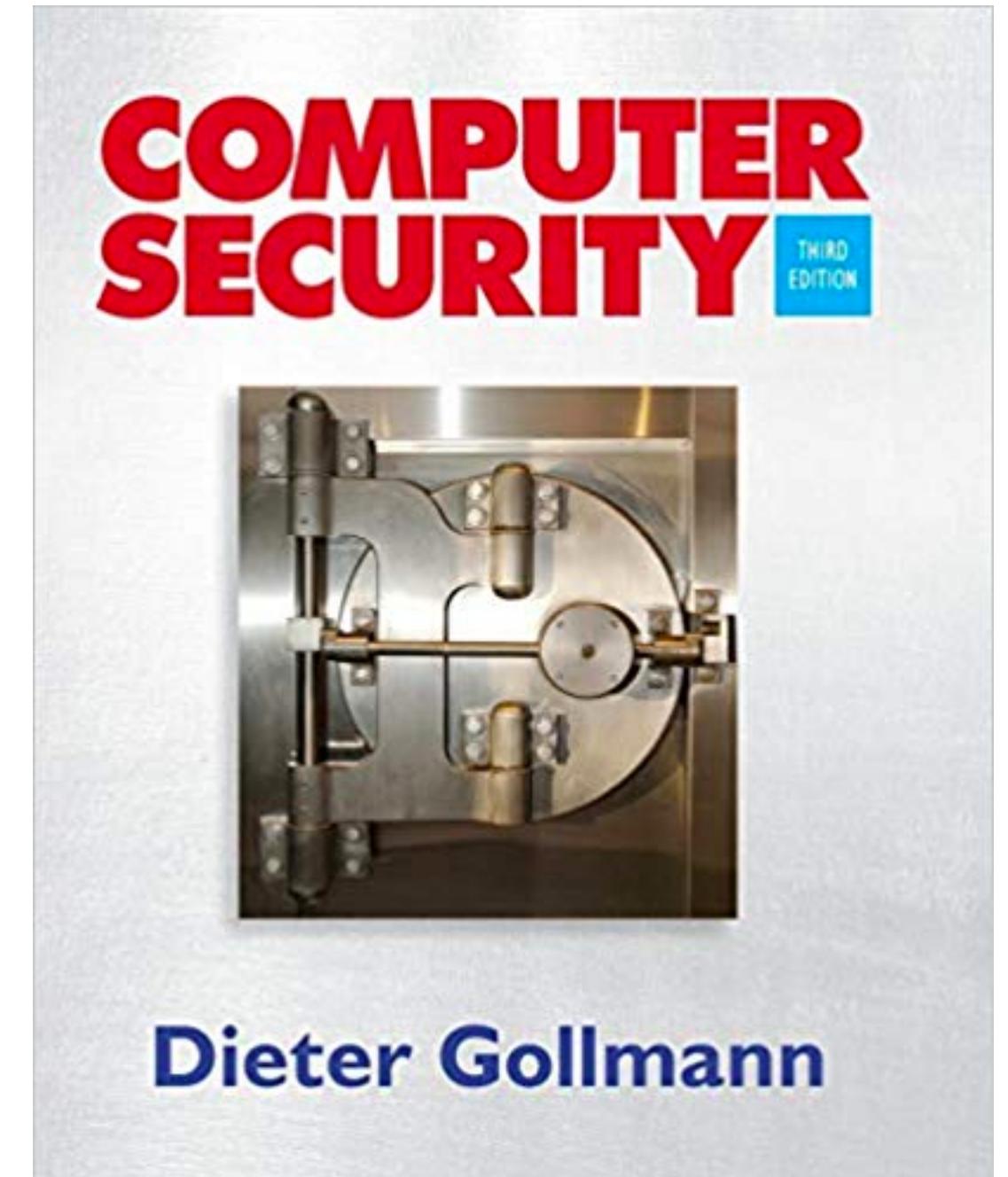
OWASP Testing Guide V4. Owasp foundation, 2016.

<https://www.owasp.org/images/1/19/OTGv4.pdf>

Blogs:

<https://heimdalsecurity.com/blog/best-internet-security-blogs/>

<https://www.schneier.com>



**OWASP**  
Open Web Application  
Security Project

# Internet Applications Design and Implementation

## 2020 - 2021

### (Lecture 6 - Session and Token based Security)

**MIEI - Integrated Master in Computer Science and Informatics  
Specialization block**

**João Costa Seco ([joao.seco@fct.unl.pt](mailto:joao.seco@fct.unl.pt))**

(with previous participations of Jácome Cunha ([jacome@fct.unl.pt](mailto:jacome@fct.unl.pt)) and João Leitão ([jc.leitao@fct.unl.pt](mailto:jc.leitao@fct.unl.pt)))



**FACULDADE DE  
CIÊNCIAS E TECNOLOGIA  
UNIVERSIDADE NOVA DE LISBOA**

# Overview: HTTP Authentication (Basic and Digest)

---

- Credentials (username/password) are repeated on each request
  - All requests are vulnerable to attacks (instead of only the login request)
  - Basic: username/password are passed in clear text and can be captured
  - Digest: digests can also be captured and guessed by brute force attacks
- Kind of ok under HTTPS, but...
  - Must have a centralised authority to control and manage principal capabilities
  - Does not support “logout” mechanisms (credentials are always valid)

# Overview: Sessions to implement security

---

- Stateless APIs are good
- but not so good for:
  - ephemeral or distributed authentication,
  - capability based authorisation models
  - protocol management,
  - user preferences (in webapps)
- ...
- Hence, let's implement session management

# Outline

---

- Sessions and cookies
- Token based authentication
- JSON Web Token (JWT)
- OAuth2

# Internet Applications Design and Implementation

2020 - 2021

(Lecture 6 - Part 1 - Sessions and Cookies)

**MIEI - Integrated Master in Computer Science and Informatics  
Specialization block**

**João Costa Seco ([joao.seco@fct.unl.pt](mailto:joao.seco@fct.unl.pt))**

(with previous participations of Jácome Cunha ([jacome@fct.unl.pt](mailto:jacome@fct.unl.pt)) and João Leitão ([jc.leitao@fct.unl.pt](mailto:jc.leitao@fct.unl.pt)))



FACULDADE DE  
CIÊNCIAS E TECNOLOGIA  
UNIVERSIDADE NOVA DE LISBOA

# Basic support for sessions, HTTP cookies

---

- Basic support to represent stateful information **on the client side**
- Designed to allow websites to remember stateful information about a session
- Shopping carts, authentication info, browser activity, search criteria, etc.
- Source of many security vulnerabilities, attacks and tracking of user activity
- Managed by client and server alike
  - Basically a string managed as a key/value store, can contain cyphered values

<https://developer.mozilla.org/en-US/docs/Web/HTTP/Session>

<https://developer.mozilla.org/en-US/docs/Web/API/Document/cookie>

# Cookies can be read and written in Spring

---

- In Spring the annotation `@CookieValue` is used to retrieve a value from the HTTP cookie and map the value to a parameter.

```
@GetMapping("/applications/")
fun getAll(
    @CookieValue (value="filter", defaultValue = "") filter:String
): List<ApplicationDTO> =
    applications.getAll(filter).map { ApplicationDTO(it) }
```

- Without a declared default value, an exception will be thrown (`java.lang.IllegalStateException`) if the cookie in the request does not contain the key “`filter`”.

# Cookies can be read and written in Spring

---

- To set the value of a cookie in SpringBoot, object `HttpServletResponse` must be added a new cookie value.

```
@PostMapping("/sudents/{id}/applications")
@ResponseStatus(HttpStatus.CREATED)
fun create2(@PathVariable student_id:String,
            @RequestBody @Valid anApplication:ApplicationDTO,
            response: HttpServletResponse) {
    val student = students.get(student_id)
    val id = applications.create(anApplication.toDAO(student))
    val cookie = Cookie("current_application", "id");
    response.addCookie(cookie);
}
```

- Disclaimer: this is just a sample on how to use cookies in Spring not a recommendation that you should do so...

# Sessions

---

- To have necessary stateful information in a stateless world
- Basic support to represent stateful information **on the server side**
- A session is a sequence of network HTTP requests and responses associated to the same principal. A session creates the opportunity to create a common context to the set of interactions between parties.
- From the first interaction, a session ID (or token) is established, even for anonymous users.
- This session token and/or identifier is used on the server side for a number of purposes.

<https://www.ietf.org/rfc/rfc2616.txt>

[https://cheatsheetseries.owasp.org/cheatsheets/Session\\_Management\\_Cheat\\_Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html)

<https://developer.mozilla.org/en-US/docs/Web/HTTP/Session>

# Session management in Spring

- Spring controls how a session is created and how Spring Security will handle it.
  - **always**: a session will always be created if one doesn't already exist
  - **ifRequired**: a session will be created only if required (default)
  - **never**: the framework will never create a session itself but it will use one if it already exists
  - **stateless**: no session will be created or used by Spring Security

```
override fun configure(http: HttpSecurity) {  
    http.csrf().disable()  
        .authorizeRequests()  
        .anyRequest().authenticated()  
        .and().sessionManagement().sessionCreationPolicy(SessionCreationPolicy.IF_REQUIRED)  
}
```

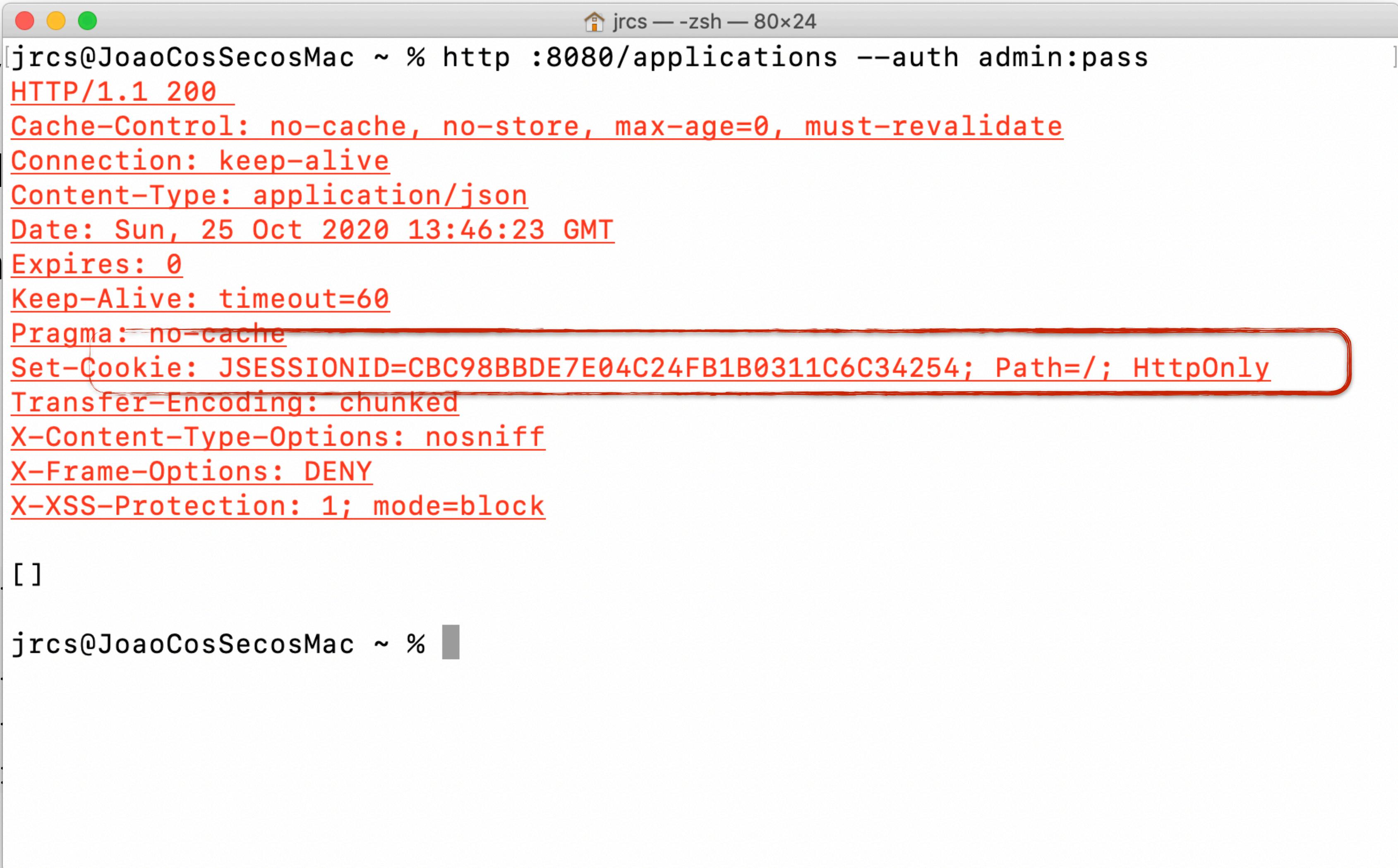
<https://www.baeldung.com/spring-security-session>

<https://docs.spring.io/spring-security/site/docs/5.4.1-SNAPSHOT/reference/html5/>

# Session management in Spring

- Spring controls how it.
  - **always:** a session will
  - **ifRequired:** a session
  - **never:** the framework
  - **stateless:** no session

```
override fun configure(http: HttpSecurity) {
    http.csrf().disable()
        .authorizeRequests()
        .anyRequest().authenticated()
        .and().sessionManagement()
}
```



```
jrcs@JoaoCosSecosMac ~ % http :8080/applications --auth admin:pass
HTTP/1.1 200
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Connection: keep-alive
Content-Type: application/json
Date: Sun, 25 Oct 2020 13:46:23 GMT
Expires: 0
Keep-Alive: timeout=60
Pragma: no-cache
Set-Cookie: JSESSIONID=CBC98BBDE7E04C24FB1B0311C6C34254; Path=/; HttpOnly
Transfer-Encoding: chunked
X-Content-Type-Options: nosniff
X-Frame-Options: DENY
X-XSS-Protection: 1; mode=block

[]
```

<https://www.baeldung.com/spring-security-session>

<https://docs.spring.io/spring-security/site/docs/5.4.1-SNAPSHOT/reference/html5/>

# Session management in Spring

- Spring controls how a session is created and how Spring Security will handle it.
  - **always**: a session will always be created if one doesn't already exist
  - **ifRequired**: a session will be created only if required (default)
  - **never**: the framework will never create a session itself but it will use one if it already exists
  - **stateless**: no session will be created or used by Spring Security

```
override fun configure(http: HttpSecurity) {  
    http.csrf().disable()  
        .authorizeRequests()  
        .anyRequest().authenticated()  
        .and().sessionManagement().sessionCreationPolicy(SessionCreationPolicy.STATELESS)  
}
```

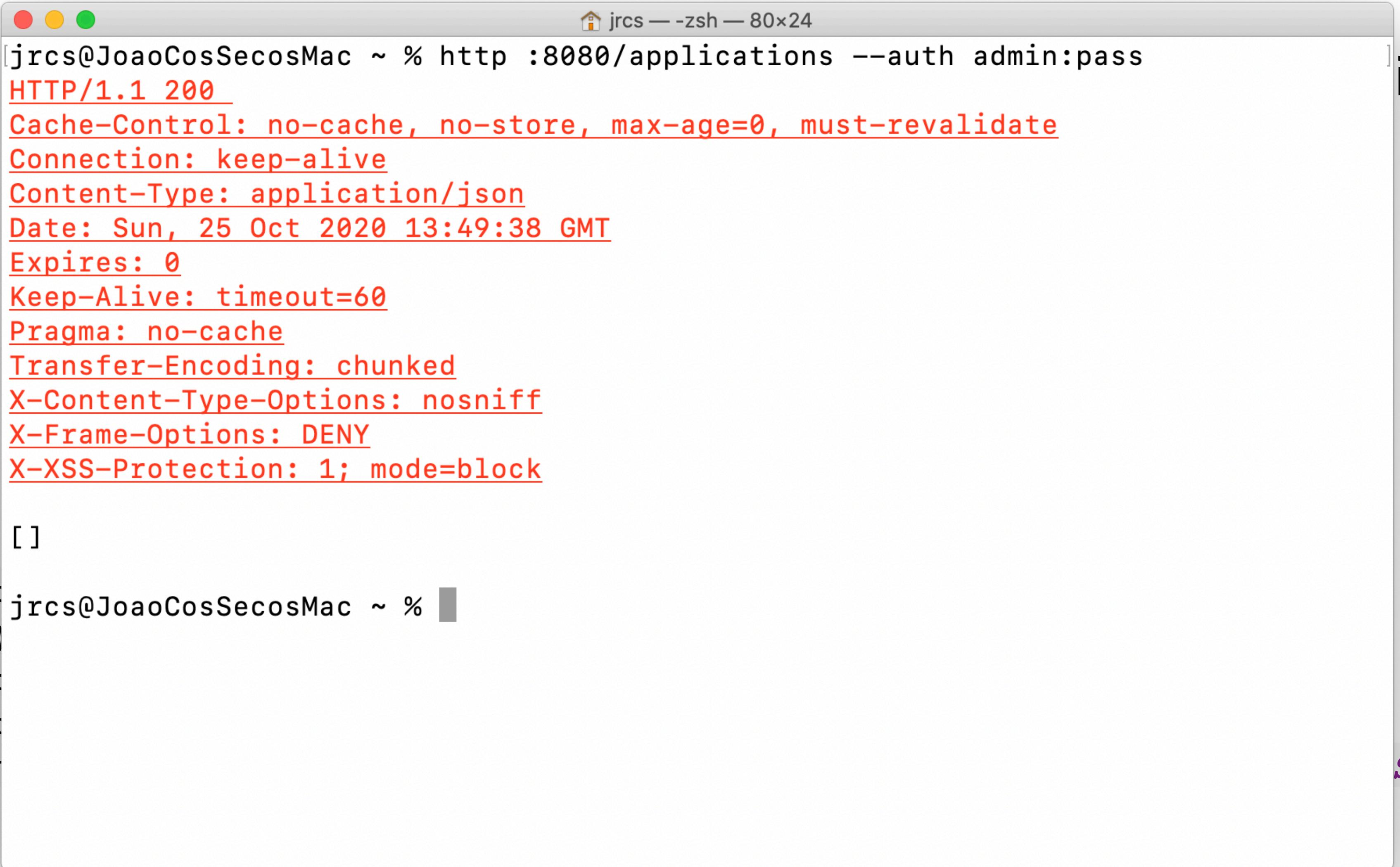
<https://www.baeldung.com/spring-security-session>

<https://docs.spring.io/spring-security/site/docs/5.4.1-SNAPSHOT/reference/html5/>

# Session management in Spring

- Spring controls how it.
  - **always**: a session will
  - **ifRequired**: a session
  - **never**: the framework
  - **stateless**: no session

```
override fun configure(ht  
    http.csrf().disable()  
        .authorizeRequest()  
        .anyRequest().aut  
        .and().sessionManag  
    }
```



A terminal window titled "jrcs — zsh — 80x24" is displayed. The command entered is "http :8080/applications --auth admin:pass". The output shows the following HTTP response headers:

```
[jrcs@JoaoCosSecosMac ~ % http :8080/applications --auth admin:pass
HTTP/1.1 200
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Connection: keep-alive
Content-Type: application/json
Date: Sun, 25 Oct 2020 13:49:38 GMT
Expires: 0
Keep-Alive: timeout=60
Pragma: no-cache
Transfer-Encoding: chunked
X-Content-Type-Options: nosniff
X-Frame-Options: DENY
X-XSS-Protection: 1; mode=block

[]
```

Below the terminal window, a portion of Java code is shown:

```
jrcs@JoaoCosSecosMac ~ %
```

<https://www.baeldung.com/spring-security-session>

<https://docs.spring.io/spring-security/site/docs/5.4.1-SNAPSHOT/reference/html5/>

# Session management

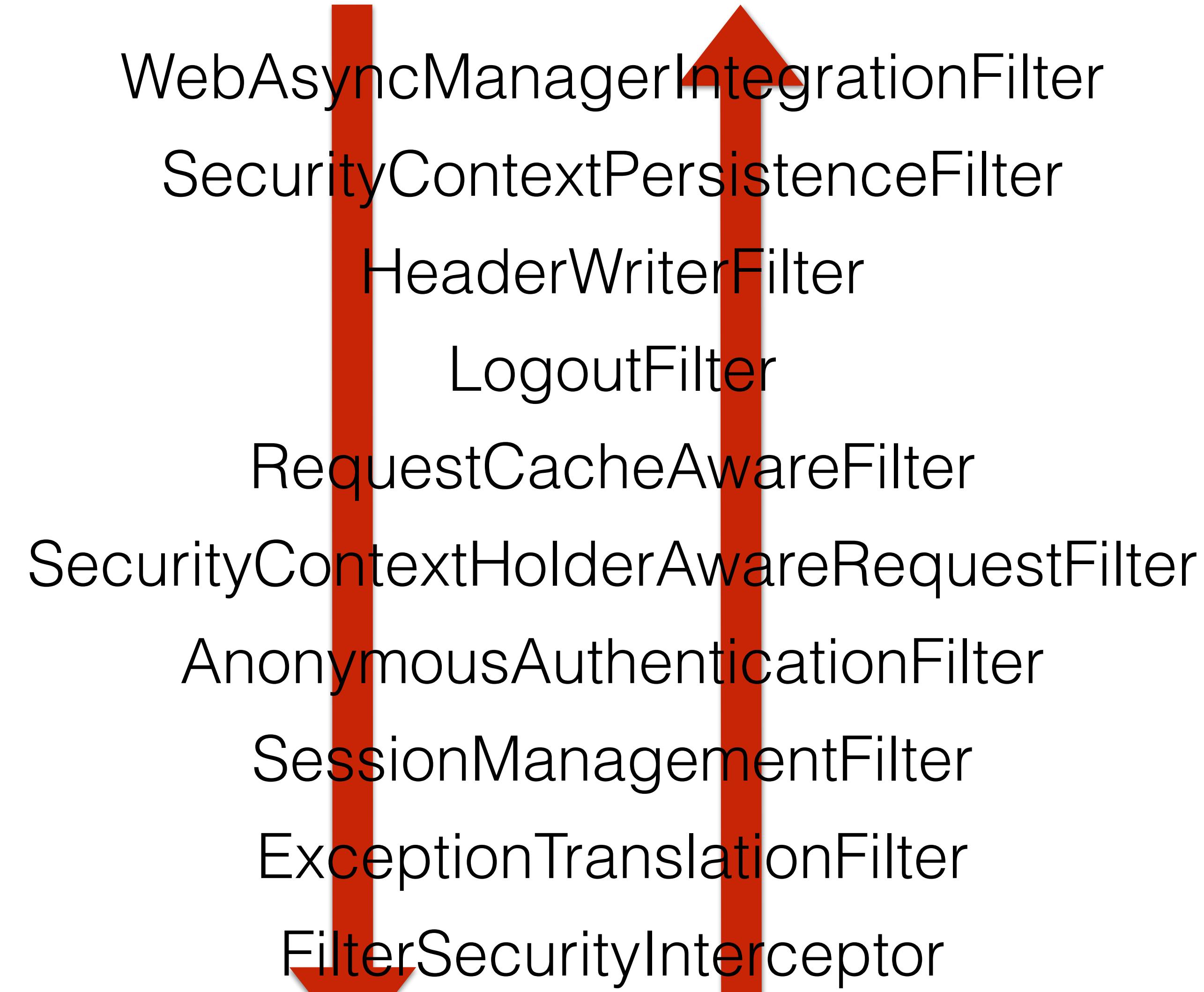
---

- Spring Security installs a filter that handles sessions in the Security Context (`SecurityContextPersistenceFilter`).
- The session can be managed using the bean (`HttpSessionSecurityContextRepository`) that uses HTTP Session as storage.
- For the STATELESS attribute (`NullSecurityContextRepository`) is used
- Sessions can be made persistent automatically by means of jdbc, or redis

```
<dependency>
    <groupId>org.springframework.boot</groupId>
    <artifactId>spring-boot-starter-data-redis</artifactId>
</dependency>
<dependency>
    <groupId>org.springframework.session</groupId>
    <artifactId>spring-session-data-redis</artifactId>
</dependency>
```

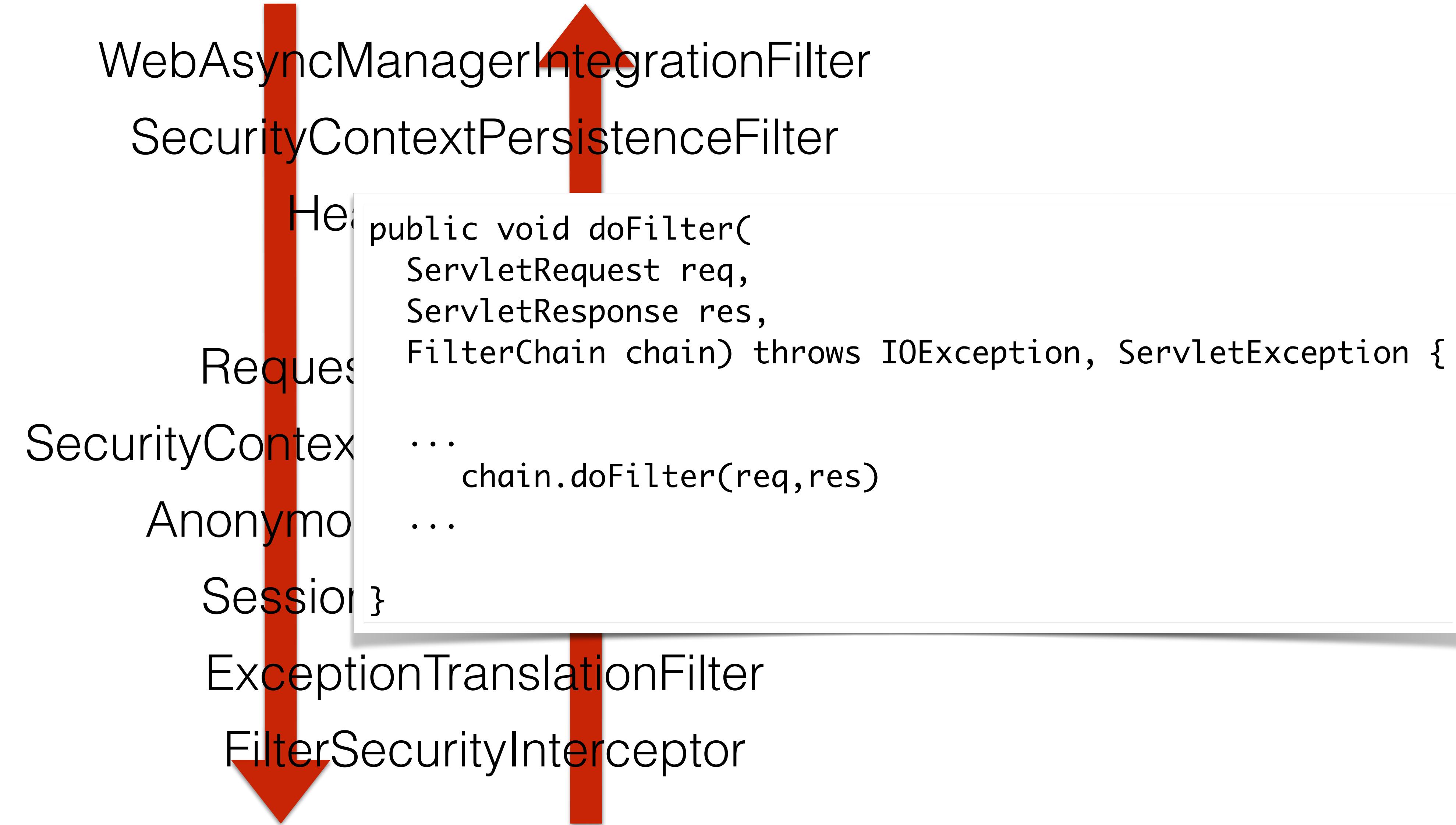


# Spring Security Filters





# Spring Security Filters



# Working With the Session

- Spring declares and handles session automatically through beans. A bean with scope “session” is created when the session is first created and linked to the lifecycle of the HttpSession object.

```
@Component  
@Scope("session", proxyMode = ScopedProxyMode.TARGET_CLASS)  
class SessionInfo(var numberOfGets:Int = 0, var numberOfPosts:Int = 0)
```

- This bean can then be used in other beans, for instance, a controller.

```
@RestController  
class ApplicationController(val applications: ApplicationService): ApplicationAPI {  
  
    @Autowired lateinit var info: SessionInfo;  
  
    override fun getAll(): List<ApplicationDTO> {  
        print(info.numberOfGets++)  
        return applications.getAll().map { ApplicationDTO(it) }  
    }  
}
```

...

<https://www.baeldung.com/spring-security-session>

# Working With the Session

- Spring declares and handles session automatically through beans. A bean with scope “session” is created when the session is first created and linked to the lifecycle of the HttpSession object.

```
@Component  
@Scope("session", proxyMode = ScopedProxyMode.TARGET_CLASS)  
class SessionInfo(var numberOfGets:Int = 0, var numberOfPosts:Int = 0)
```

- This bean can then be used in other beans, for instance, a controller.

```
@RestController  
class ApplicationController(val applications: ApplicationService): ApplicationAPI {  
  
    @Autowired lateinit var info: SessionInfo;  
  
    override fun getAll(session:HttpSession): List<ApplicationDTO> {  
        var info = session.getAttribute(SessionInfo) as SessionInfo;  
        session.setAttribute(SessionInfo, SessionInfo(info.numberOfGets+1, info.numberOfPosts))  
        return applications.getAll().map { ApplicationDTO(it) }  
    }  
}
```

<https://www.baeldung.com/spring-security-session>

# Internet Applications Design and Implementation

2020 - 2021

(Lecture 6 - Part 2 - Token-based Authentication - JWT)

**MIEI - Integrated Master in Computer Science and Informatics  
Specialization block**

**João Costa Seco ([joao.seco@fct.unl.pt](mailto:joao.seco@fct.unl.pt))**

(with previous participations of Jácome Cunha ([jacome@fct.unl.pt](mailto:jacome@fct.unl.pt)) and João Leitão ([jc.leitao@fct.unl.pt](mailto:jc.leitao@fct.unl.pt)))



FACULDADE DE  
CIÊNCIAS E TECNOLOGIA  
UNIVERSIDADE NOVA DE LISBOA

# HTTP Authentication modes

- Basic Authentication
  - username/password in the header of requests using Base64 encoding
- Digest Authentication
  - has of username/password in the header of requests (MD5 hashing with nonce)
- OAuth Token-based authentication and JWT
  - signed bearer token that allows interactions between independent authorisation and resource servers

<https://spring.io/guides/tutorials/spring-boot-oauth2/>

The image shows a screenshot of the JSON Web Token (JWT) RFC document. At the top right, it displays the document's metadata: Internet Engineering Task Force (IETF), Request for Comments: 7519, Category: Standards Track, ISSN: 2070-1721, and the authors: M. Jones (Microsoft), J. Bradley (Ping Identity), and N. Sakimura (NRI), dated May 2015. Below this, the title "JSON Web Token (JWT)" is centered. Under the title, there is an "Abstract" section which defines JWT as a compact, URL-safe means of representing claims to be transferred between two parties. It describes how claims are encoded as a JSON object and used in various structures like JWS or JWE. Following the abstract, there is a "Status of This Memo" section stating it is an Internet Standards Track document. A detailed description of the document's purpose and status is provided, mentioning its approval by the Internet Engineering Steering Group (IESG). At the bottom, there is a note about the current status and feedback information, with a link to the RFC editor.

Internet Engineering Task Force (IETF)  
Request for Comments: 7519  
Category: Standards Track  
ISSN: 2070-1721

M. Jones  
Microsoft  
J. Bradley  
Ping Identity  
N. Sakimura  
NRI  
May 2015

**JSON Web Token (JWT)**

**Abstract**

JSON Web Token (JWT) is a compact, URL-safe means of representing claims to be transferred between two parties. The claims in a JWT are encoded as a JSON object that is used as the payload of a JSON Web Signature (JWS) structure or as the plaintext of a JSON Web Encryption (JWE) structure, enabling the claims to be digitally signed or integrity protected with a Message Authentication Code (MAC) and/or encrypted.

**Status of This Memo**

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in [Section 2 of RFC 5741](#).

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at <http://www.rfc-editor.org/info/rfc7519>.

# Token-based authentication

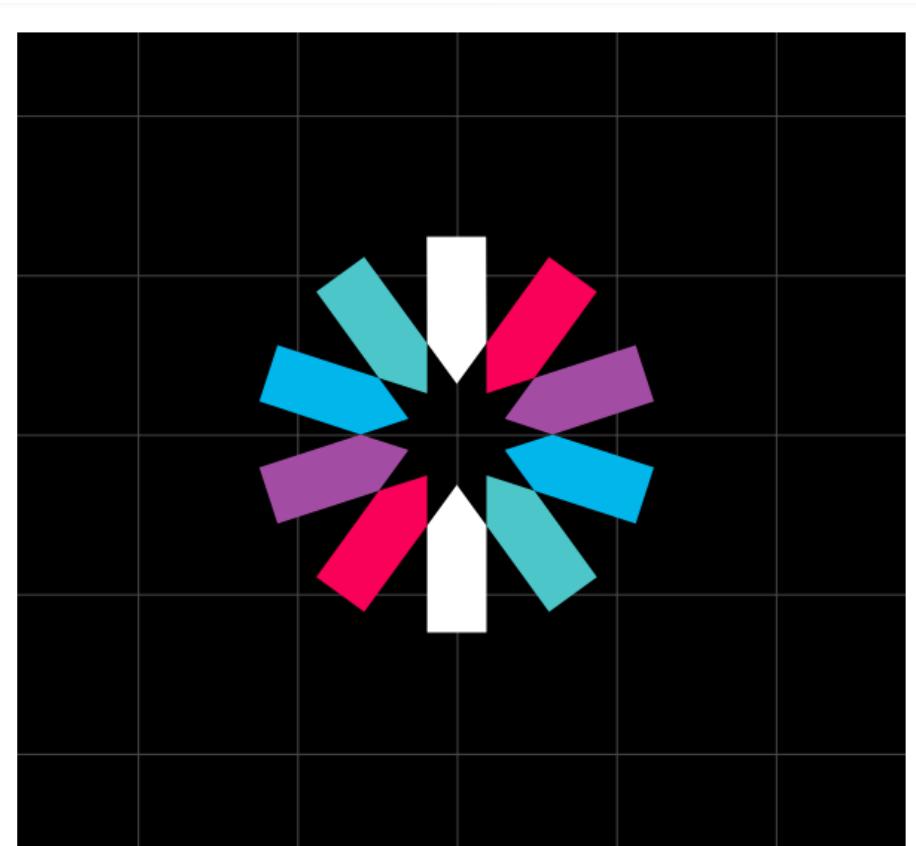
---

- Adds a level of indirection and avoids repeated username/password validation (avoids password discovery attacks on basic authentication mode)
- Allows users to access and manipulate a given resource without using username/password
- More benefits:
  - robust authentication solution for repeated requests
  - allows custom limited session duration (limited trust)
  - quickly transfer (user) information between systems (micro services)
  - allows the customisation of roles assigned to a given user at a given time
  - single sign-on in federated systems
  - external authorization servers (google, facebook, github, etc)
  - can be stored in local storage/cookies, can be invalidated or customized



# Token-based authentication

- (Good list of benefits, unknown author, [link](#)) 
- **Cross-domain / CORS:** cookies + CORS don't play well across different domains. A token-based approach allows you to make AJAX calls to any server, on any domain because you use an HTTP header to transmit the user information.
- **Stateless (a.k.a. Server side scalability):** there is no need to keep a session store, the token is a self-contained entity that conveys all the user information. The rest of the state lives in cookies or local storage on the client side.
- **CDN:** you can serve all the assets of your app from a CDN (e.g. javascript, HTML, images, etc.), and your server side is just the API.
- **Decoupling:** you are not tied to any particular authentication scheme. The token might be generated anywhere, hence your API can be called from anywhere with a single way of authenticating those calls.
- **Mobile ready:** when you start working on a native platform (iOS, Android, Windows 8, etc.) cookies are not ideal when consuming a token-based approach simplifies this a lot.
- **CSRF:** since you are not relying on cookies, you don't need to protect against cross site requests (e.g. it would not be possible to sib your site, generate a POST request and re-use the existing authentication cookie because there will be none).
- **Performance:** we are not presenting any hard perf benchmarks here, but a network roundtrip (e.g. finding a session on database) is likely to take more time than calculating an HMACSHA256 to validate a token and parsing its contents.



JWT HANDBOOK

By Sebastián Peyrott



Auth0

# Token Based Authentication

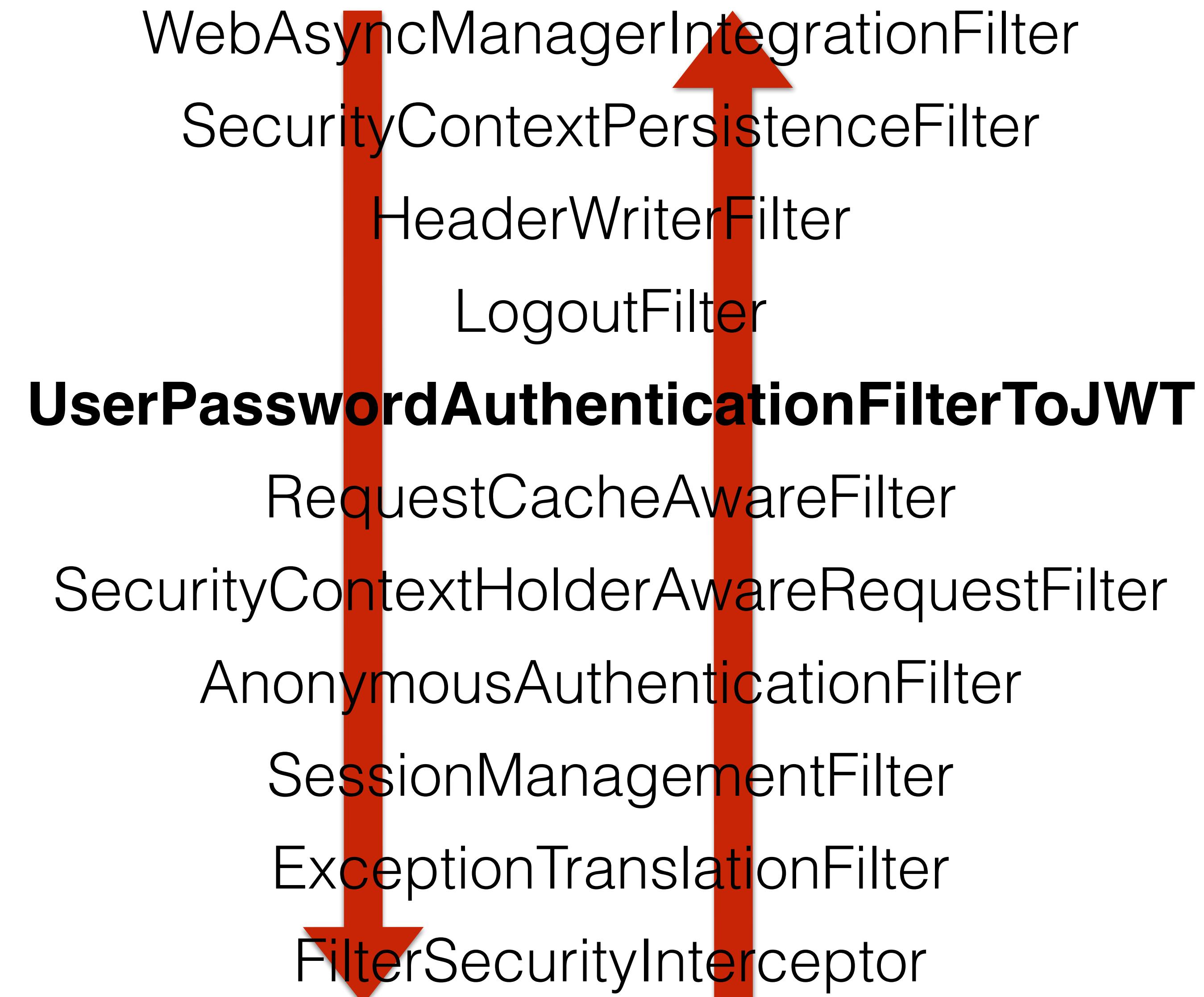
---

- Tokens can be managed manually in Spring using cookies (client-side) and sessions (server-side).
- The integration in Spring Security is performed by adding a filter in the Security Filter Chain that intercepts and overrides the authentication attempts.
- A standardised way of providing authentication is Bearer Authentication, where a token is inserted in the “Authorization Header”.

<https://tools.ietf.org/html/rfc6750>



# Spring Security Filters



# Token Creation - Login



```
class UserPasswordAuthenticationFilterToJWT {
    defaultFilterProcessesUrl: String?,
    private val anAuthenticationManager: AuthenticationManager
) : AbstractAuthenticationProcessingFilter(defaultFilterProcessesUrl) {

    override fun attemptAuthentication(request: HttpServletRequest?,
                                       response: HttpServletResponse?): Authentication? {
        //getting user from request body
        val user = ObjectMapper().readValue(request!!.InputStream, UserDAO::class.java)

        // perform the "normal" authentication
        val auth = anAuthenticationManager.authenticate(UsernamePasswordAuthenticationToken(user.username, user.password))

        return if (auth.isAuthenticated) {
            // Proceed with an authenticated user
            SecurityContextHolder.getContext().authentication = auth
            auth
        } else
            null
    }

    override fun successfulAuthentication(request: HttpServletRequest,
                                         response: HttpServletResponse,
                                         filterChain: FilterChain?,
                                         auth: Authentication) {

        // When returning from the Filter loop, add the token to the response
        addResponseToken(auth, response)
    }
}
```

<https://auth0.com/blog/implementing-jwt-authentication-on-spring-boot/>

# Token Creation - Login



```
object JWTSecret {  
    private const val passphrase = "este é um grande segredo que tem que ser mantido escondido"  
    val KEY: String = Base64.getEncoder().encodeToString(passphrase.toByteArray())  
    const val SUBJECT = "JSON Web Token for CIAI 2019/20"  
    const val VALIDITY = 1000 * 60 * 60 * 10 // 10 minutes in microseconds  
}  
  
private fun addResponseToken(authentication: Authentication, response: HttpServletResponse) {  
  
    val claims = HashMap<String, Any?>()  
    claims["username"] = authentication.name  
  
    val token = Jwts  
        .builder()  
        .setClaims(claims)  
        .setSubject(JWTSecret.SUBJECT)  
        .setIssuedAt(Date(System.currentTimeMillis()))  
        .setExpiration(Date(date: System.currentTimeMillis() + JWTSecret.VALIDITY))  
        .signWith(SignatureAlgorithm.HS256, JWTSecret.KEY)  
        .compact()  
  
    response.addHeader("Authorization", "Bearer $token")  
}
```



```
class UserPasswordAuthenticationFilterToJWT {  
    defaultFilterProcessesUrl: String?,  
    private val anAuthenticationManager: AuthenticationManager
```

```
iadi-2019-20-private — bash — 70x23  
$ http POST :8080/login username=user password=password  
HTTP/1.1 200  
Authorization: Bearer eyJhbGciOiJIUzI1NiJ9.eyJzdWIiOiJKU090IFd1YiBUb2t  
lbiBmb3IgQ01BSSAyMDE5LzIwIiwidXhwIjoxNTcxNzg0MjI0LCJpYXQiOjE1NzE3NDgyM  
jQsInVzZXJuYW1lIjoidXNlcjI9.MqIv5EUab1HjD1vST5Lfku0bvHsY0MyEHFt7-KDVoZ  
4  
Cache-Control: no-cache, no-store, max-age=0, must-revalidate  
Content-Length: 0  
Date: Tue, 22 Oct 2019 12:43:44 GMT  
Expires: 0  
Pragma: no-cache  
Set-Cookie: JSESSIONID=B7AED89D85B4BBB68257666D32E51E26; Path=/; HttpOnly  
X-Content-Type-Options: nosniff  
X-Frame-Options: DENY  
X-XSS-Protection: 1; mode=block
```

```
$ █
```

# JSON Web Token (JWT)

---



- Base64, signed token that asserts claims about a session/user
- Customisable claims (can carry user information, roles, dates)
- Can include ciphered information also, e.g. user capabilities
- Bearer

eyJhbGciOiJIUzI1NiJ9.eyJzdWIiOiJKU09OIFdIYiBUb2tlbiBmb3IgQ0IBSSAyM  
DE5LzlwlwiZXhwIjoxNTcxNzg0MjI0LCJpYXQiOjE1NzE3NDgyMjQsInVzZXJuY  
W1lljoidXNlcij9.Mqlv5EUab1HjD1vST5LfkuObvHsY0MyEHFt7-KDVoZ4

headerB64.payloadB64.SignHS256

[Debugger](#)[Libraries](#)[Introduction](#)[Ask](#)[Get a T-shirt!](#)

Crafted by Auth0

ALGORITHM

HS256

## Encoded

PASTE A TOKEN HERE

```
eyJhbGciOiJIUzI1NiJ9.eyJzdWIiOiJKU090IFd  
1YiBUb2tlbiBmb3IgQ01BSSAyMDE5LzIwIiwiZXh  
wIjoxNTcxNzg0MjI0LCJpYXQiOjE1NzE3NDgyMjQ  
sInVzZXJuYW1lIjoidXNlciJ9.MqIv5EUab1HjD1  
vST5LfU0bvHsY0MyEHFt7-KDVoZ4
```

## Decoded

EDIT THE PAYLOAD AND SECRET

### HEADER: ALGORITHM & TOKEN TYPE

```
{  
  "alg": "HS256"  
}
```

### PAYOUT: DATA

```
{  
  "sub": "JSON Web Token for CIAI 2019/20",  
  "exp": 1571784224,  
  "iat": 1571748224, Tue Oct 22 2019 13:43:44 GMT+0100 (Western European Summer Time)  
  "username": "user"  
}
```

### VERIFY SIGNATURE

```
HMACSHA256(  
  base64UrlEncode(header) + "." +
```

# Token Validation

```
class JWTAuthenticationFilter: GenericFilterBean() {  
  
    // To try it out, go to https://jwt.io to generate custom tokens, in this case we only need a name...  
  
    override fun doFilter(request: ServletRequest?,  
                         response: ServletResponse?,  
                         chain: FilterChain?) {  
  
        val authHeader = (request as HttpServletRequest).getHeader("Authorization")  
  
        if( authHeader != null && authHeader.startsWith("Bearer ") ) {  
            val token = authHeader.substring(7) // Skip 7 characters for "Bearer "  
            val claims = Jwts.parser().setSigningKey(JWTSecret.KEY).parseClaimsJws(token).body  
  
            // should check for token validity here (e.g. expiration date, session in db, etc.)  
            val exp = (claims["exp"] as Int).toLong()  
            if ( exp < System.currentTimeMillis()/1000 ) // in seconds  
  
                (response as HttpServletResponse).sendError(HttpServletResponse.SC_UNAUTHORIZED) // RFC 6750 3.1  
  
            else {  
  
                val authentication = UserAuthToken(claims["username"] as String)  
                // Can go to the database to get the actual user information (e.g. authorities)  
  
                SecurityContextHolder.getContext().authentication = authentication  
  
                // Renew token with extended time here. (before doFilter)  
                addResponseToken(authentication, response as HttpServletResponse)  
  
                chain!!.doFilter(request, response)  
            }  
        } else {  
            chain!!.doFilter(request, response)  
        }  
    }  
}
```

<https://bitbucket.org/costaseco/iadi-2019-20/src/master/>

# Token Validation



```
class UserPasswordAuthenticationFilterToJWT {
    defaultFilterProcessesUrl: String?,
    ) : A[ $ http :8080/pets Authorization:"Bearer eyJhbGciOiJIUzI1NiJ9eyJzdWIiO
    iJKU090IFd1YiBUb2tlbiBmb3IgQ01BSSAyMDE5LzIwIiwizXhwIjoxNTcxNzg0Nzg1LCJ
    pYXQiOjE1NzE3NDg3ODUsInVzZXJuYW1lIjoidXNlcij9.hBenpmApZMcEOalI4p-UKIy5
    9FSe0-19Fw987He7HGg"
HTTP/1.1 200
Authorization: Bearer eyJhbGciOiJIUzI1NiJ9eyJzdWIiOiJKU090IFd1YiBUb2t
    1biBmb3IgQ01BSSAyMDE5LzIwIiwizXhwIjoxNTcxNzg0ODM3LCJpYXQiOjE1NzE3NDg4M
    zcsInVzZXJuYW1lIjoidXNlcij9.cPog74fYmoFirCYvyOR_HeJ3DyYPRbUPEqHUiVbfgh
Q
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Content-Type: application/json; charset=UTF-8
Date: Tue, 22 Oct 2019 12:53:57 GMT
Expires: 0
Pragma: no-cache
Set-Cookie: JSESSIONID=D11358DC1A75490FCAF2C314DF5413EA; Path=/; HttpO
    nly
Transfer-Encoding: chunked
X-Content-Type-Options: nosniff
X-Frame-Options: DENY
X-XSS-Protection: 1; mode=block

[ ]

$ // When returning from the Filter loop, add the token to the response
addResponseToken(auth, response)
}
```

# Internet Applications Design and Implementation

## 2020 - 2021

### (Lecture 6 - Part 3 -OAuth)

**MIEI - Integrated Master in Computer Science and Informatics  
Specialization block**

**João Costa Seco ([joao.seco@fct.unl.pt](mailto:joao.seco@fct.unl.pt))**

(with previous participations of Jácome Cunha ([jacome@fct.unl.pt](mailto:jacome@fct.unl.pt)) and João Leitão ([jc.leitao@fct.unl.pt](mailto:jc.leitao@fct.unl.pt)))



FACULDADE DE  
CIÊNCIAS E TECNOLOGIA  
UNIVERSIDADE NOVA DE LISBOA

# OAuth 2.0

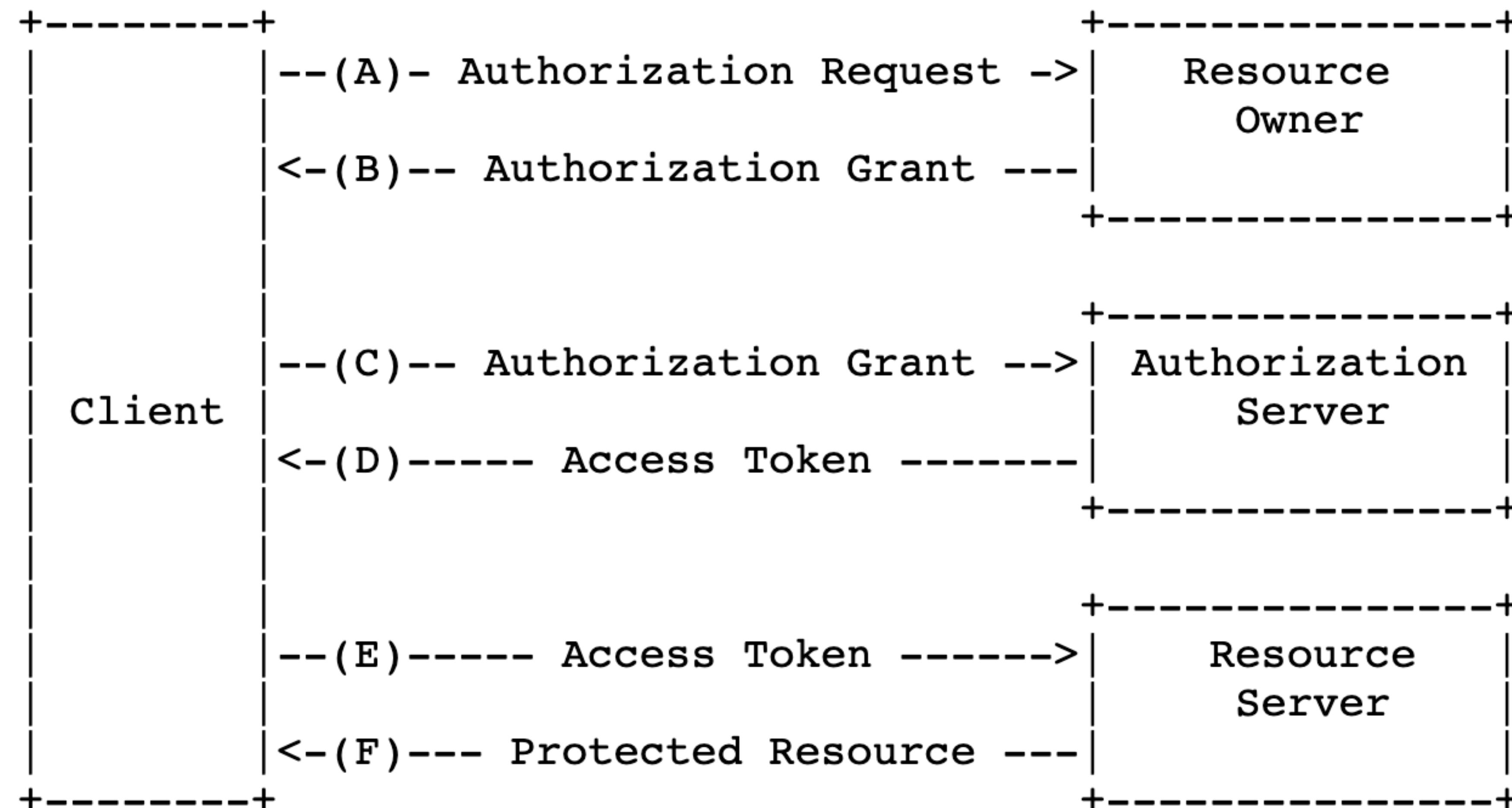
---

- Provides a protocol for authorisation for Internet applications, resource owners, through third-parties on behalf of a principal.
- OAuth defines four roles (from the RFC):
  - **resource owner:** An entity capable of granting access to a protected resource. When the resource owner is a person, it is referred to as an end-user.
  - **resource server:** The server hosting the protected resources, capable of accepting and responding to protected resource requests using access tokens.
  - **client:** An application making protected resource requests on behalf of the resource owner and with its authorisation.
  - **authorization server:** The server issuing access tokens to the client after successfully authenticating the resource owner and obtaining authorisation.

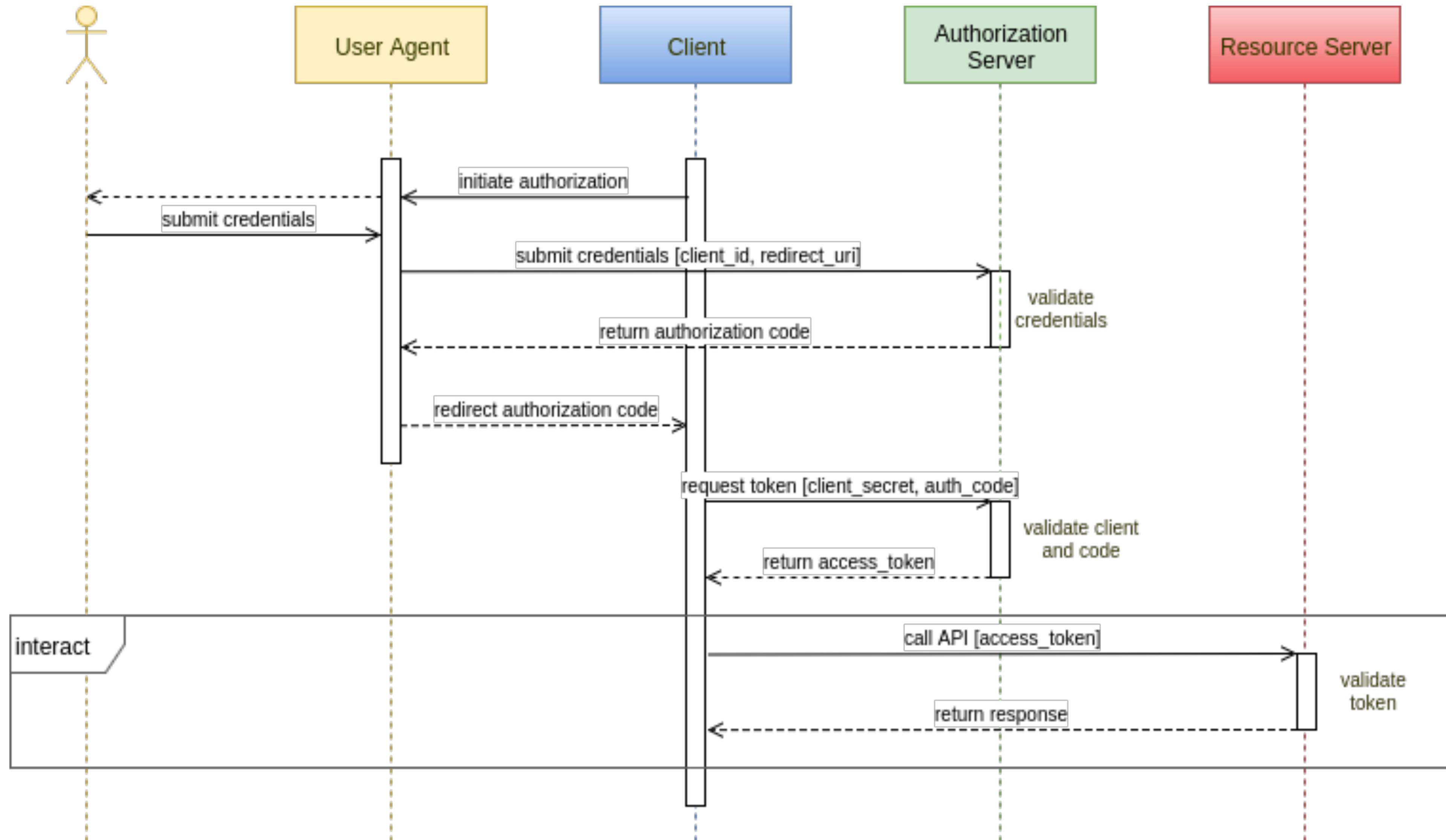
<https://tools.ietf.org/html/rfc6749>



# Auth 2.0 protocol flow



# Token-based interactions



# Using spring...

---

- Spring Boot provides an implementation for oAuth 2.0 that is easy to configure by loading a single module:

```
<dependency>
    <groupId>org.springframework.boot</groupId>
    <artifactId>spring-boot-starter-oauth2-client</artifactId>
</dependency>
```

- and configuring two properties

```
spring.security.oauth2.client.registration.github.client-id = client-id
spring.security.oauth2.client.registration.github.client-secret = client-secret
```

# The network interactions

---

1. A request is captured by a filter in Spring Security with no token
2. It is redirected to :  
[http://localhost:8080/oauth2/authorize/github?redirect\\_uri=<TheURIOfYourApp>](http://localhost:8080/oauth2/authorize/github?redirect_uri=<TheURIOfYourApp>)
3. The user is redirected to the AuthorizationUrl of GitHub
4. When authorised, it is redirected to:  
<http://localhost:8080/oauth2/callback/github>
5. A JWT token is created and the user is redirected to the TheURIOfYourApp