Introduction to Software Business Product Management

Week 2 Day 3

Led by: Emily Crose

for

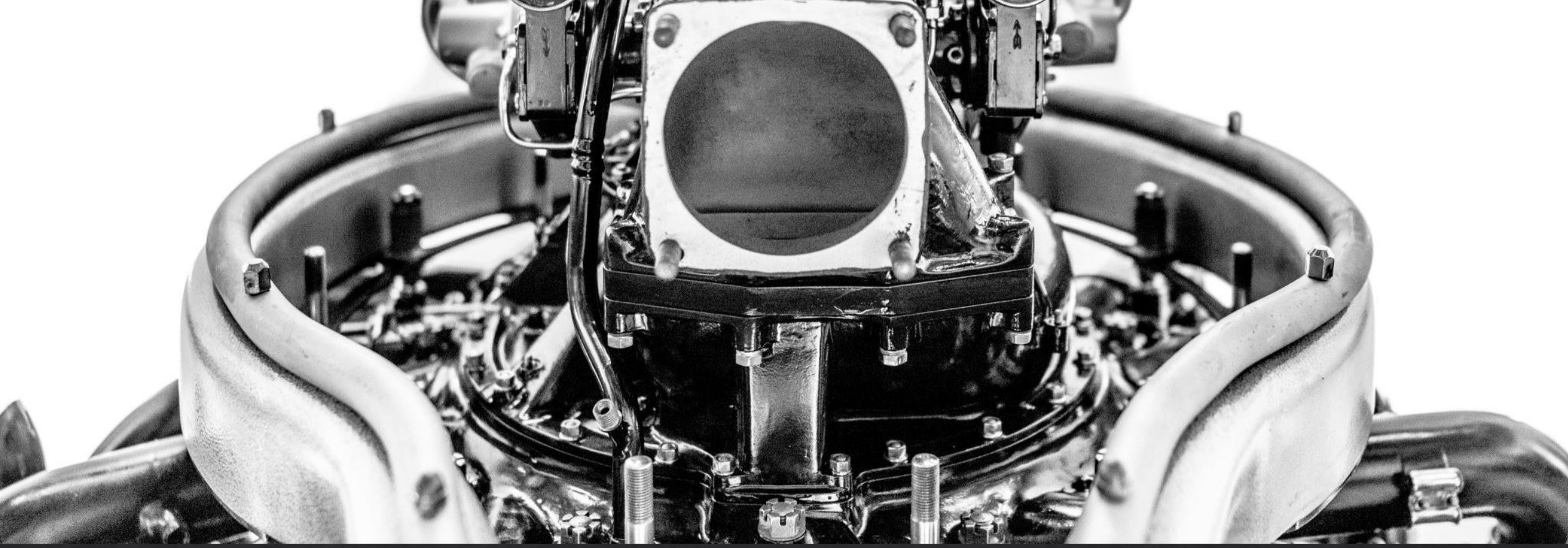
Oakland University

Day 2 Recap


Questions From Day 2?

Terms To Listen For

- Application Programming Interface (API)
  - Enables automated, programmatic retrieval of information using a standard framework.
- Authentication
  - Refers to the process of verifying a user's identity.
- Rate-Limit
  - How many requests can occur at a given time.
- Denial of Service
  - A forced outage of a service based on a misconfiguration or a concerted effort

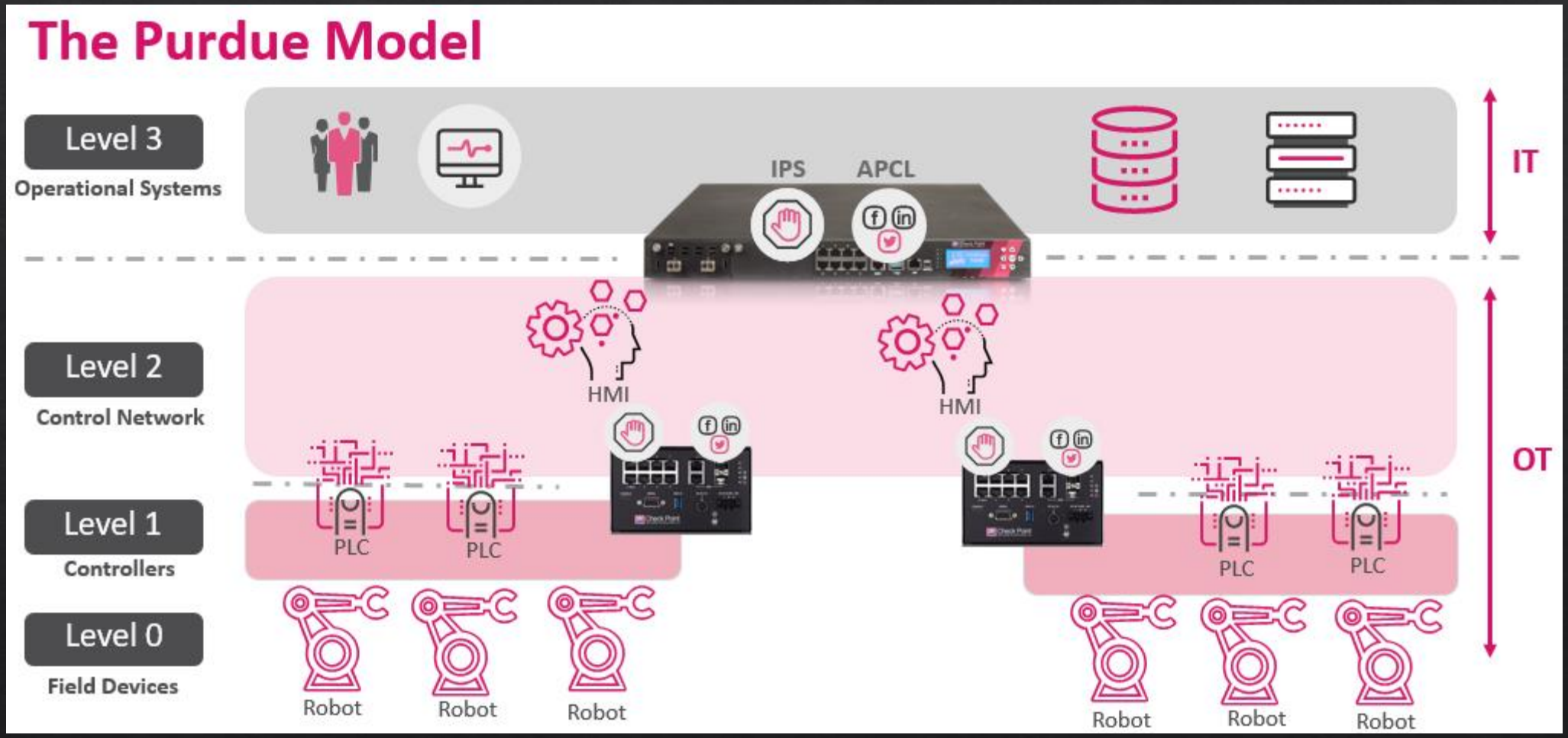


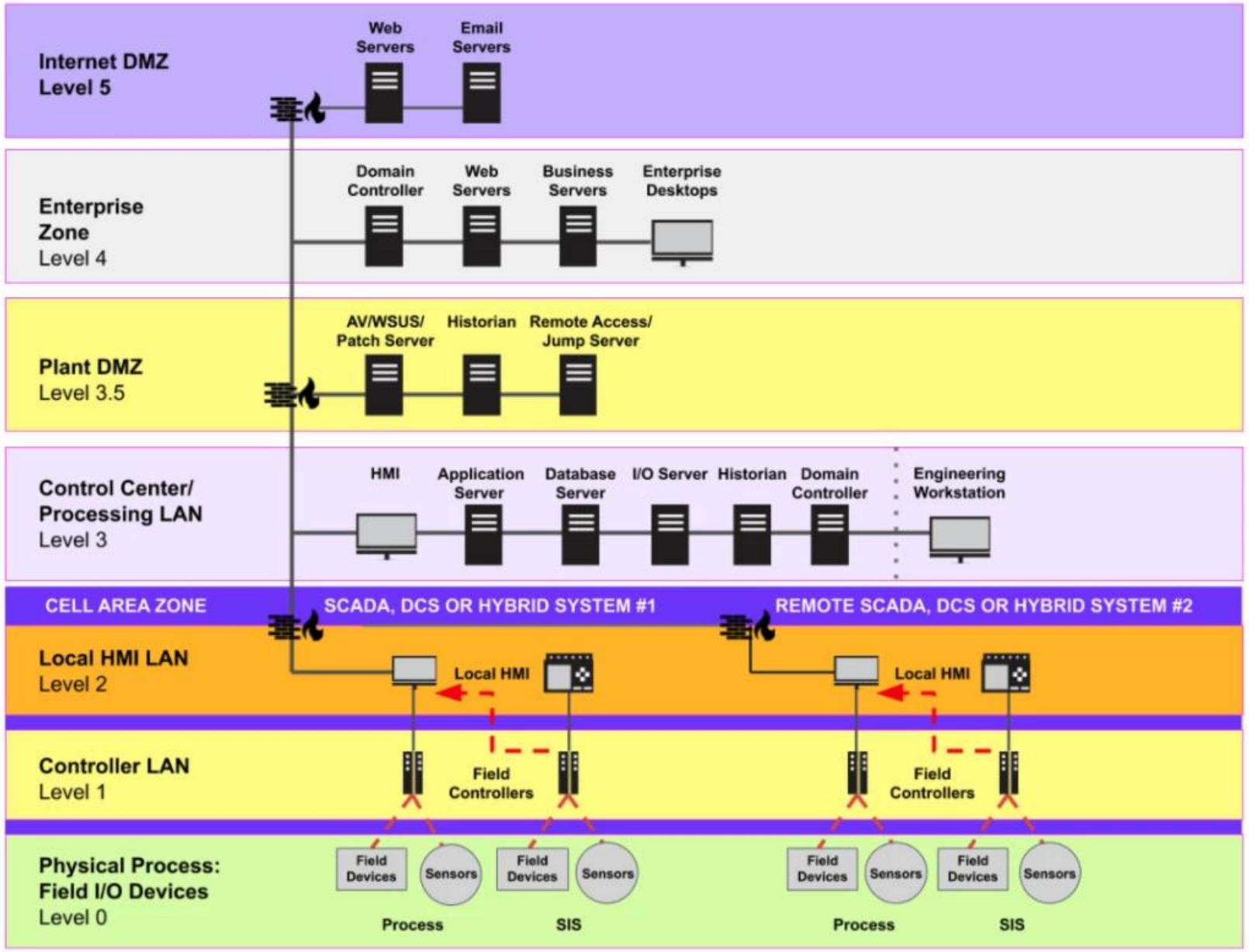
Purdue Model Explained

Purdue Model, What Is It?

- A method of arranging and segmenting networked operational technology (OT) devices.

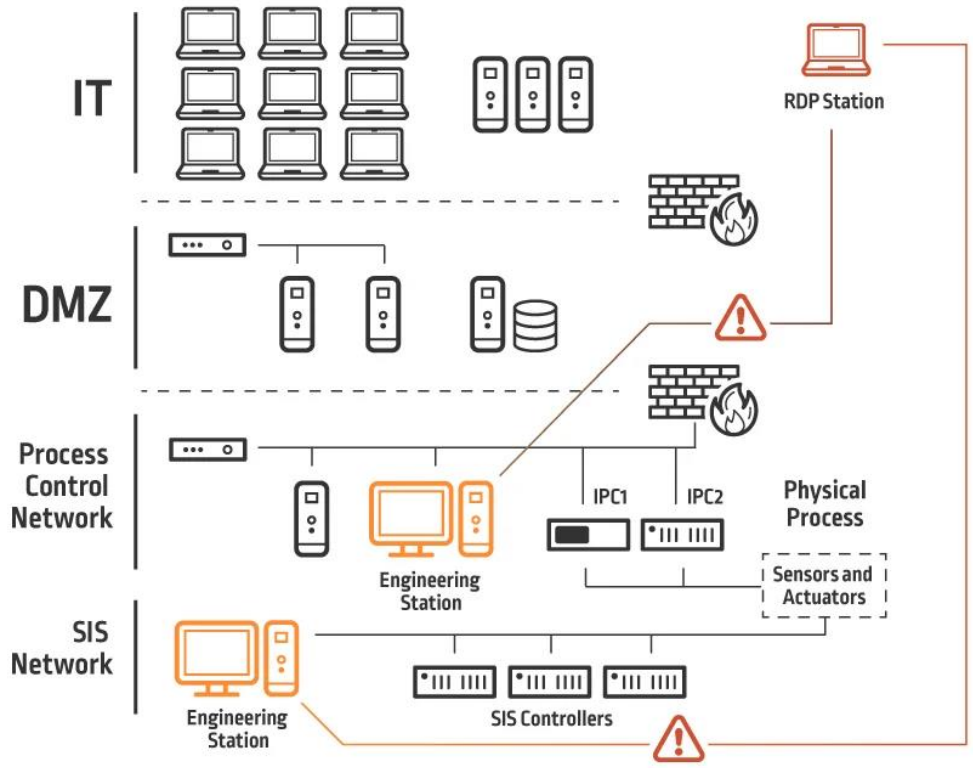
The Purdue Model




Internet DMZ
Level 5
Web Servers
Email Servers
Enterprise Zone
Level 4
Domain Controller
Web Servers
Business Servers
Enterprise Desktops
Plant DMZ
Level 3.5
AV/WSUS/ Patch Server
Historian
Remote Access/ Jump Server
Control Center/ Processing LAN
Level 3
HMI
Application Server
Database Server
I/O Server
Historian
Domain Controller
Engineering Workstation
CELL AREA ZONE
SCADA, DCS OR HYBRID SYSTEM #1
REMOTE SCADA, DCS OR HYBRID SYSTEM #2
Local HMI LAN
Level 2
Local HMI
Local HMI
Controller LAN
Level 1
Field Controllers
Field Controllers
Physical Process: Field I/O Devices
Level 0
Field Devices
Sensors
Field Devices
Sensors
Field Devices
Sensors
Field Devices
Sensors
Process
SIS
Process
SIS

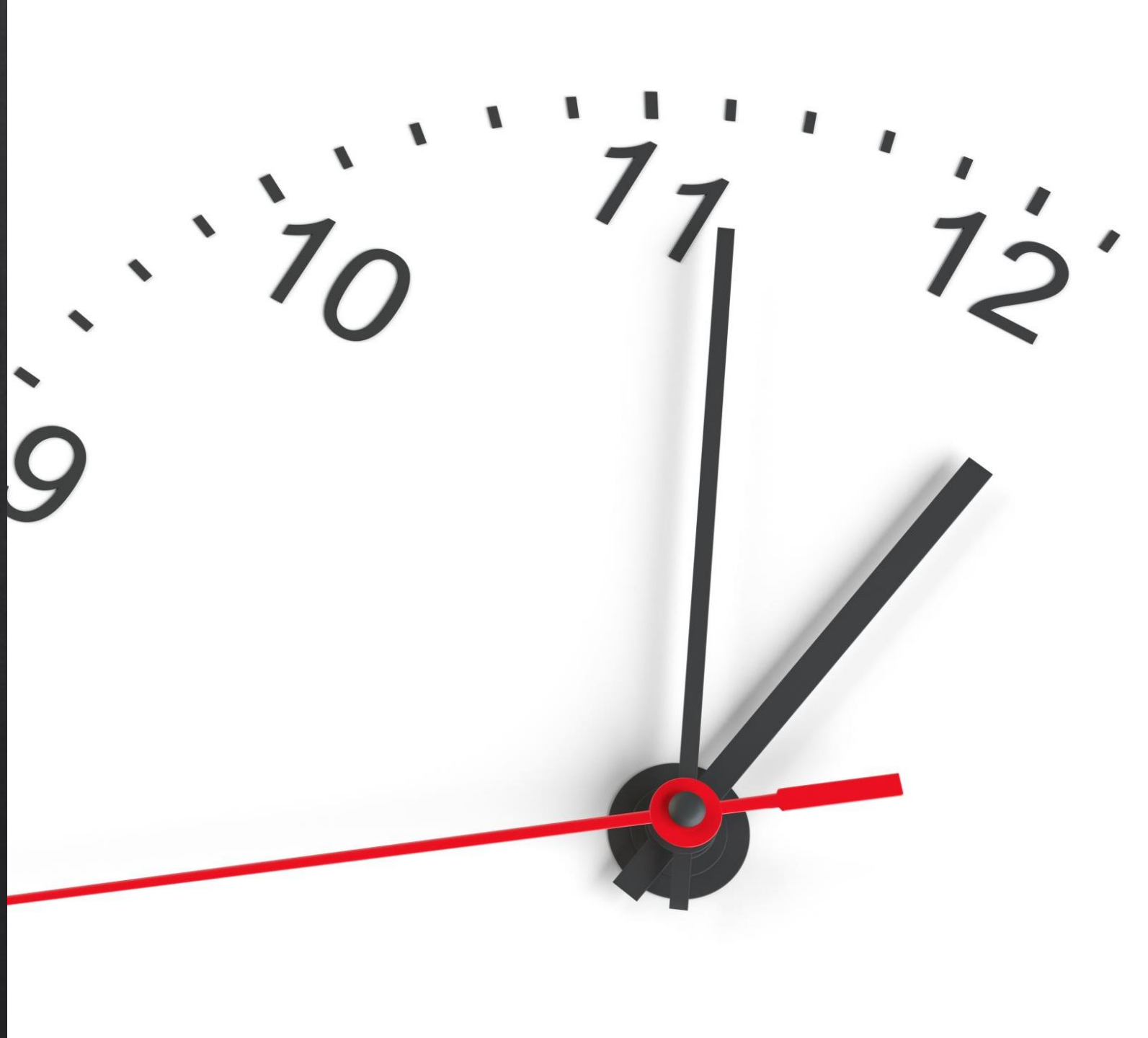
Anatomy Of A Complex OT Attack

Inside The Victim Network



Who Cares About This?

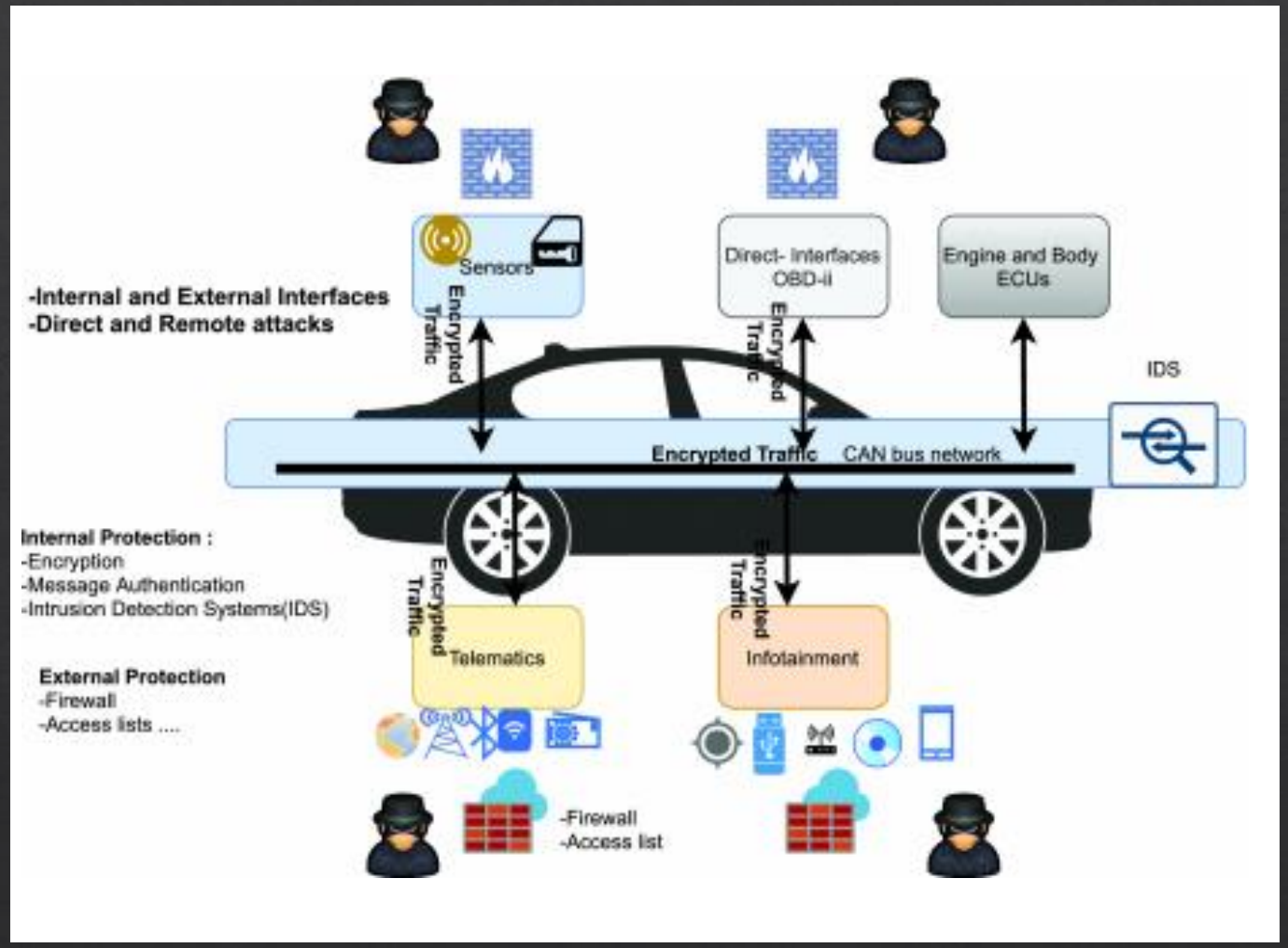
10 minute break

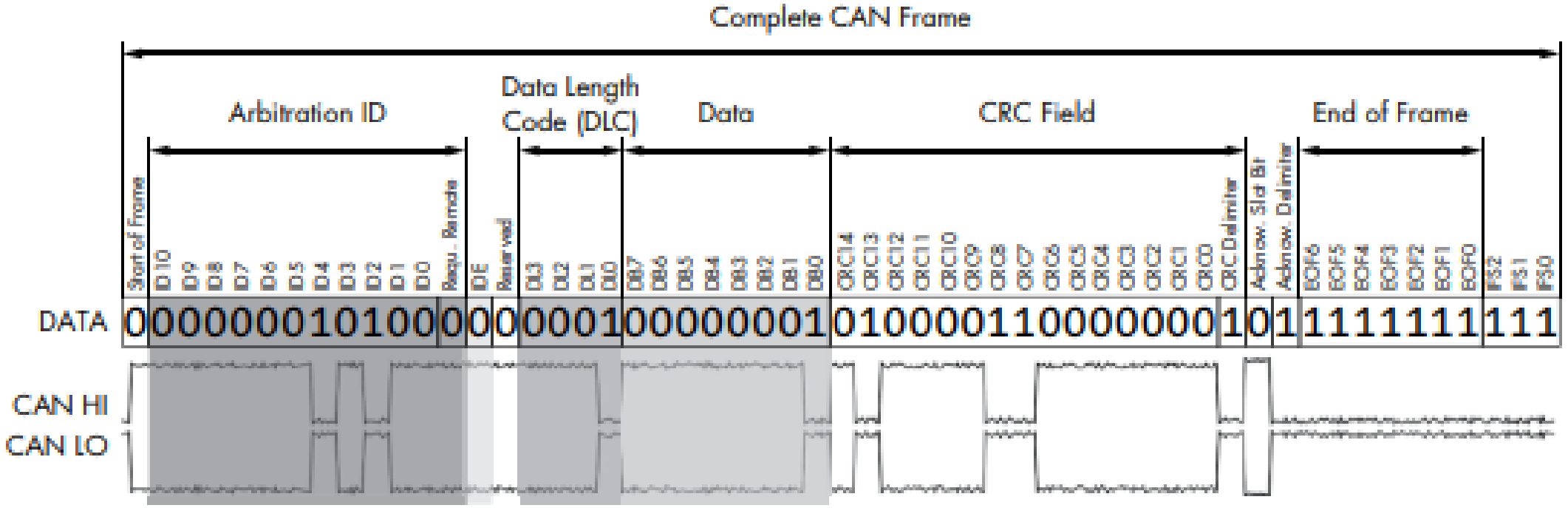


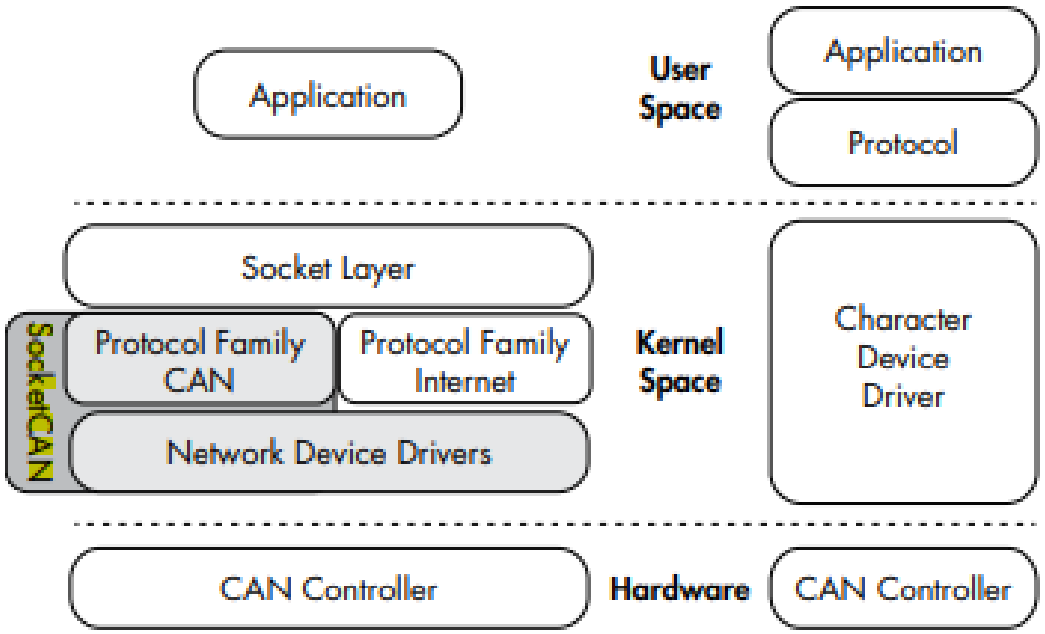
How Does Software Fit In?


Can This Apply To Cars?

Controller Area Network




Complete CAN Frame
Arbitration ID
Data Length Code (DLC)
Data
CRC Field
End of Frame
Start of Frame
ID10 ID9 ID8 ID7 ID6 ID5 ID4 ID3 ID2 ID1 ID0
Requ. Remote
IDE
Reserved
DL3 DL2 DL1 DL0
DB7 DB6 DB5 DB4 DB3 DB2 DB1 DB0
CRC14 CRC13 CRC12 CRC11 CRC10 CRC9 CRC8 CRC7 CRC6 CRC5 CRC4 CRC3 CRC2 CRC1 CRC0
CRC Delimiter
Acknow. Slot Bit
Acknow. Delimiter
EOF6 EOF5 EOF4 EOF3 EOF2 EOF1 EOF0
IFS2 IFS1 IFS0
DATA
0 00000010100 0 0 0 0001 00000001 0100001 1 0000000 1 0 1111111 111
CAN HI
CAN LO

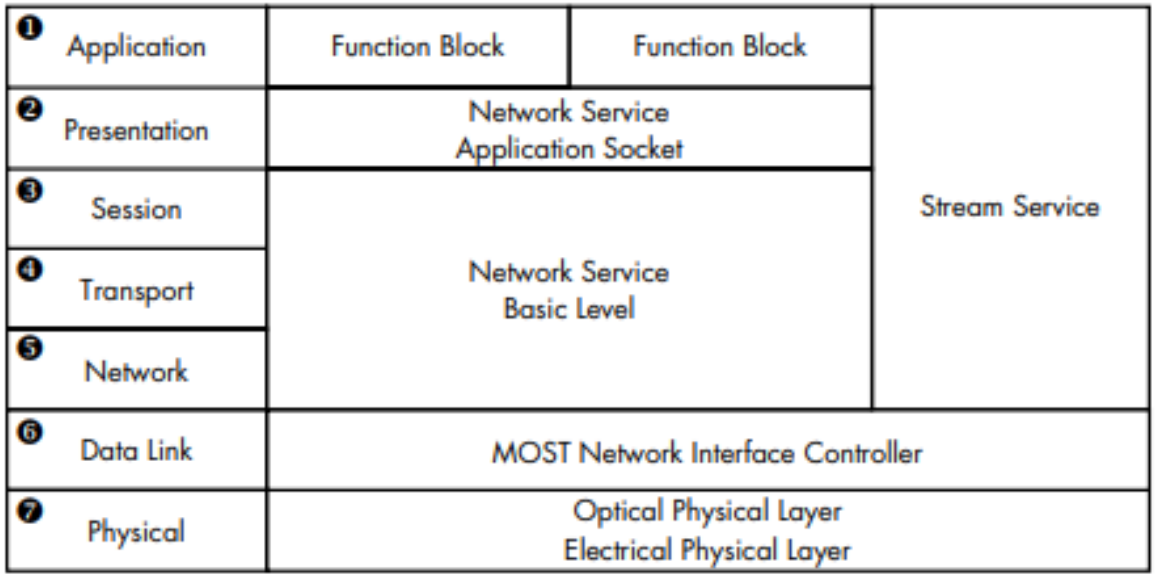

Application
User Space
Application
Protocol
Socket Layer
SocketCAN
Protocol Family CAN
Protocol Family Internet
Network Device Drivers
Kernel Space
Character Device Driver
CAN Controller
Hardware
CAN Controller

SocketCAN

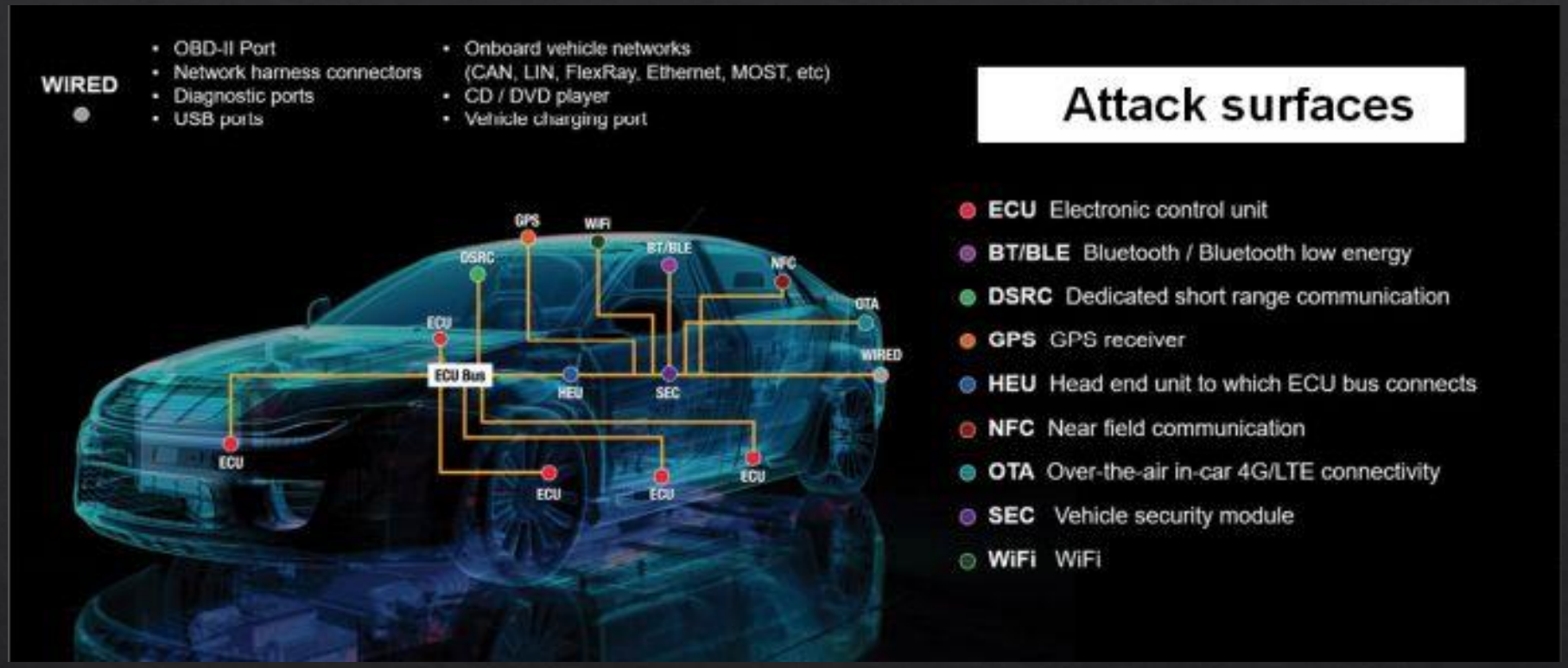

Where’s the Security??

Additional Protocols In Use

- ISO-TP
  - A.K.A. ISO 15765-2
- CANopen
- GMLAN

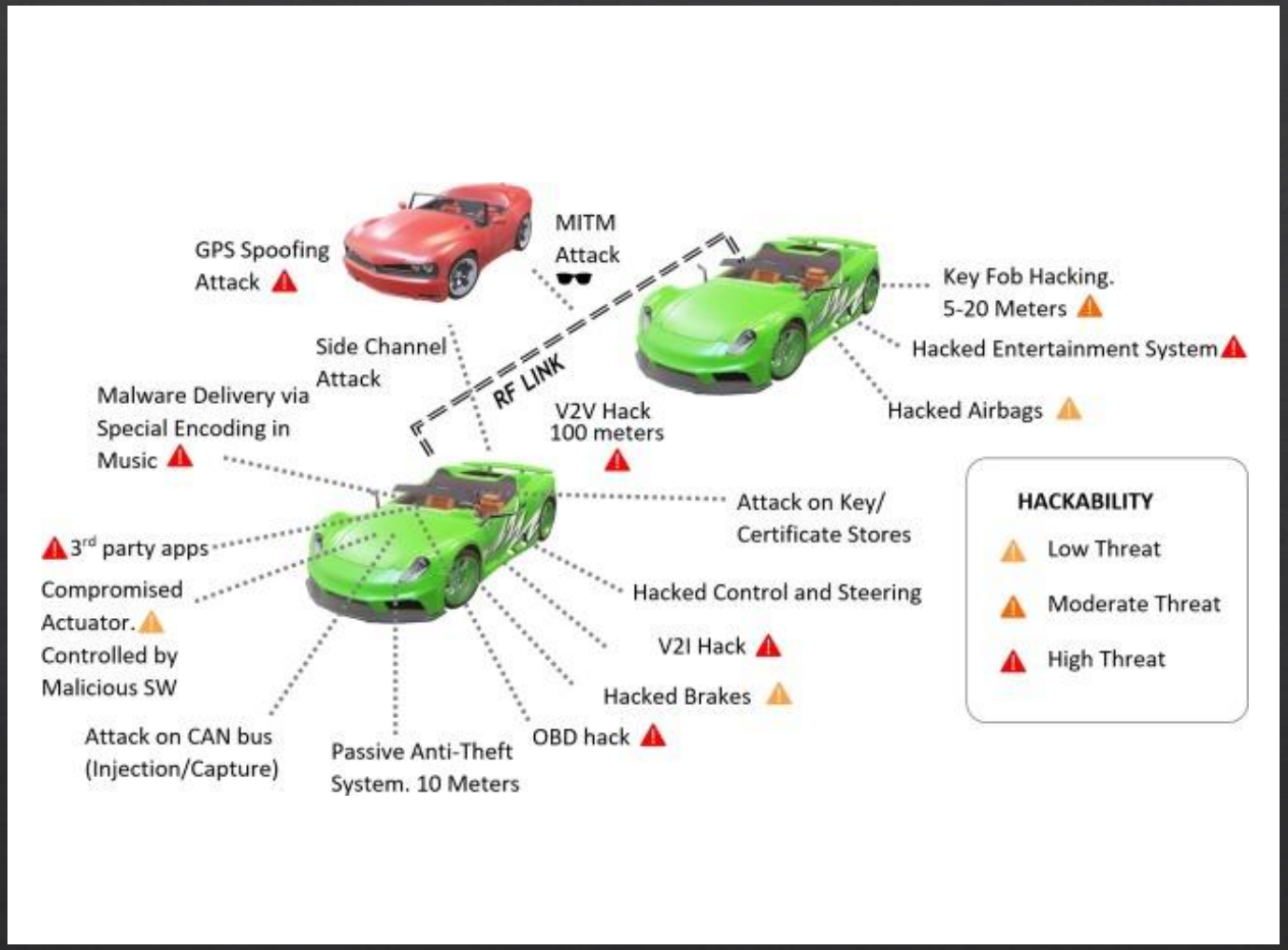


Vehicle Media Systems



Car Software Attack Surface

Popular Car Attack Surfaces



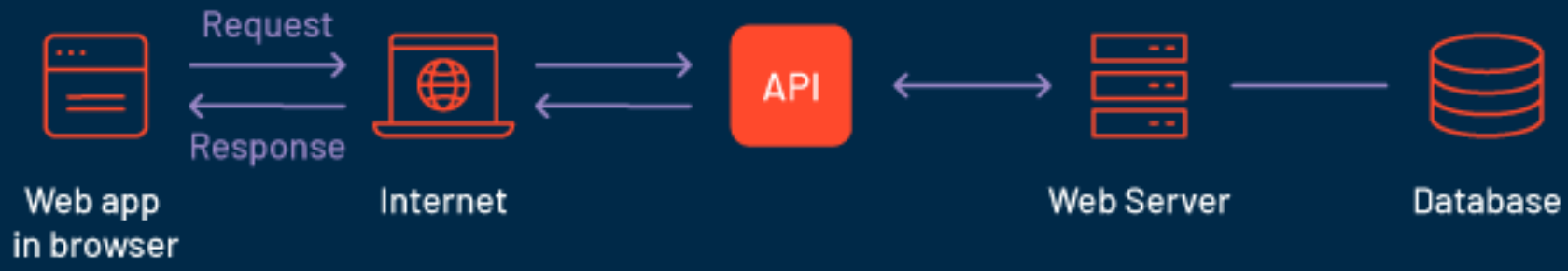
References

- The Car Hackers Handbook: A Guide For The Penetration Tester by Craig Smith

Application Programming Interfaces (APIs)

- What do they do for applications?
- When would we want to use an API?

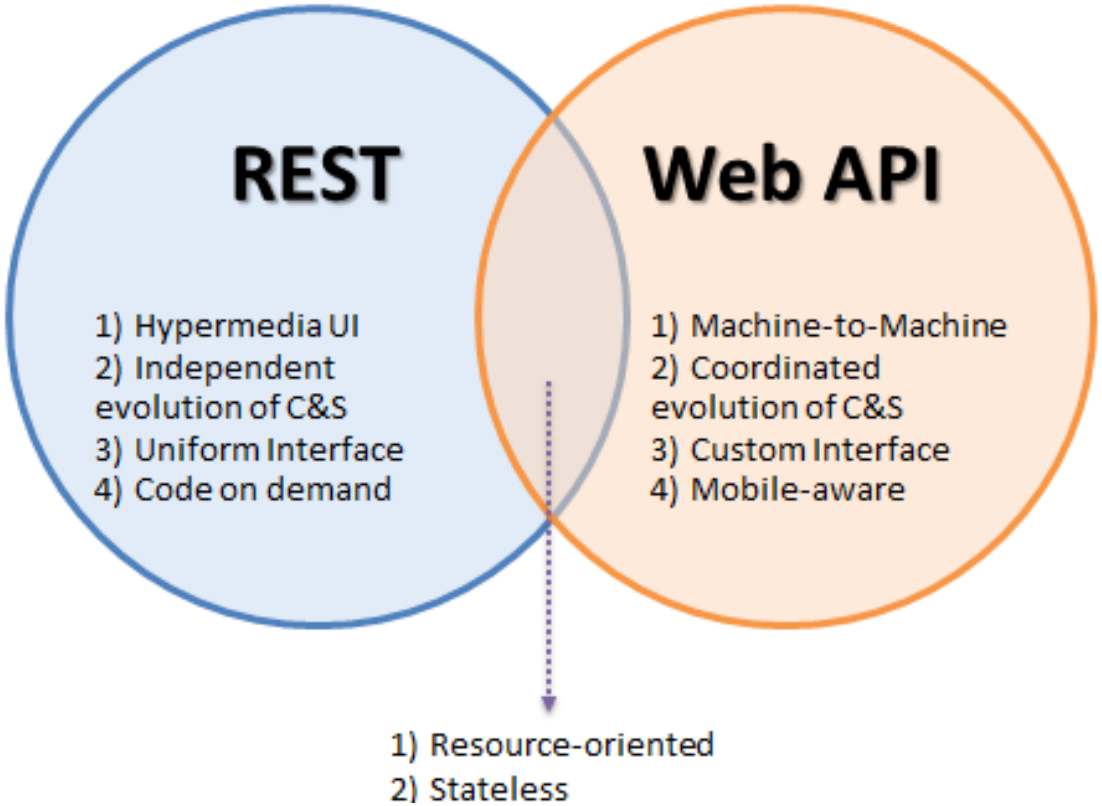
How Do APIs Work



Familiar APIs

- Representational State Transfer (REST or RESTful) API
  - Fast
  - Reliable
  - Widely adopted
  - Simple!
- Simple Object Access Protocol (SOAP)
  - Used in some OT network appliances
- Browser API
- iOS/Android API
  - Allows developers the tools they need to utilize local resources in their own programs
    - Notification API calls
    - Camera activation
    - Media integration

```
{
  "employees": [
    {
      "id": 1,
      "first_name": "Sebastian",
      "last_name": "Eschweiler",
      "email": "sebastian@codingthesmartway.com"
    },
    {
      "id": 2,
      "first_name": "Steve",
      "last_name": "Palmer",
      "email": "steve@codingthesmartway.com"
    },
    {
      "id": 3,
      "first_name": "Ann",
      "last_name": "Smith",
      "email": "ann@codingthesmartway.com"
    }
  ]
}
```

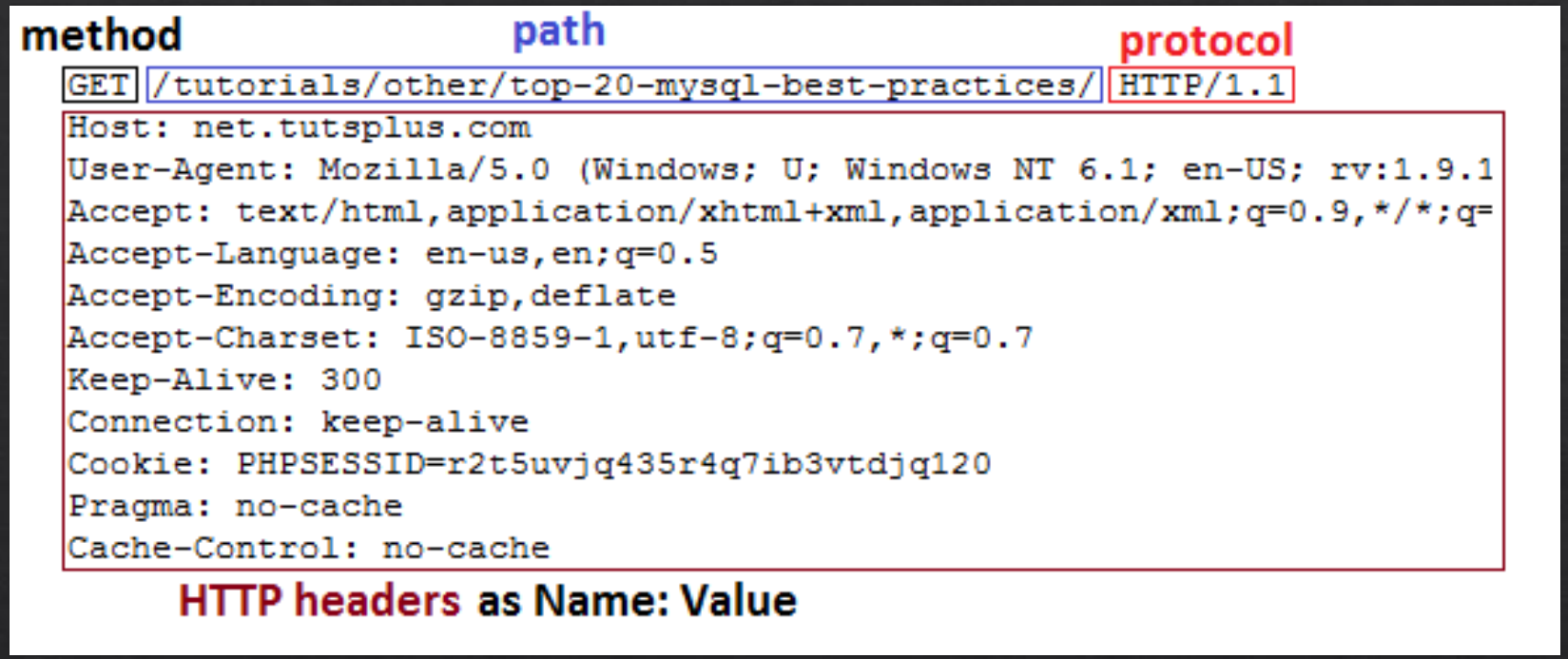


Popular API Frameworks

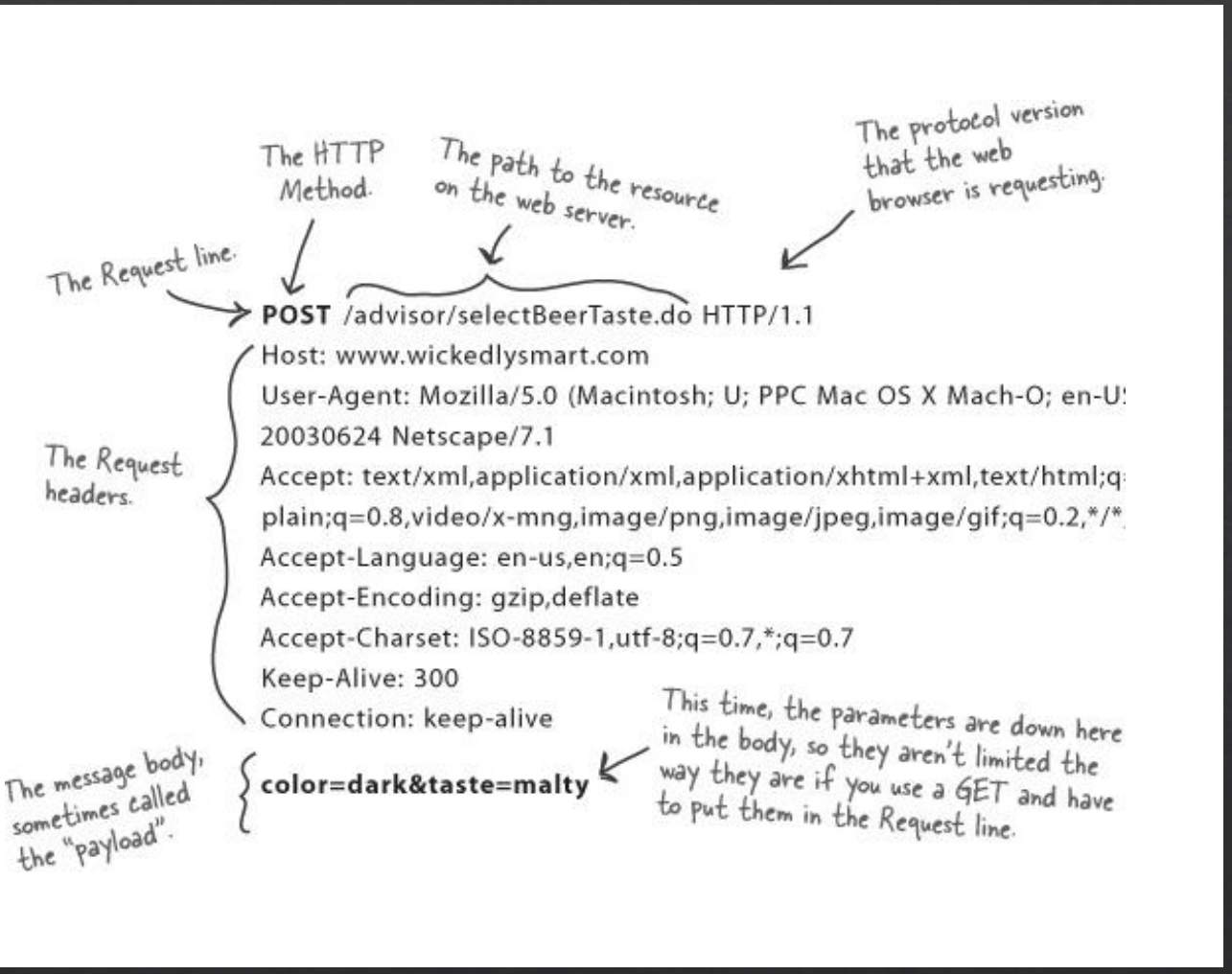

HTTP/Web API

HTTP API Verbs

- HTTP
  - GET
  - POST
  - PUT
  - DELETE



HTTP GET Header



HTTP POST Header

Weather API Documentation

- https://rapidapi.com/weatherapi/api/weatherapi-com

(Node.js) Axios Copy Code

```
const axios = require("axios");

const options = {
  method: 'GET',
  url: 'https://weatherapi-com.p.rapidapi.com/current.json',
  params: {q: '53.1,-0.13'},
  headers: {
    'X-RapidAPI-Key': 'SIGN-UP-FOR-KEY',
    'X-RapidAPI-Host': 'weatherapi-com.p.rapidapi.com'
  }
};

axios.request(options).then(function (response) {
    console.log(response.data);
}).catch(function (error) {
    console.error(error);
});
```

Working With APIs

- Can be programmed
- Can be used in a raw request

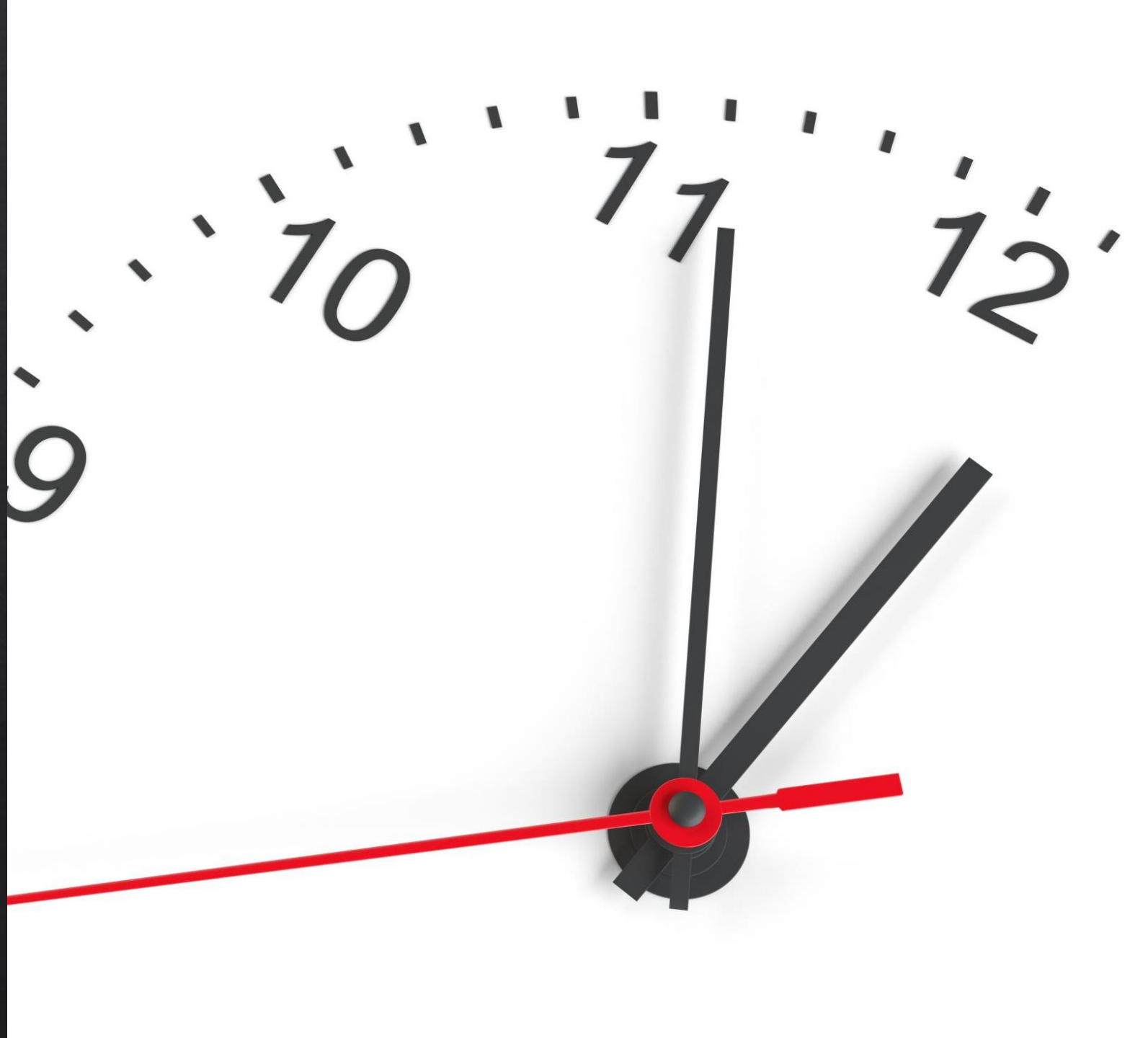
Programming Mobile Apps w/APIs

- Android
  - Kotlin
- Apple iOS
  - SWIFT
- Both have access to device APIs!

Mobile Device API Example


```
{"coord":{"lon":-0.13,"lat":51.51},"weather":[{"id":300,"main":"Drizzle","description":"light
intensity drizzle","icon":"09d"}],"base":"stations","main":
{"temp":280.32,"pressure":1012,"humidity":81,"temp_min":279.15,"temp_max":281.15},"visibility"
:10000,"wind":{"speed":4.1,"deg":80},"clouds":{"all":90},"dt":1485789600,"sys":
{"type":1,"id":5091,"message":0.0103,"country":"GB","sunrise":1485762037,"sunset":1485794875},
"id":2643743,"name":"London","cod":200}
```

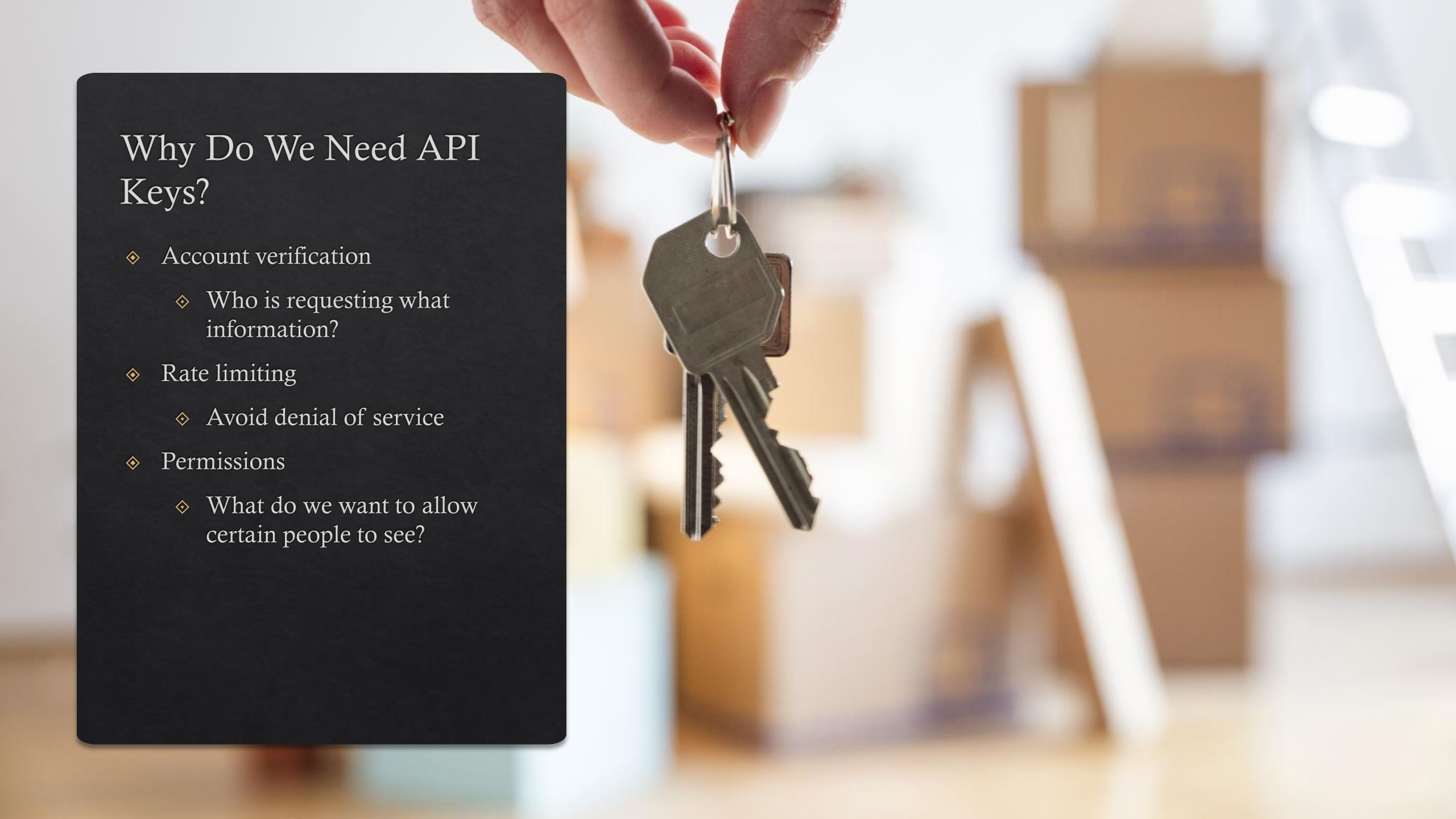
10 minute break

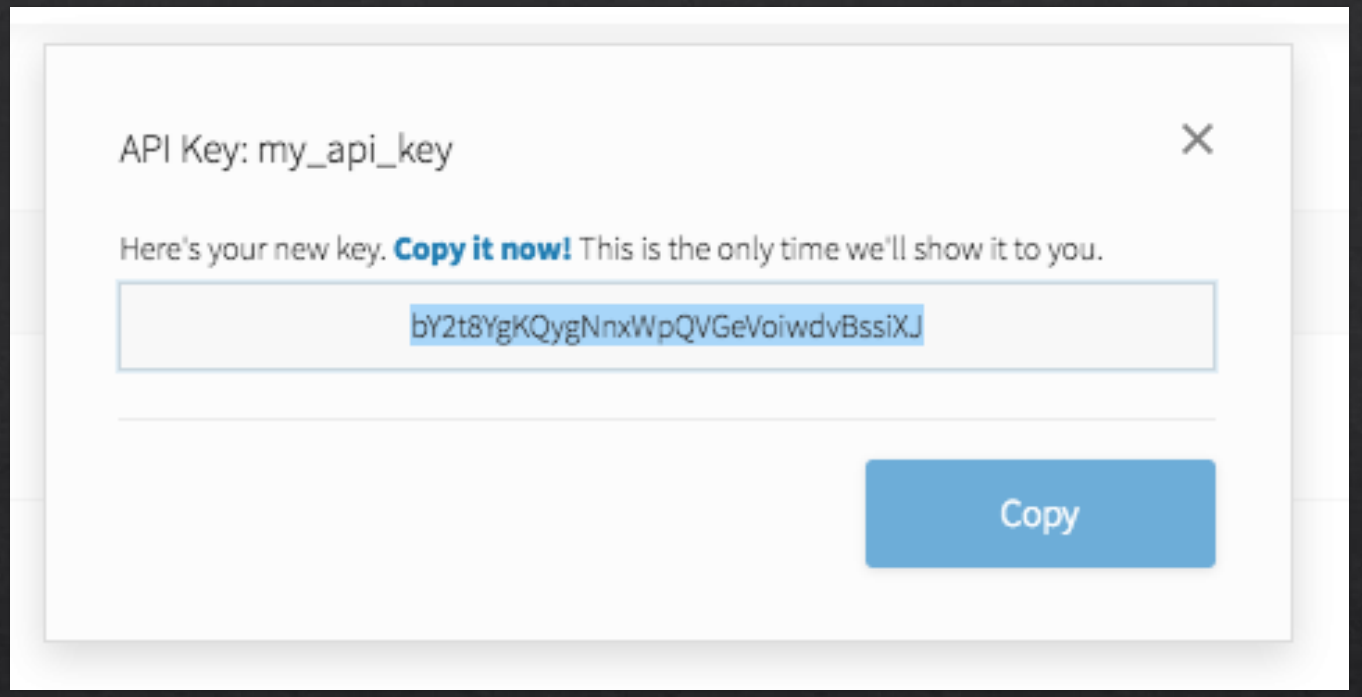


Securing APIs

Why Do We Need API Keys?

- Account verification
  - Who is requesting what information?
- Rate limiting
  - Avoid denial of service
- Permissions
  - What do we want to allow certain people to see?

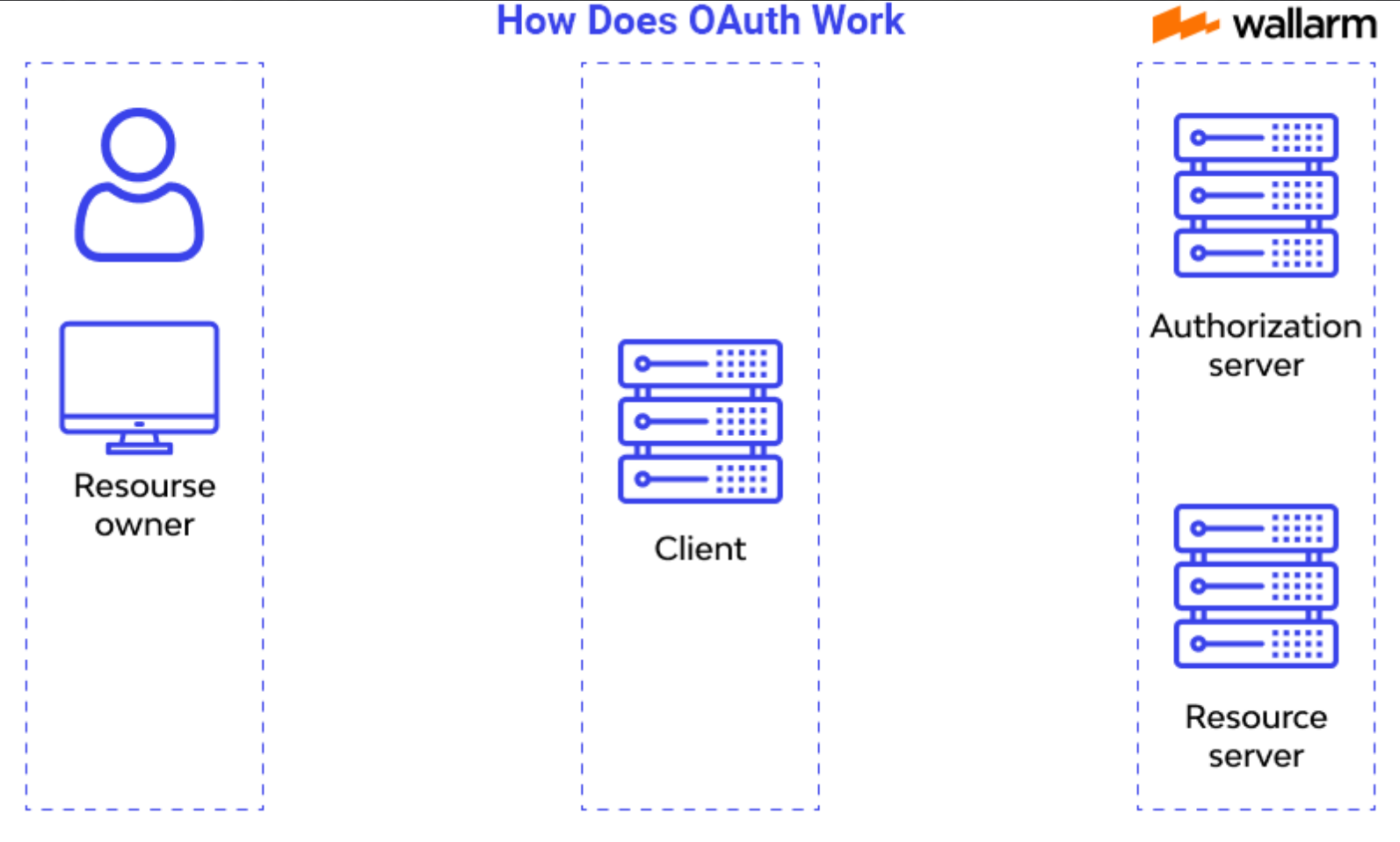



API Key: my_api_key
Here's your new key. Copy it now! This is the only time we'll show it to you.
bY2t8YgKQygNnxWpQVGeVoiwdvBssiXJ
Copy

API Key

What is Oauth?

How does OAuth work?



Let’s Make A Github Account!

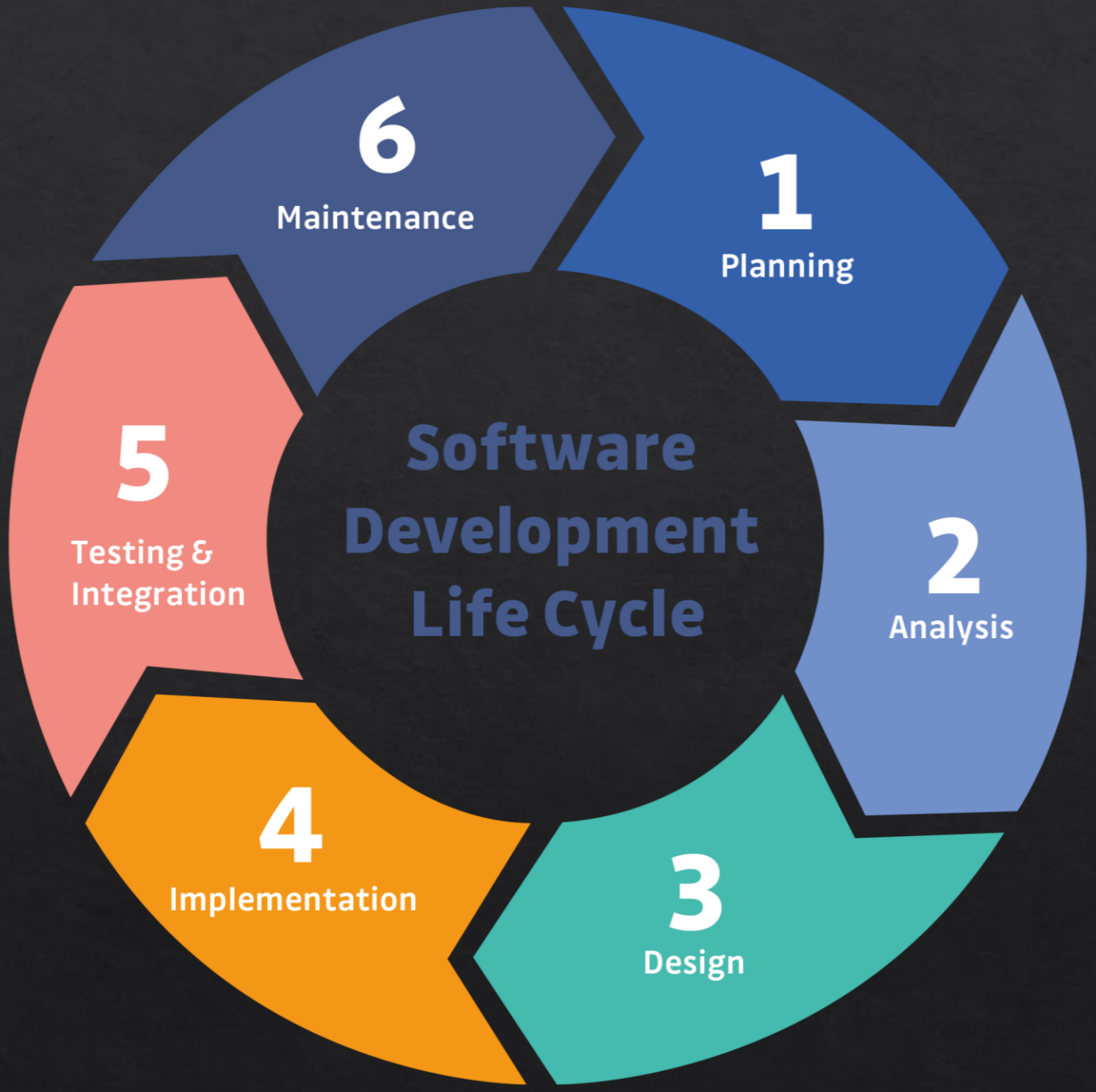
- https://github.com

Software Development: The Lifecycle

What is the Software Development Life Cycle?

- The SDLC helps us organize the process of building software
- Includes steps for building, revising, and deploying software
- Includes roles associated with each step along the building process

Why Do We Need An SDLC?


Software Development Life Cycle
1
Planning
2
Analysis
3
Design
4
Implementation
5
Testing & Integration
6
Maintenance

Question or clarifications?

QUESTIONS?

Review Day 3

Preview Week 3