Introduction to Software Development

Week 2 Day 4

Led by: Emily Crose

for

Oakland University

Last Session Recap


Questions From Last Session?

Terms To Listen For

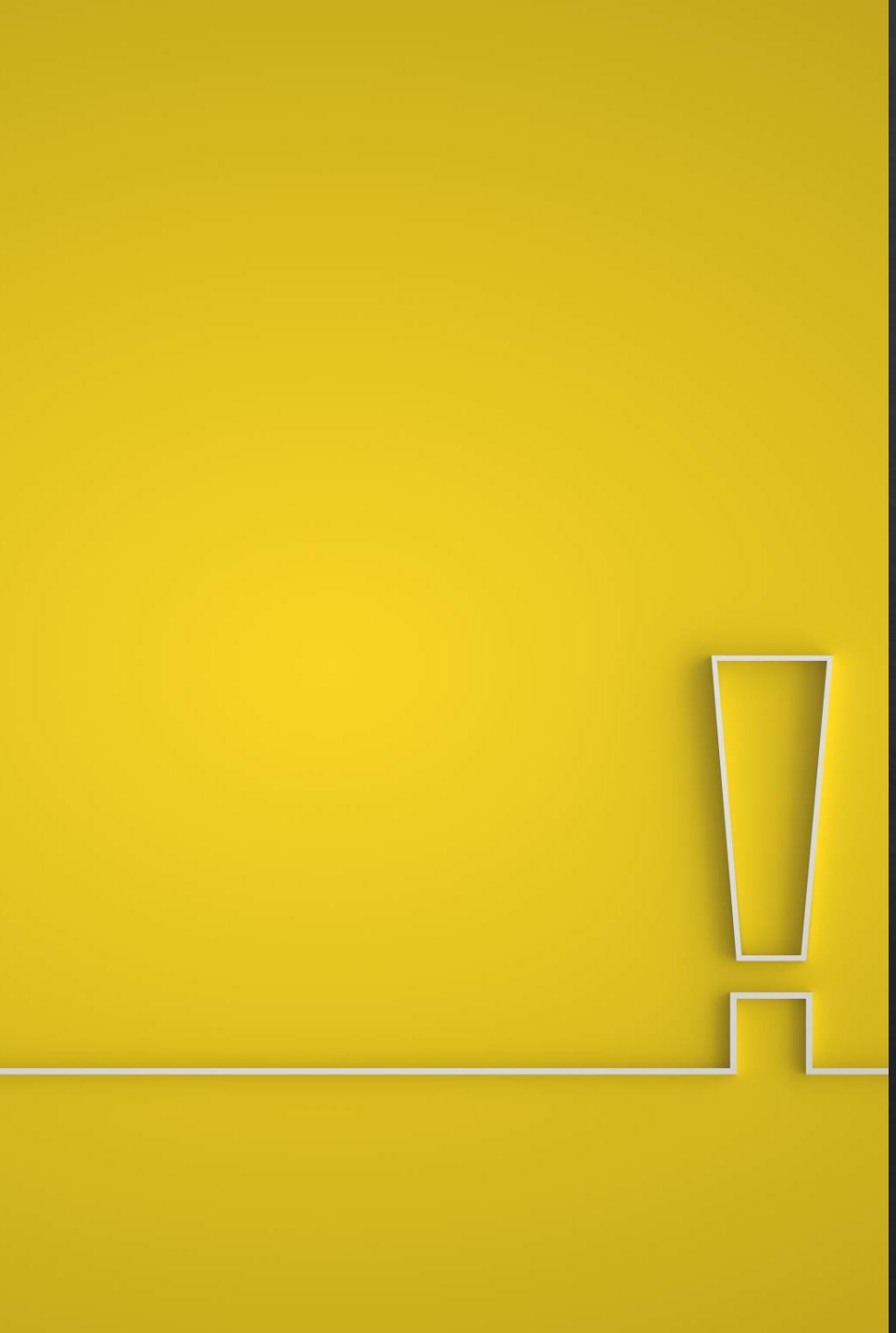
- Discretionary Access Control (DAC)
  - A method of access control provisioned by an administrator
- Mandatory Access Control (MAC)
  - Access control provisioned by data labeling
- Authentication
  - Refers to the process of verifying a user's identity.
- Denial of Service
  - A forced outage of a service based on a misconfiguration or a concerted effort

Anatomy of a Vulnerability

- Missing data encryption
- Arbitrary Code Injection
- SQL Injection
- Buffer Overflow
- Lack of authorization/authorization circumvention
- Unrestricted upload
- Unvalidated inputs
- Supply-Chain attacks

Arbitrary Code Execution

- Mishandled execution permissions can lead to arbitrary code execution
  - Remote Code Execution (RCE)
  - Privilege Escalation (Privesc)

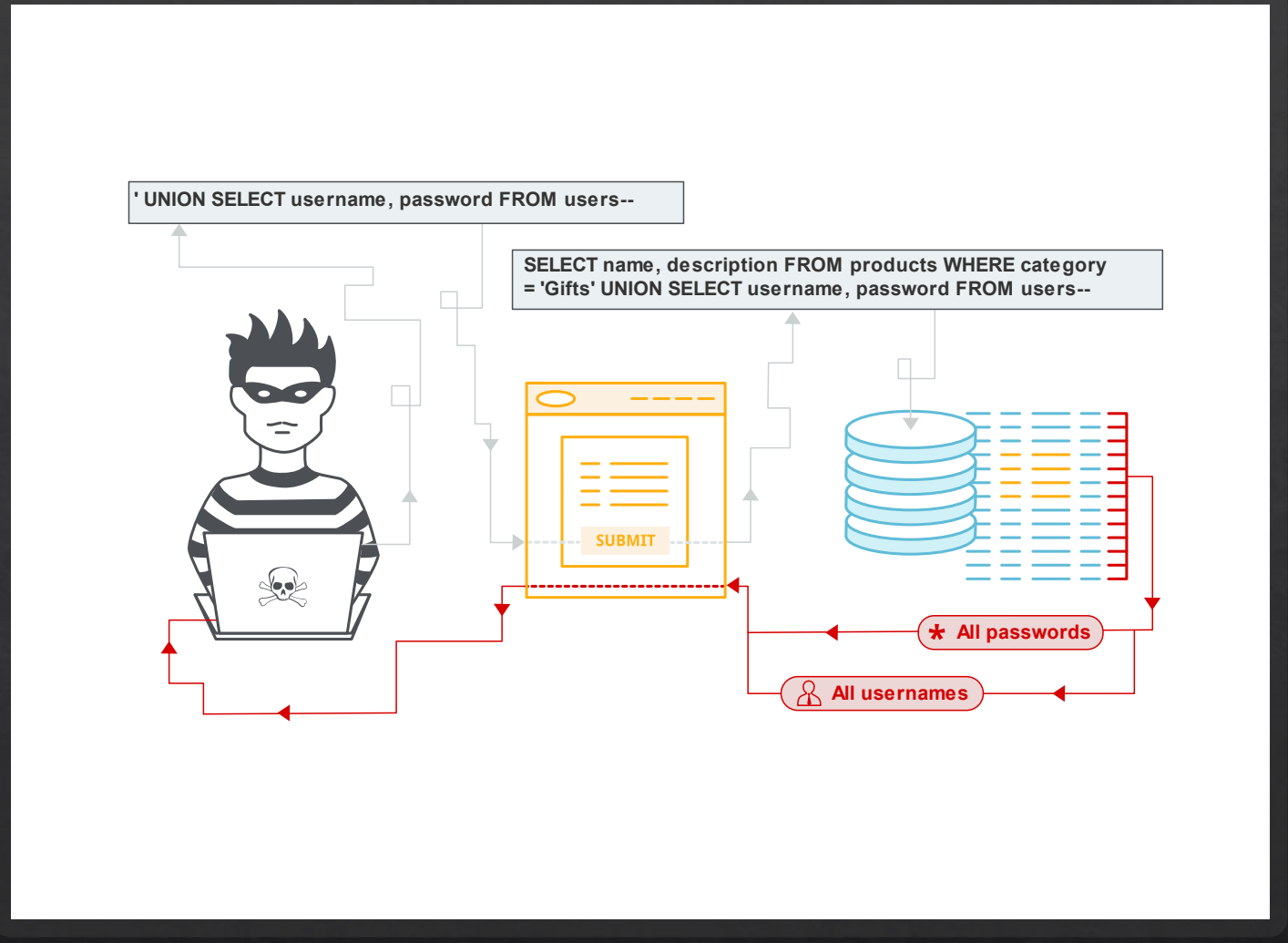


Missing Data Encryption

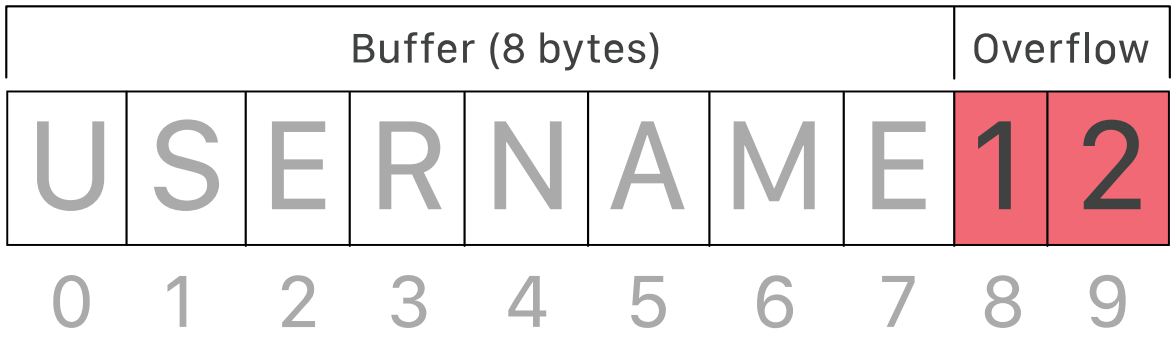
Readable traffic!

SQL Injection

- Allows Databases to be read without authorization
- Can be caused by a lack of input validation



Buffer Overflow

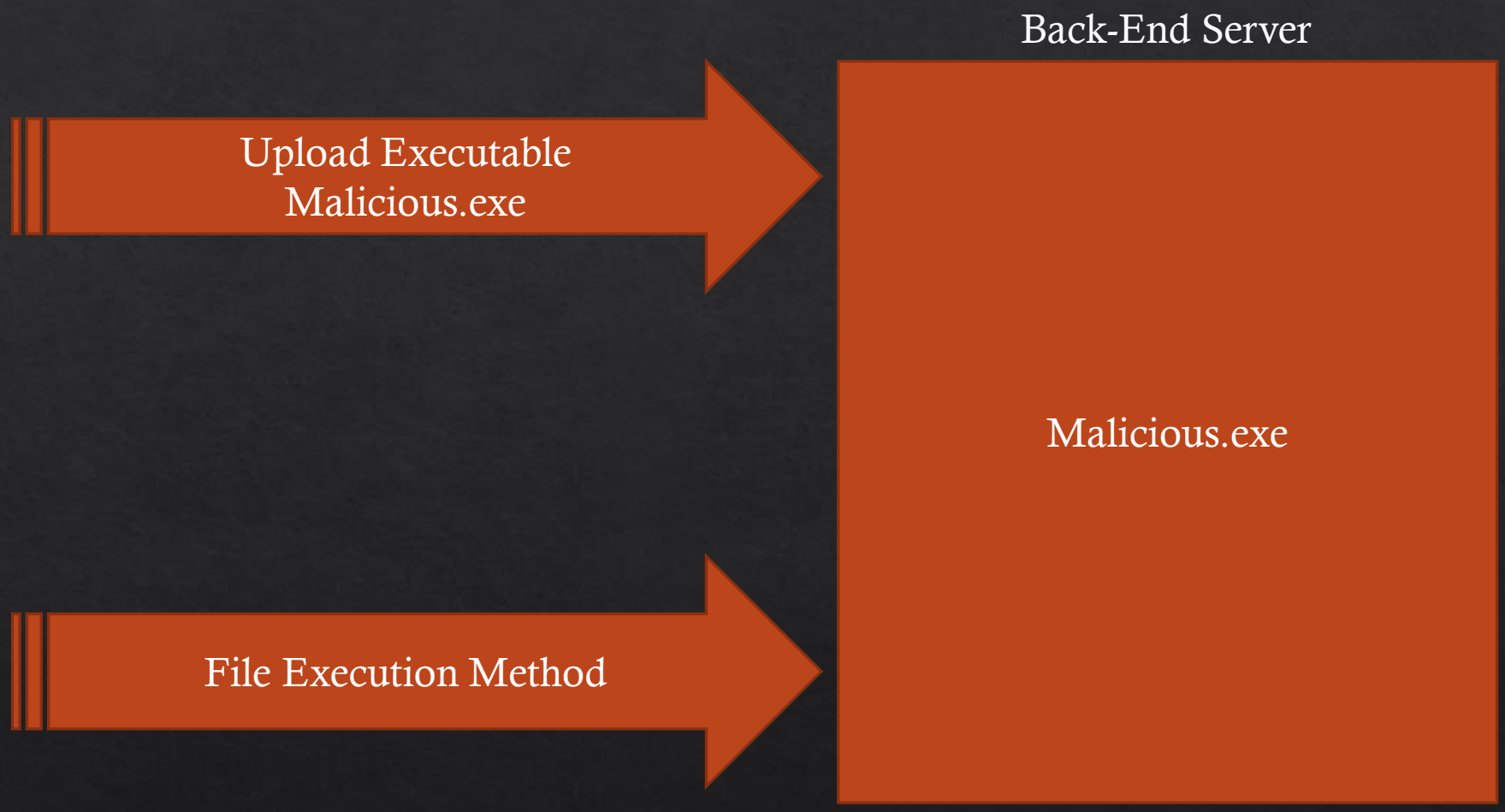


Unrestricted Upload

- May allow users to upload files or filetypes that shouldn't be allowed.
  - Suppose we allow users to upload image files like .jpg, but we don't validate input. This may lead to the upload of executable code to our back-end.

Does This Mean We’re Breached?

- Not yet!


Back-End Server
Upload Executable
Malicious.exe
Malicious.exe
File Execution Method

Supply-Chain Attacks

- Sneak malicious code into our codebase?
  - Physically?
    - Insider threat?
  - Spoofed code-signing certificate?
  - Compromise legitimate user?

Common Vulnerabilities and Exposures (CVEs)

CVE-ID

CVE-2017-0144

Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

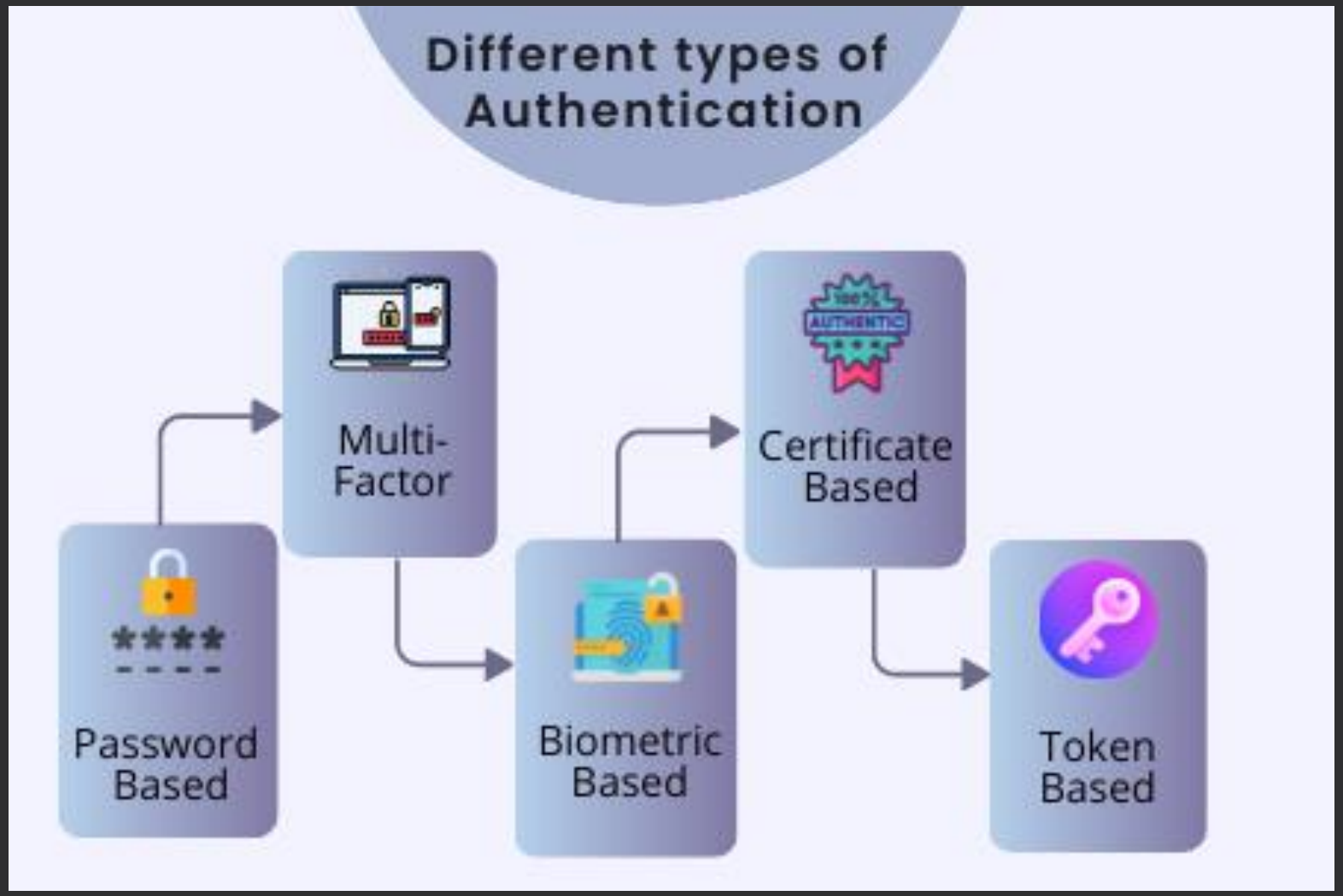
The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0143, CVE-2017-0145, CVE-2017-0146, and CVE-2017-0148.

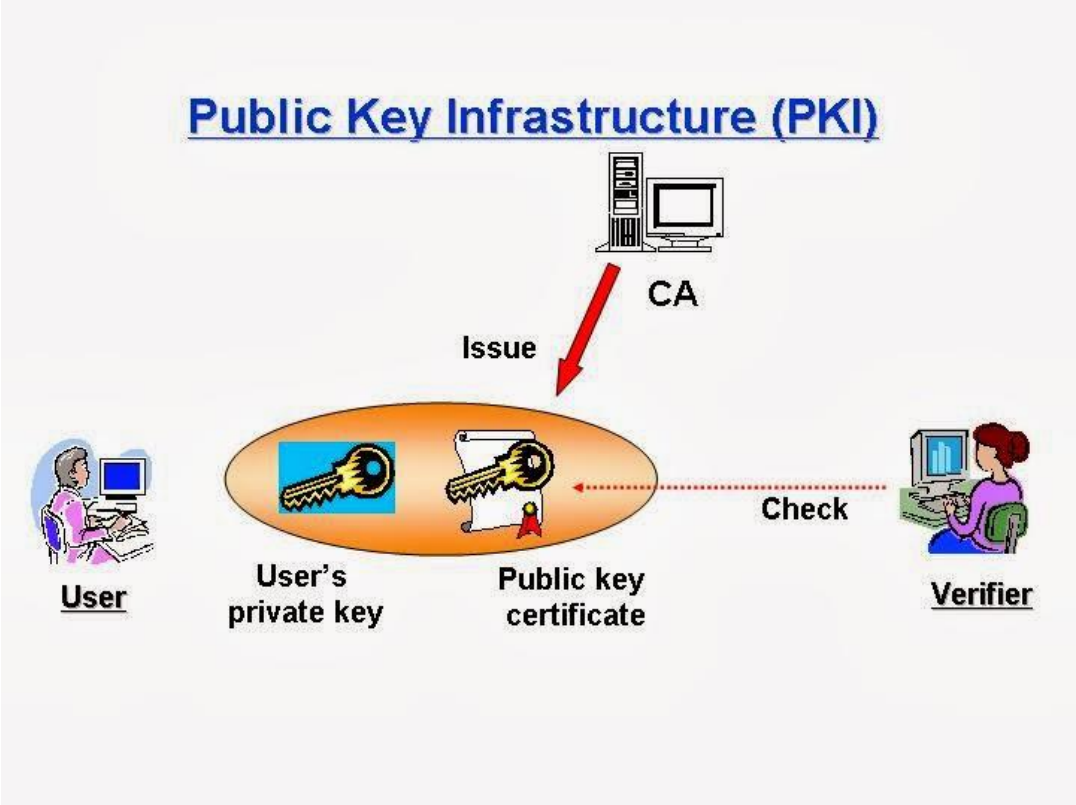
References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- BID:96704
- URL:http://www.securityfocus.com/bid/96704
- CONFIRM:https://cert-portal.siemens.com/productcert/pdf/ssa-701903.pdf
- CONFIRM:https://cert-portal.siemens.com/productcert/pdf/ssa-966341.pdf
- CONFIRM:https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0144
- EXPLOIT-DB:41891
- URL:https://www.exploit-db.com/exploits/41891/
- EXPLOIT-DB:41987
- URL:https://www.exploit-db.com/exploits/41987/
- EXPLOIT-DB:42030
- URL:https://www.exploit-db.com/exploits/42030/
- EXPLOIT-DB:42031
- URL:https://www.exploit-db.com/exploits/42031/
- MISC:http://packetstormsecurity.com/files/154690/DOUBLEPULSAR-Payload-Execution-Neutralization.html
- MISC:http://packetstormsecurity.com/files/156196/SMB-DOUBLEPULSAR-Remote-Code-Execution.html
- MISC:https://ics-cert.us-cert.gov/advisories/ICSMA-18-058-02
- SECTRACK:1037991
- URL:http://www.securitytracker.com/id/1037991

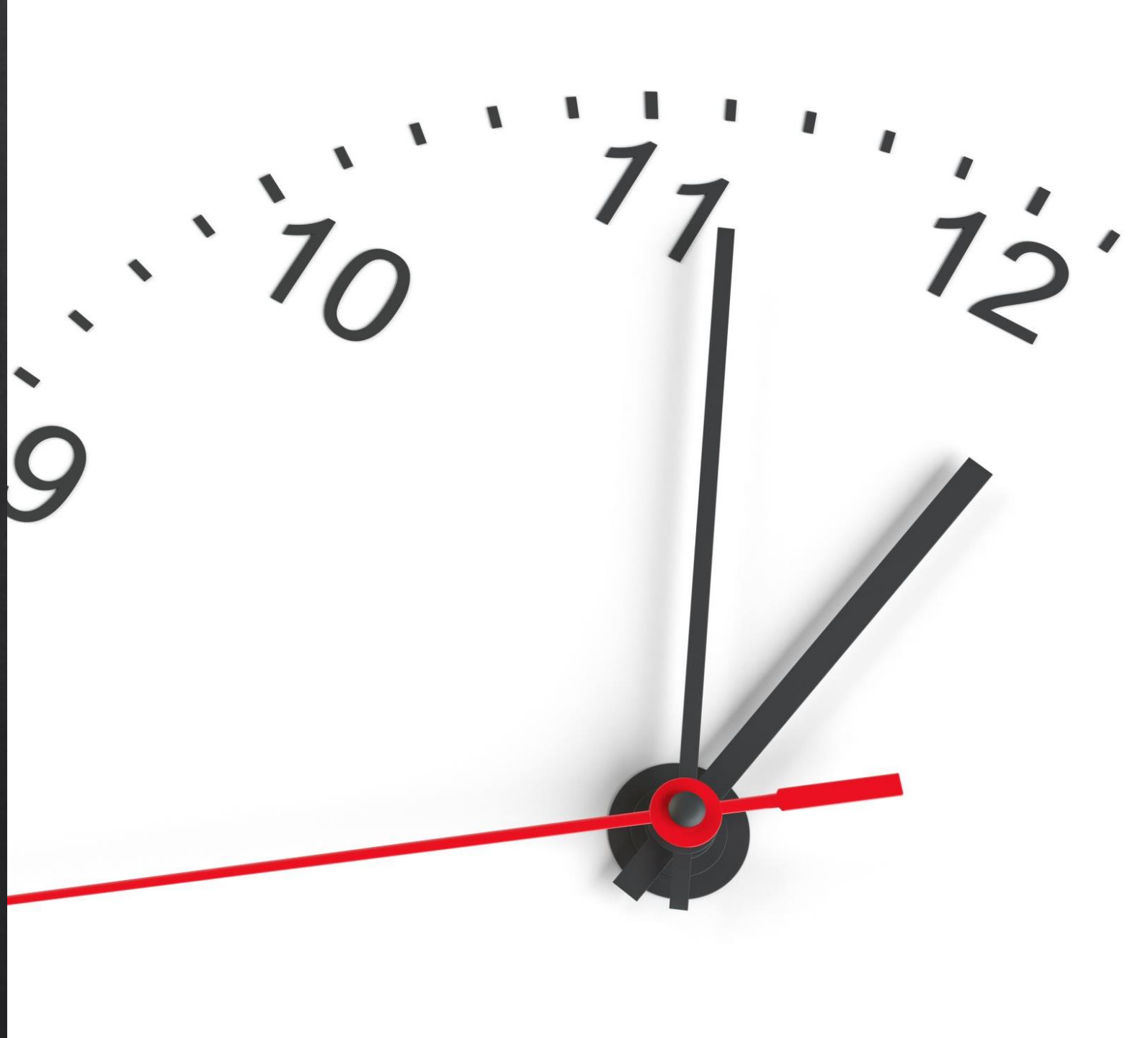
Authentication

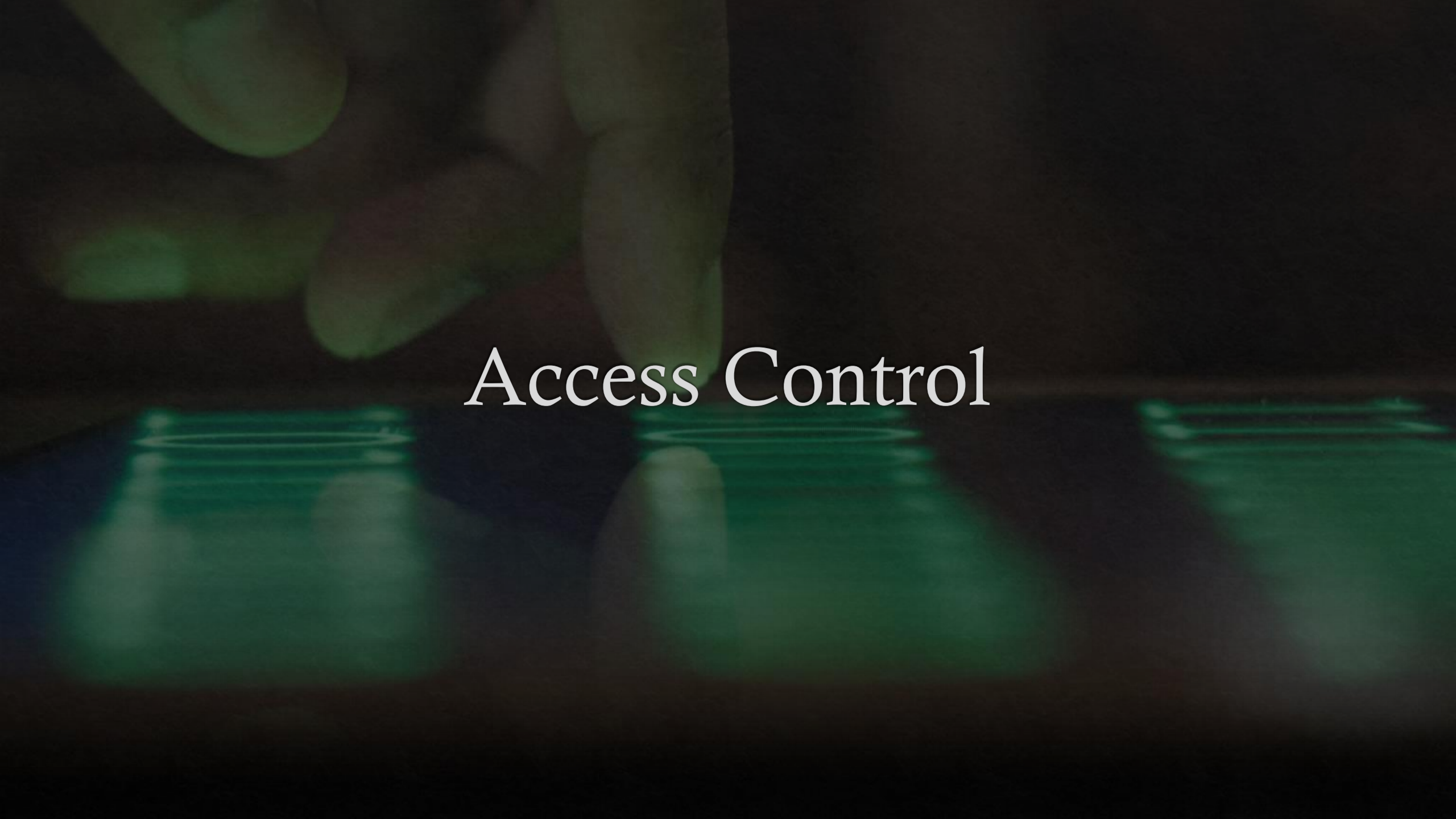

Different types of Authentication
Multi-Factor
Certificate Based
Password Based
Biometric Based
Token Based



Public Key Infrastructure (PKI)

10-minute break

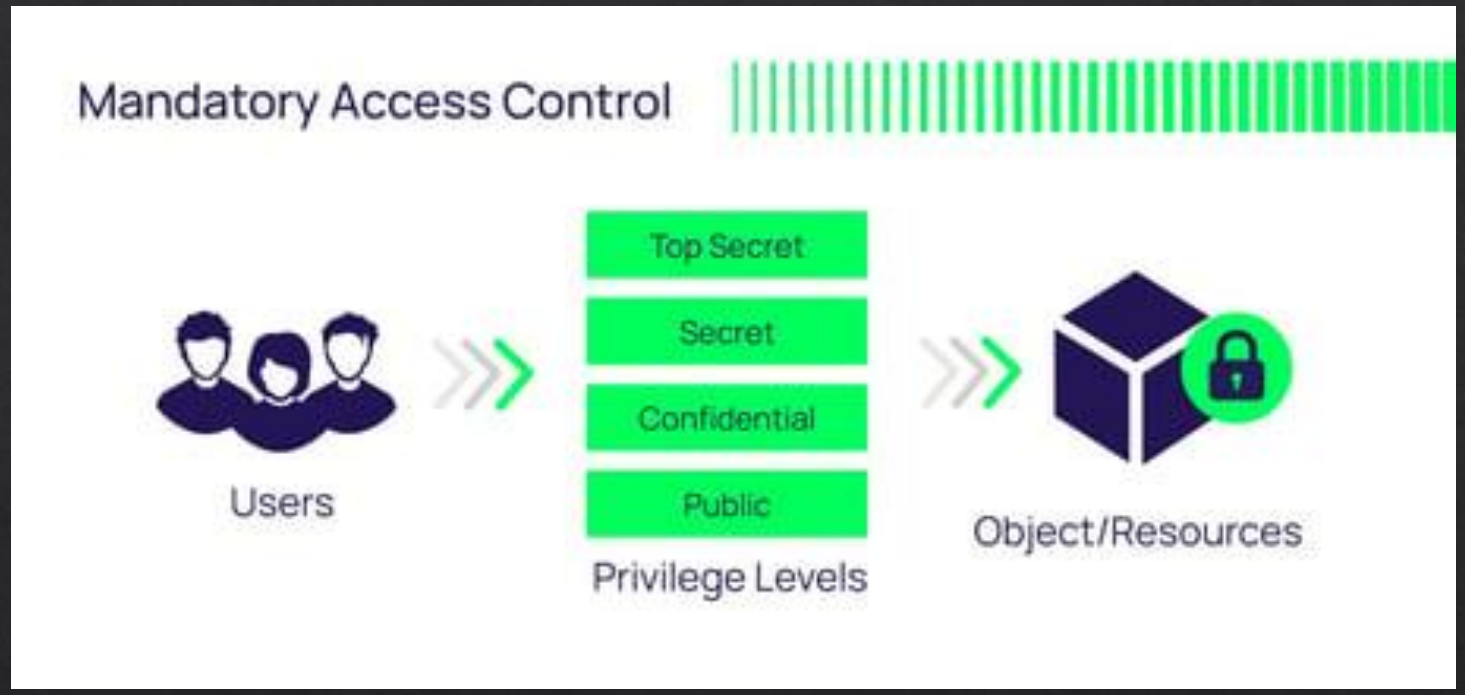




Access Control

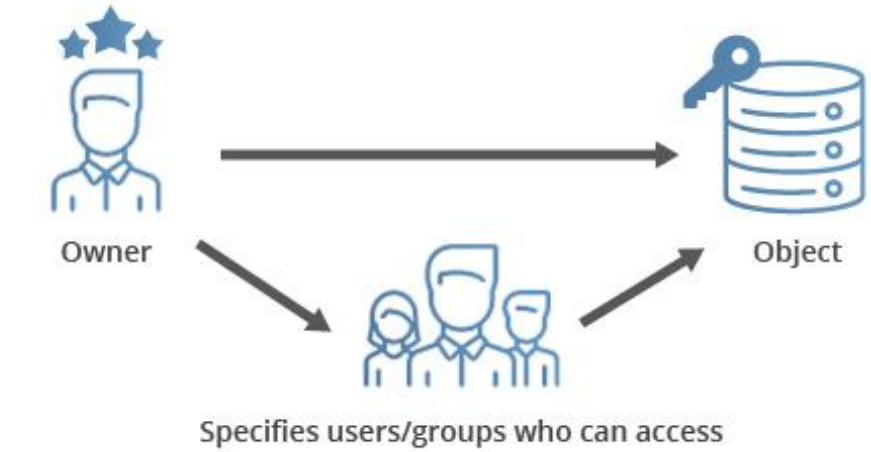
MAC, DAC, and RBAC

Mandatory Access Control

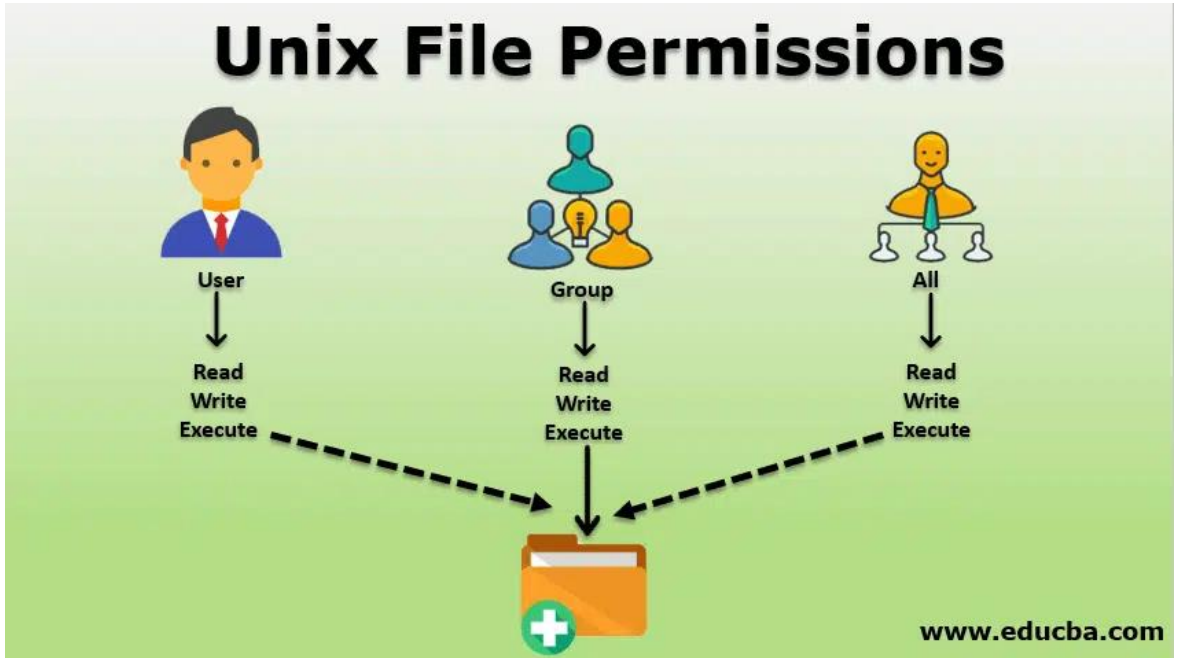


Mandatory Access Control (MAC)

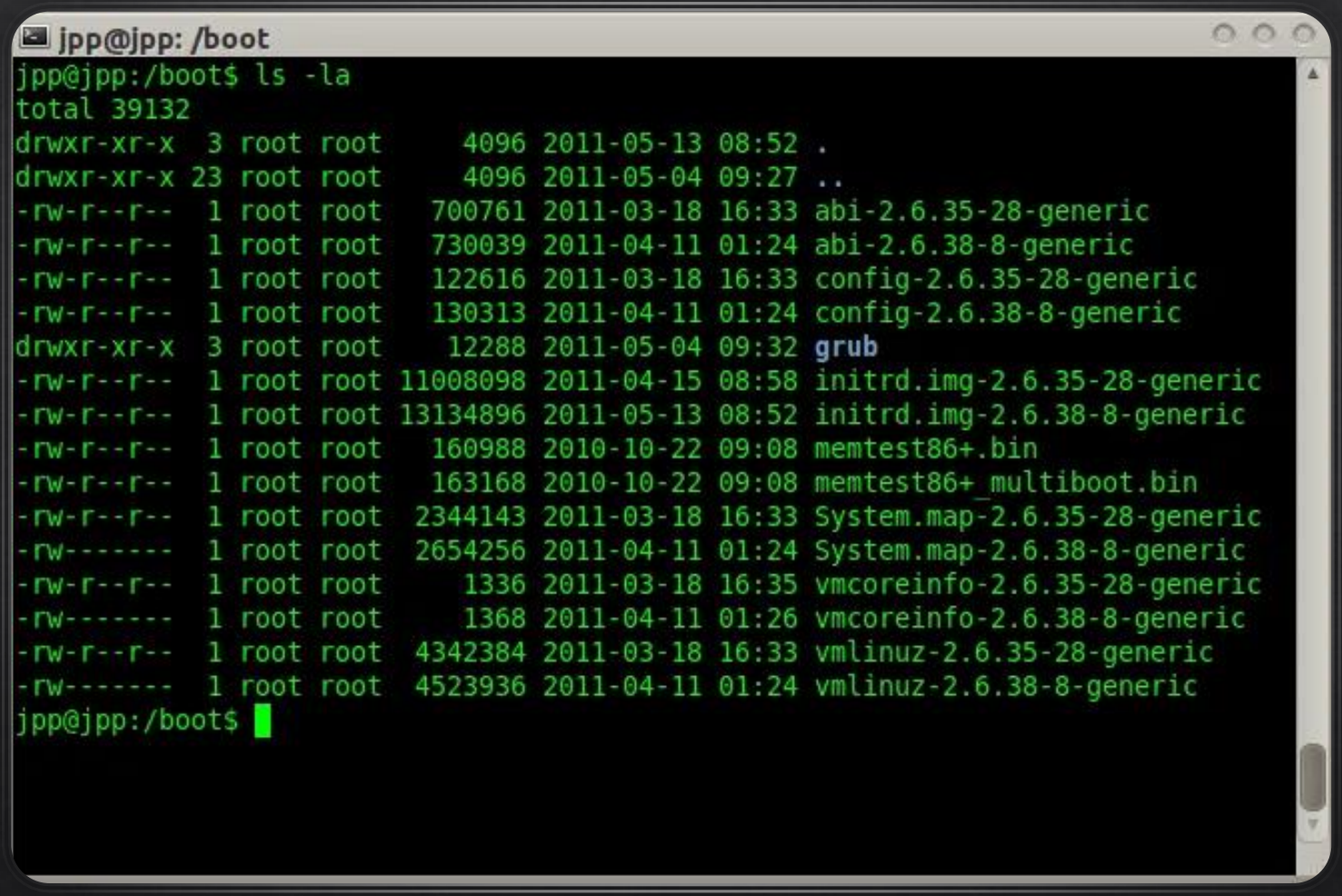
Discretionary Access Control (DAC)


Discretionary Access Control (DAC)
Owner
Object
Specifies users/groups who can access

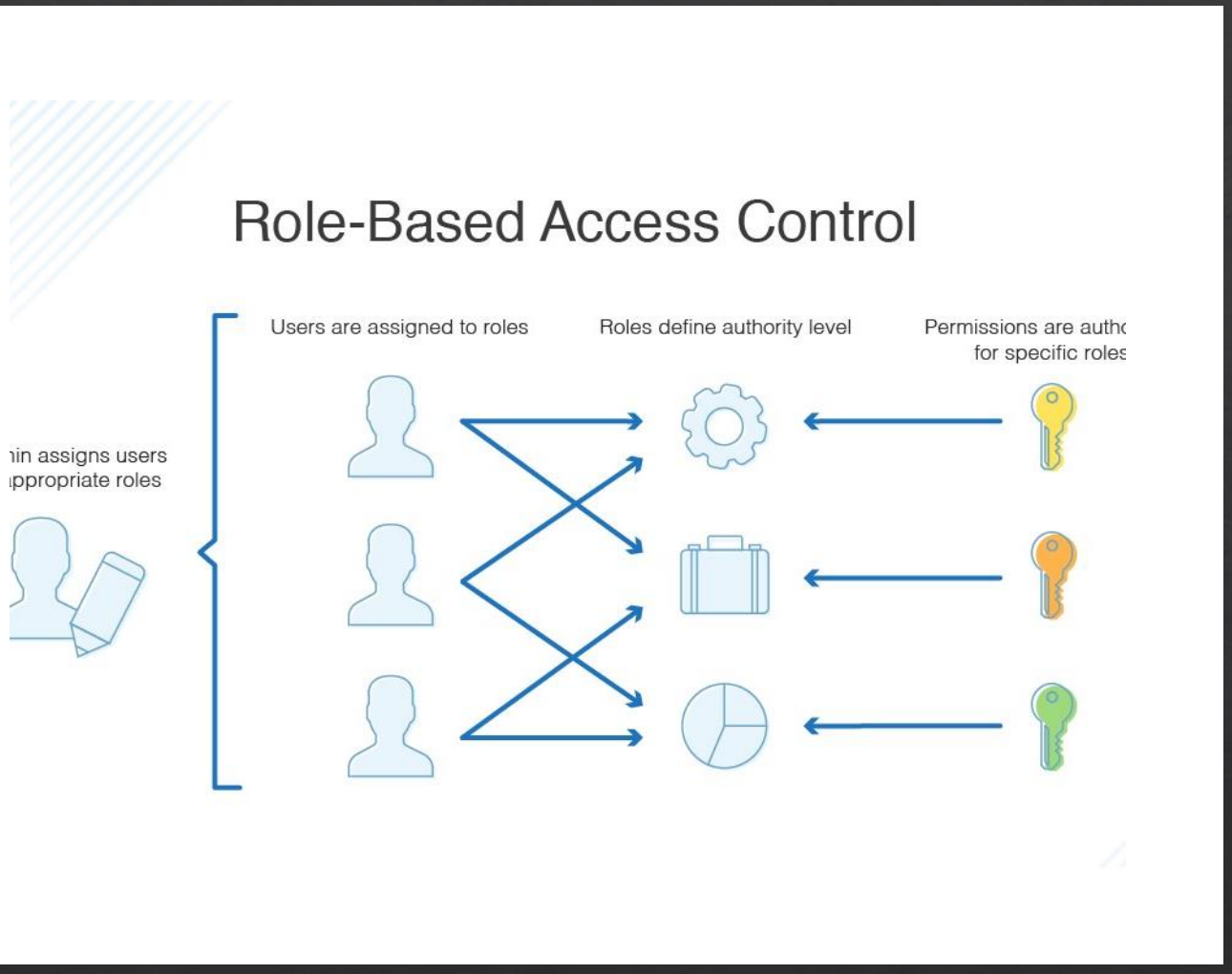
DAC



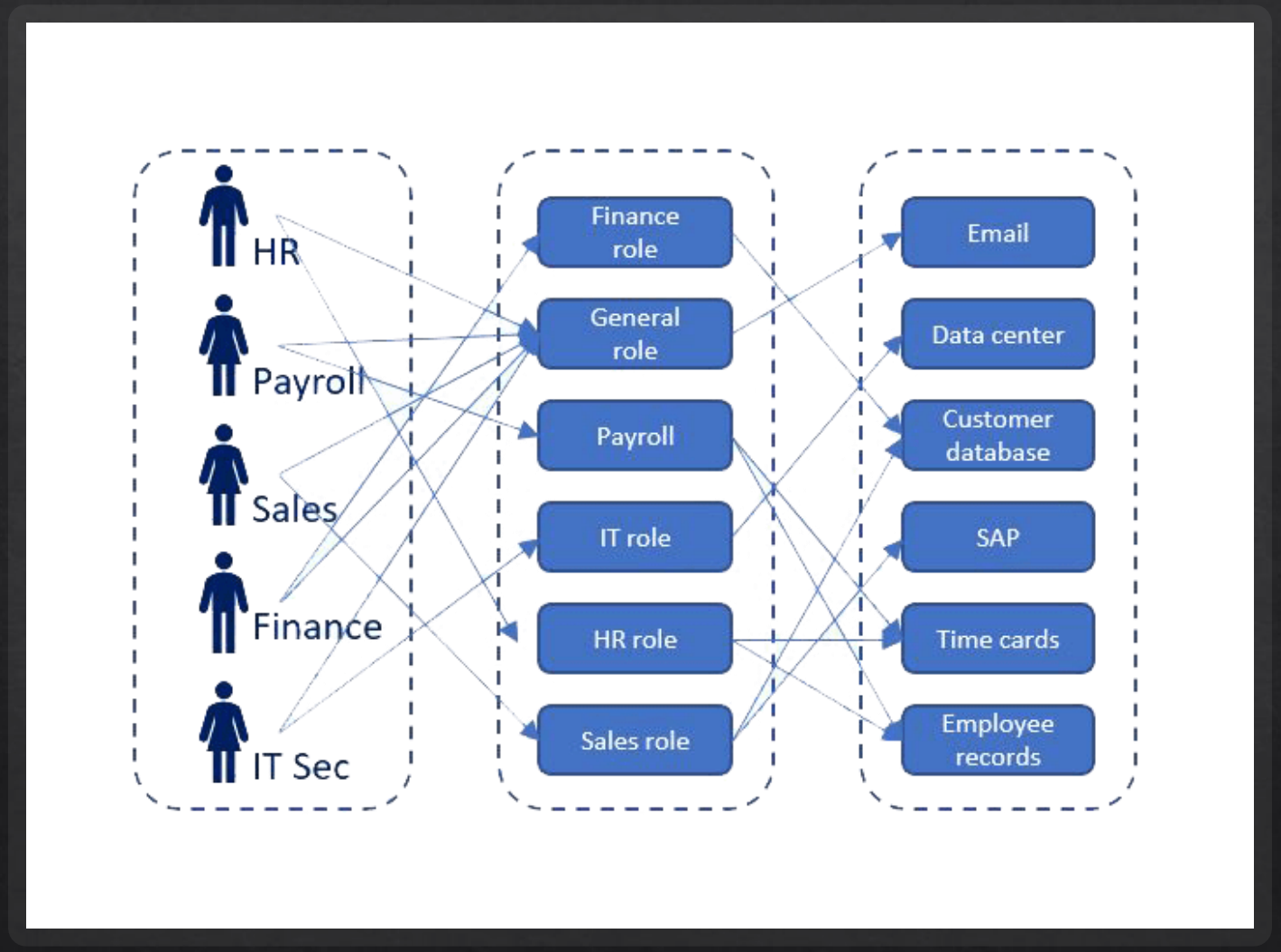
DAC In Action



Linux permissions in practice



Role Based Access Control (RBAC)



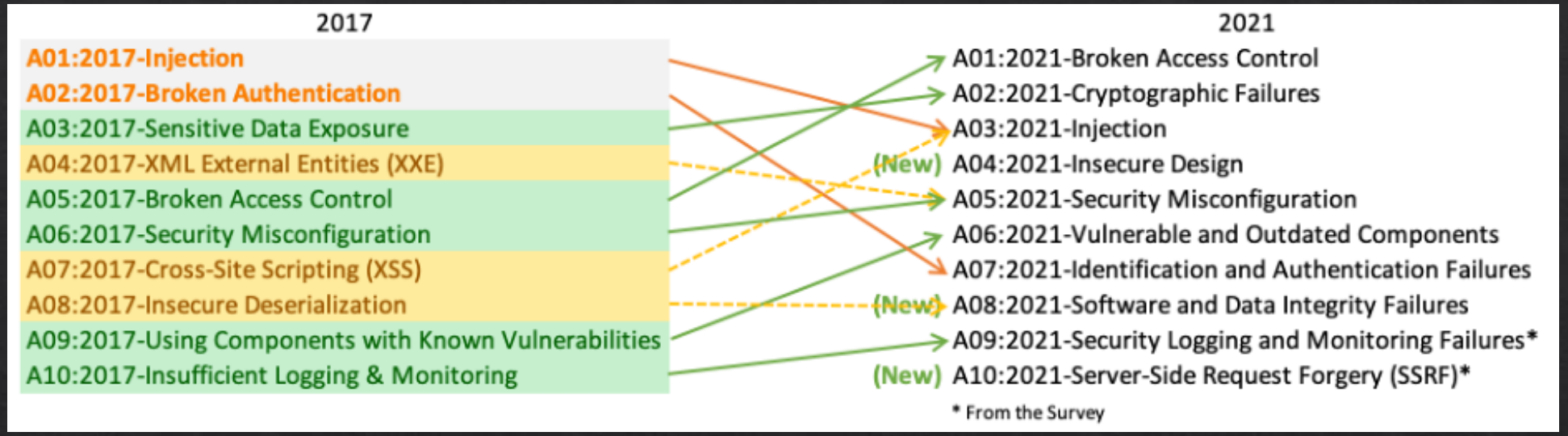
RBAC In Action

Pentesting Methodology


01
Passive Reconnaissance
02
Active Reconnaissance
03
Social Engineering
04
Exploitation
05
Post Exploitation
06
Privilege Escalation
07
Lateral Movement
08
Maintain Access
09
Cover Tracks
10
Reporting
OCDTECH

Standards

OWASP

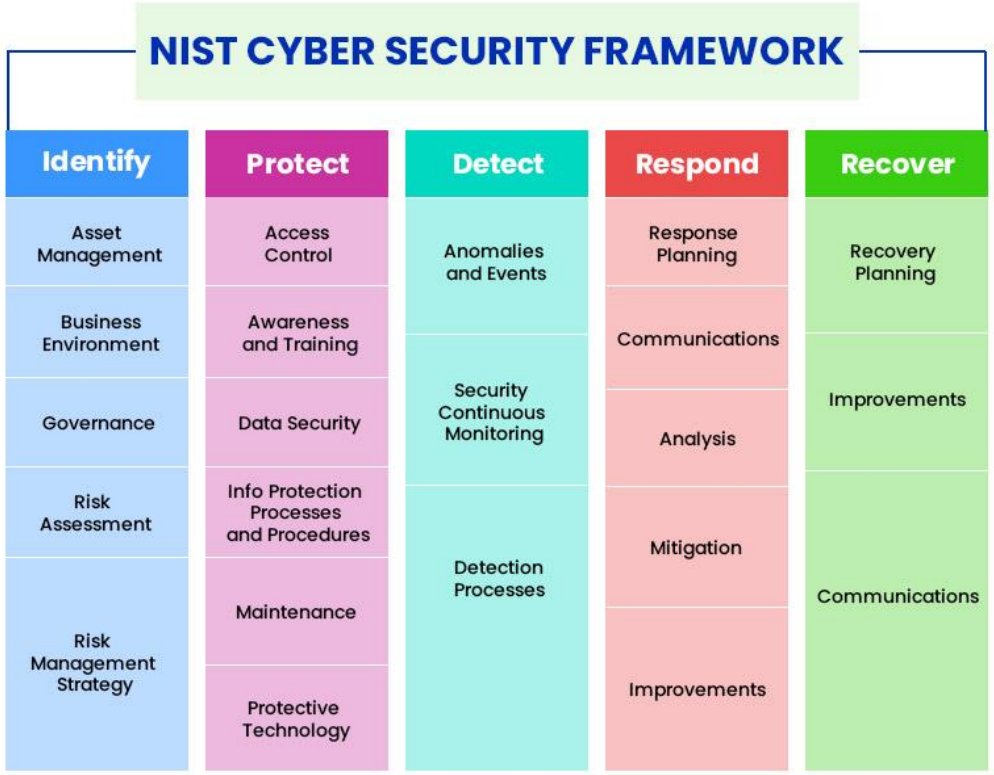

2017
A01:2017-Injection
A02:2017-Broken Authentication
A03:2017-Sensitive Data Exposure
A04:2017-XML External Entities (XXE)
A05:2017-Broken Access Control
A06:2017-Security Misconfiguration
A07:2017-Cross-Site Scripting (XSS)
A08:2017-Insecure Deserialization
A09:2017-Using Components with Known Vulnerabilities
A10:2017-Insufficient Logging & Monitoring
2021
A01:2021-Broken Access Control
A02:2021-Cryptographic Failures
A03:2021-Injection
(New) A04:2021-Insecure Design
A05:2021-Security Misconfiguration
A06:2021-Vulnerable and Outdated Components
A07:2021-Identification and Authentication Failures
(New) A08:2021-Software and Data Integrity Failures
A09:2021-Security Logging and Monitoring Failures*
(New) A10:2021-Server-Side Request Forgery (SSRF)*
* From the Survey

OWASP Top 10

Mobile Application Security Verification Standard (MASVS)

https://github.com/OWASP/owasp-masvs/


NIST
National Institute of
Standards and Technology



NIST Cybersecurity Framework

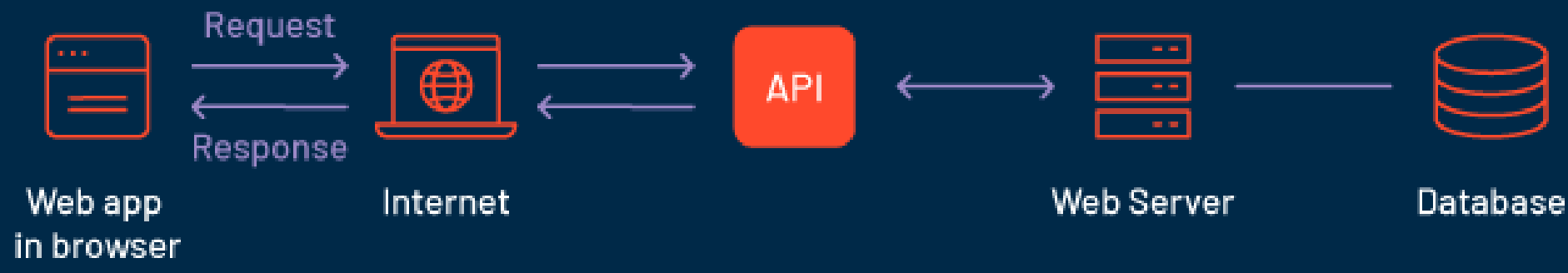
Application Programming Interface (APIs)

Application Programming Interfaces (APIs)

What do they do for applications?

When would we want to use an API?

How Do APIs Work



API

End User *with Browser*

Request

Response

Server *Back-end System*

Customer

Make the Order

Delivery of order

Waiter

Take the Order

Bringing from Kitchen

Chef

Common API Protocols

Representational State Transfer (REST or RESTful) API

Fast

Reliable

Widely adopted

Simple!

Simple Object Access Protocol (SOAP)

Used in some OT network appliances

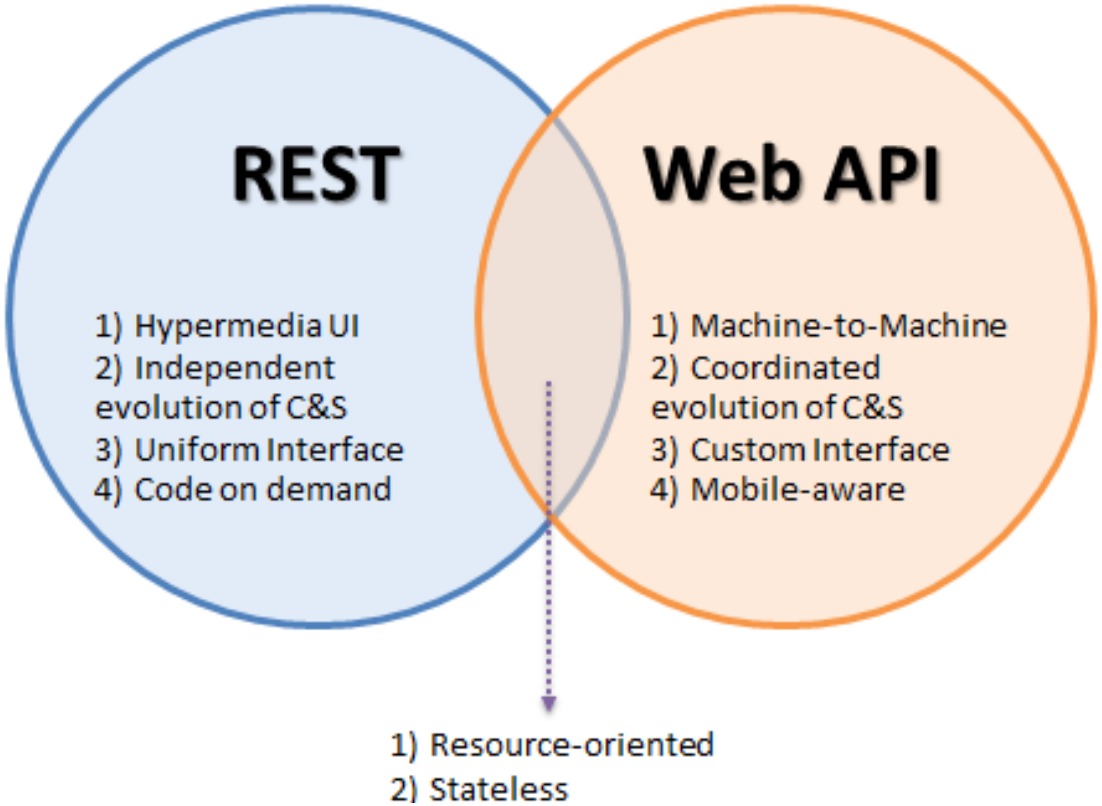
Browser API

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"
    }
  ]
}
```



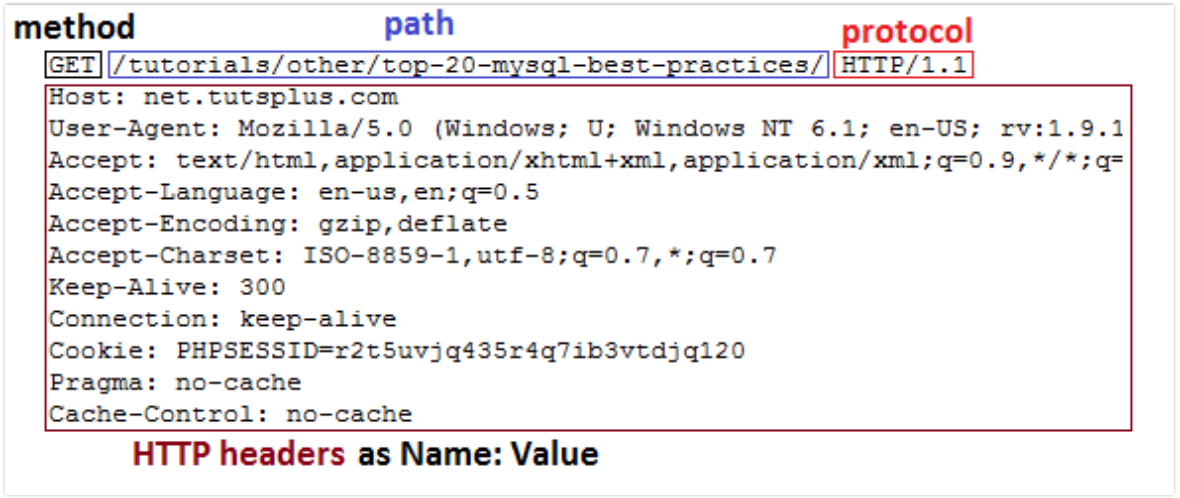
API Similarities

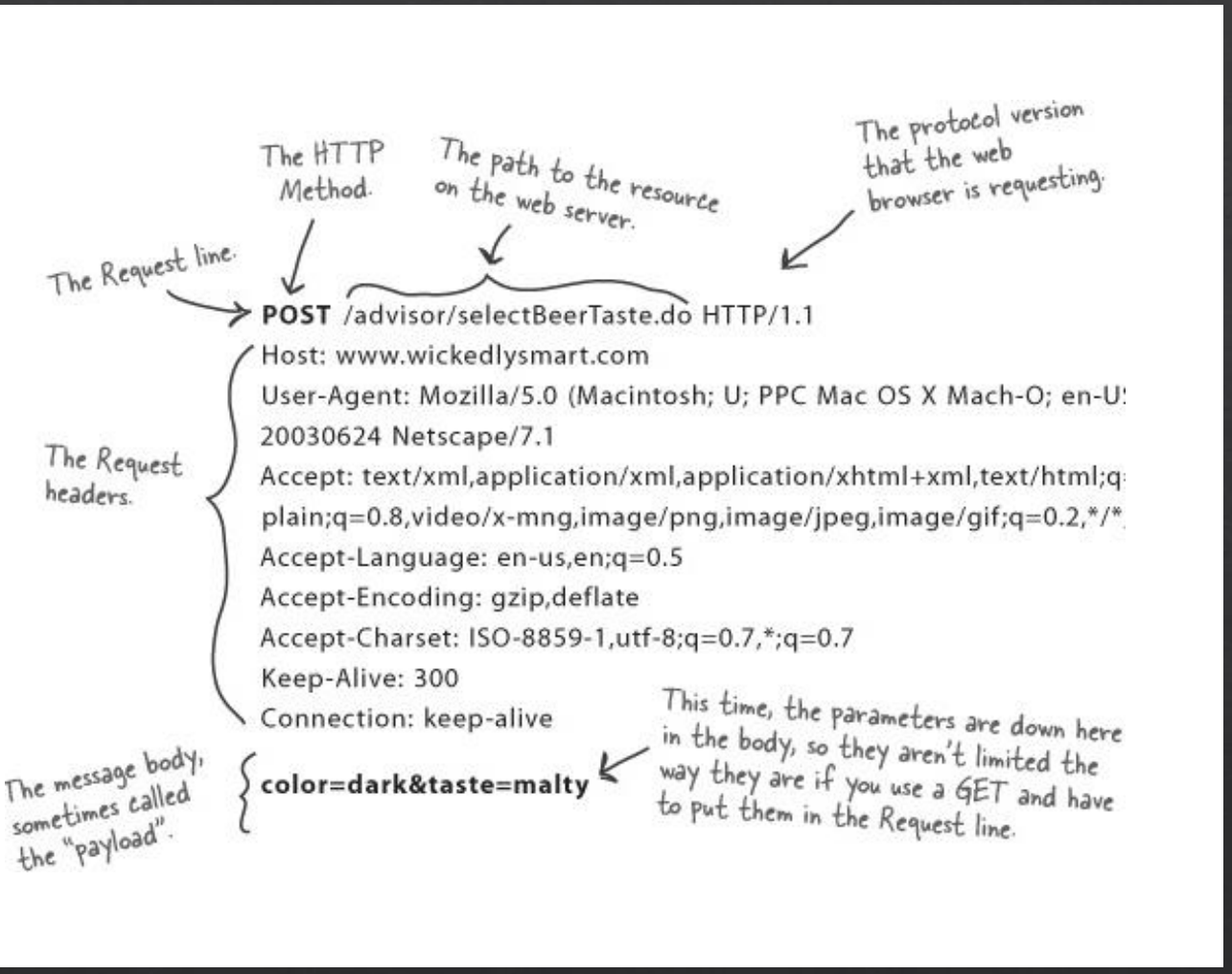

HTTP/Web API

HTTP API Verbs

- HTTP
  - GET
  - POST
  - PUT
  - DELETE

HTTP GET Header





HTTP POST Header

WEATHER API DOCUMENTATION

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

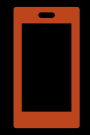
(Node.js) Axios Copy Code

```
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

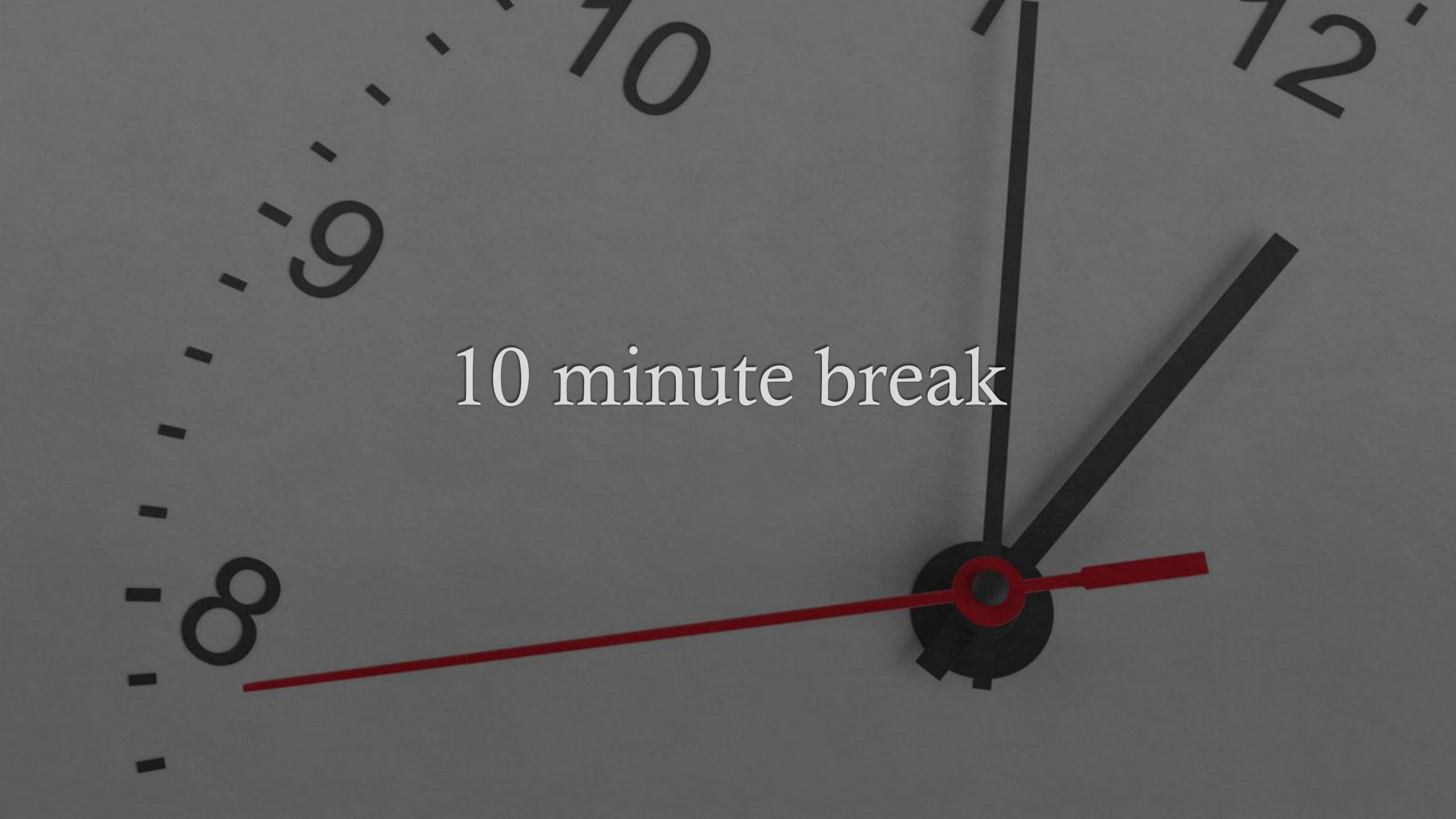
Both have access to device APIs!

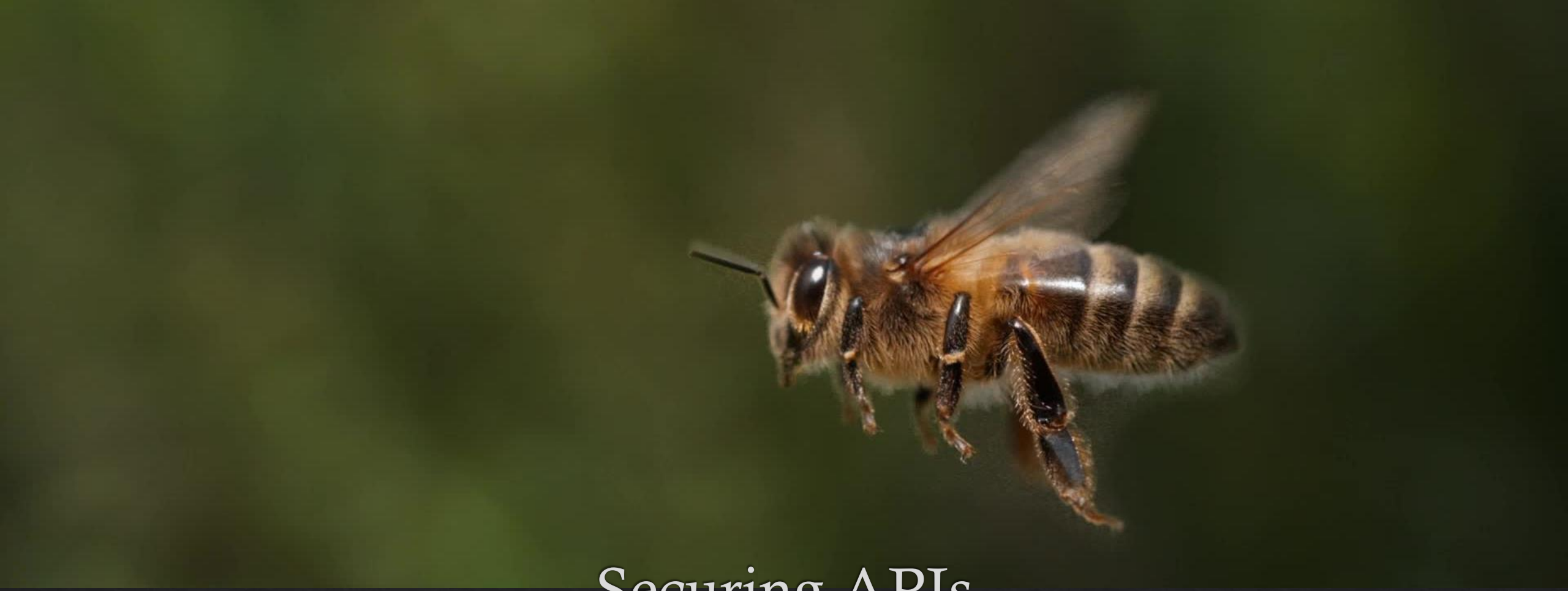
Mobile APIs vs. Web APIs

- Camera Roll
- Sensor inputs
  - Gyroscope
  - Geolocation

{"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}

Mobile Device API Example


10 minute break



Securing APIs

SAML vs. Oauth

Security Assertion Markup Language (SAML)	Windows uses this for Single Sign On (SSO) Integrates with Windows domain Optimized for enterprise security
Oauth	Optimized for mobile applications Uses API calls itself! Tends to play better with mobile & lightweight IoT environments

What is Oauth?

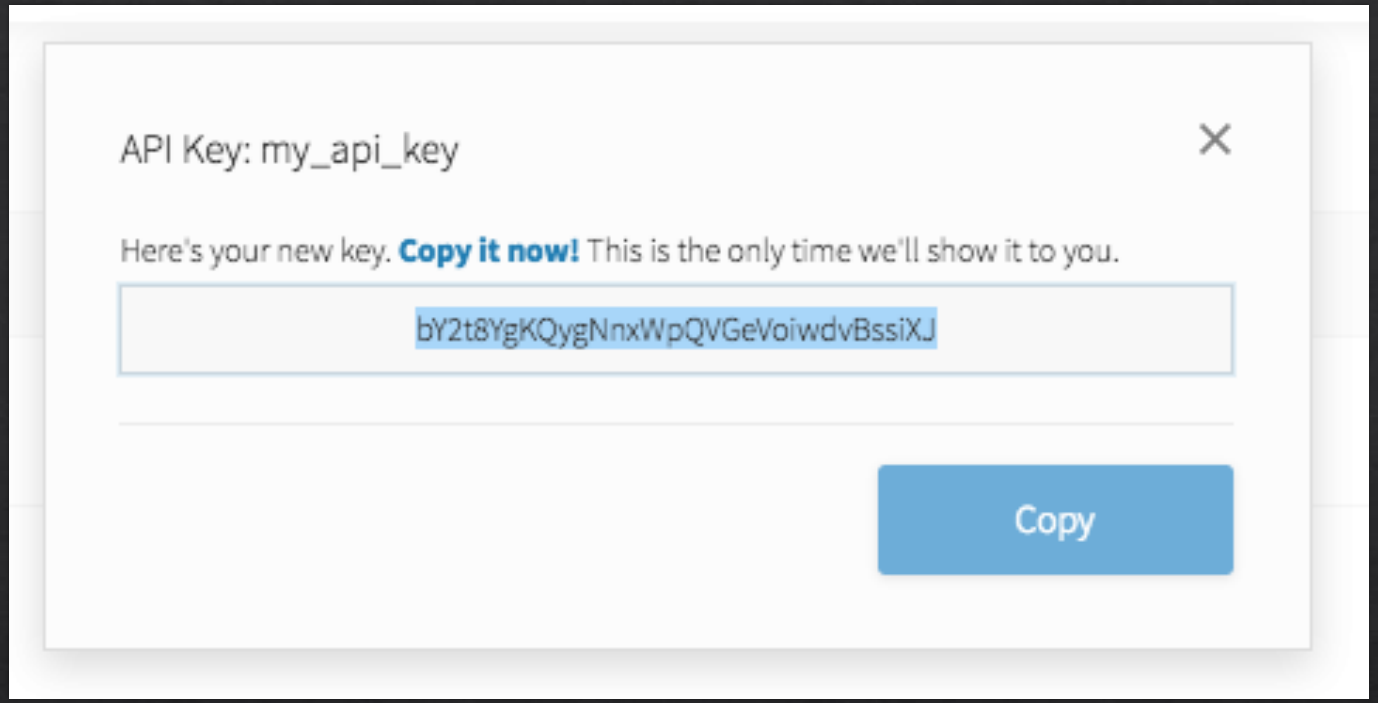
Oauth

Allows one application to validate itself with another application

Uses tokens for authentication

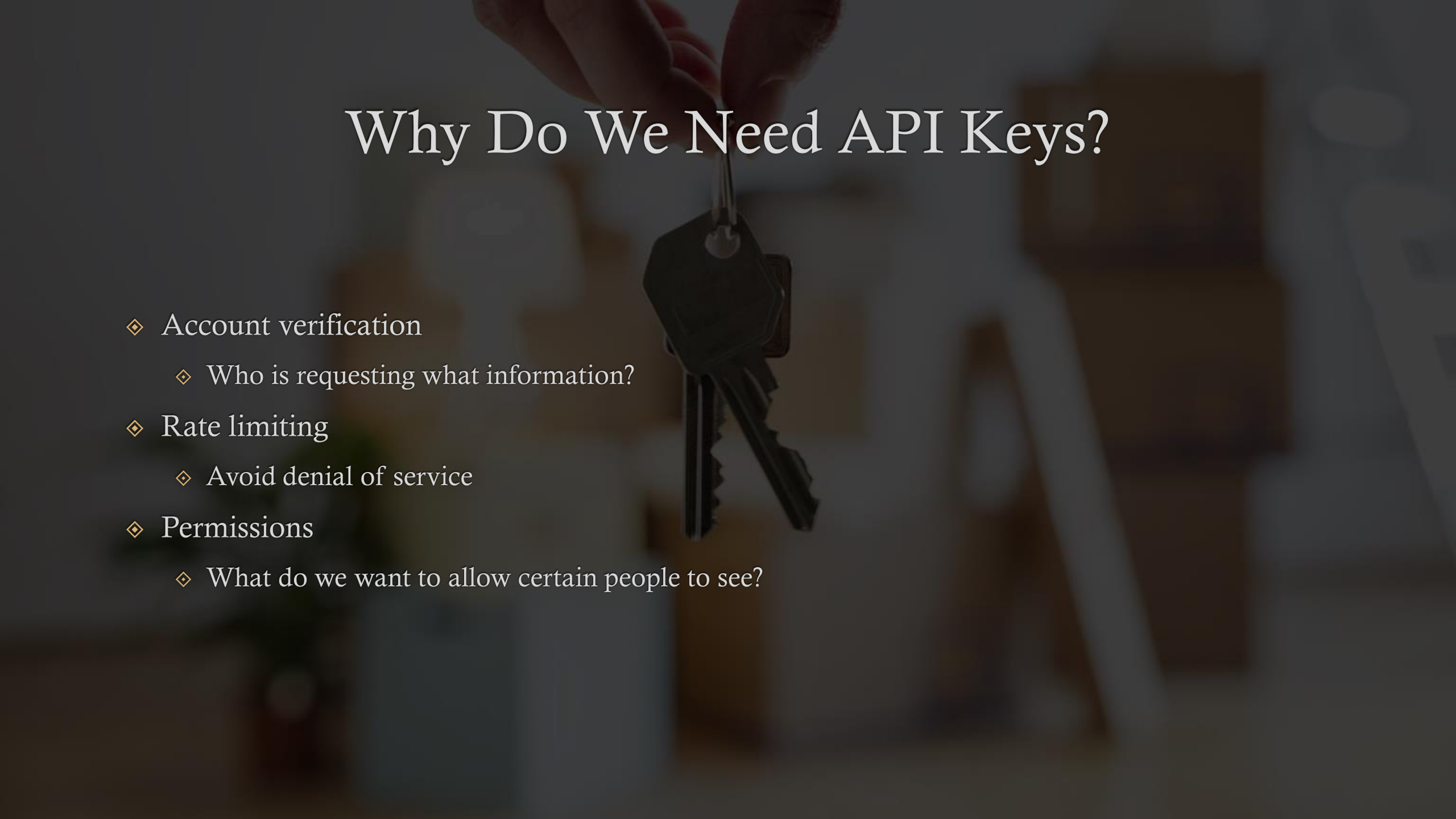
We give applications permission to play with other applications via Oauth

Think of it like a valet for your apps!

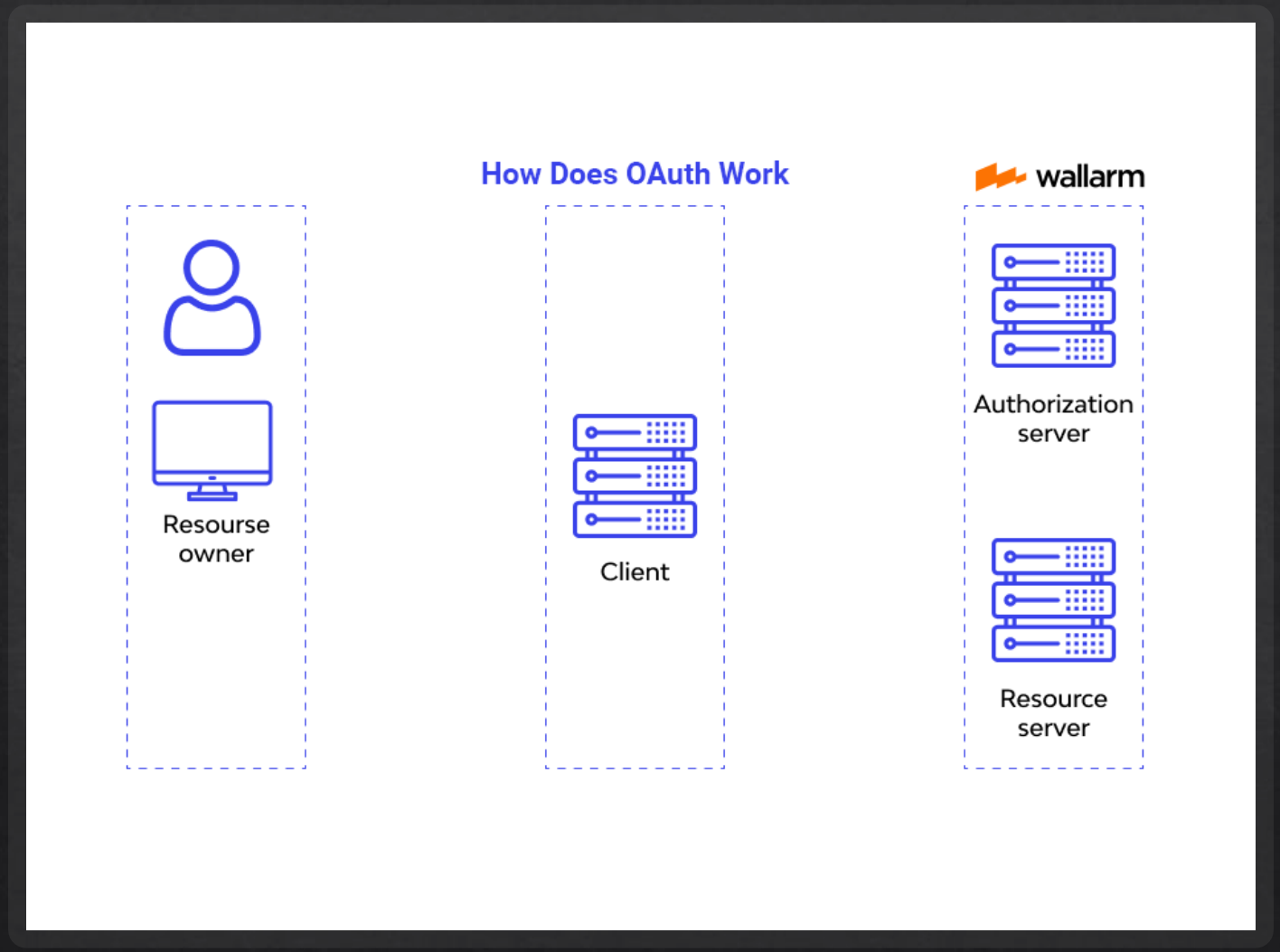

API Key: my_api_key
Here's your new key. Copy it now! This is the only time we'll show it to you.
bY2t8YgKQygNnxWpQVGeVoiwdvBssiXJ
Copy

API Key

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?



How does OAuth work?

Question or clarifications?

Review Day 3

Preview Week 3