

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

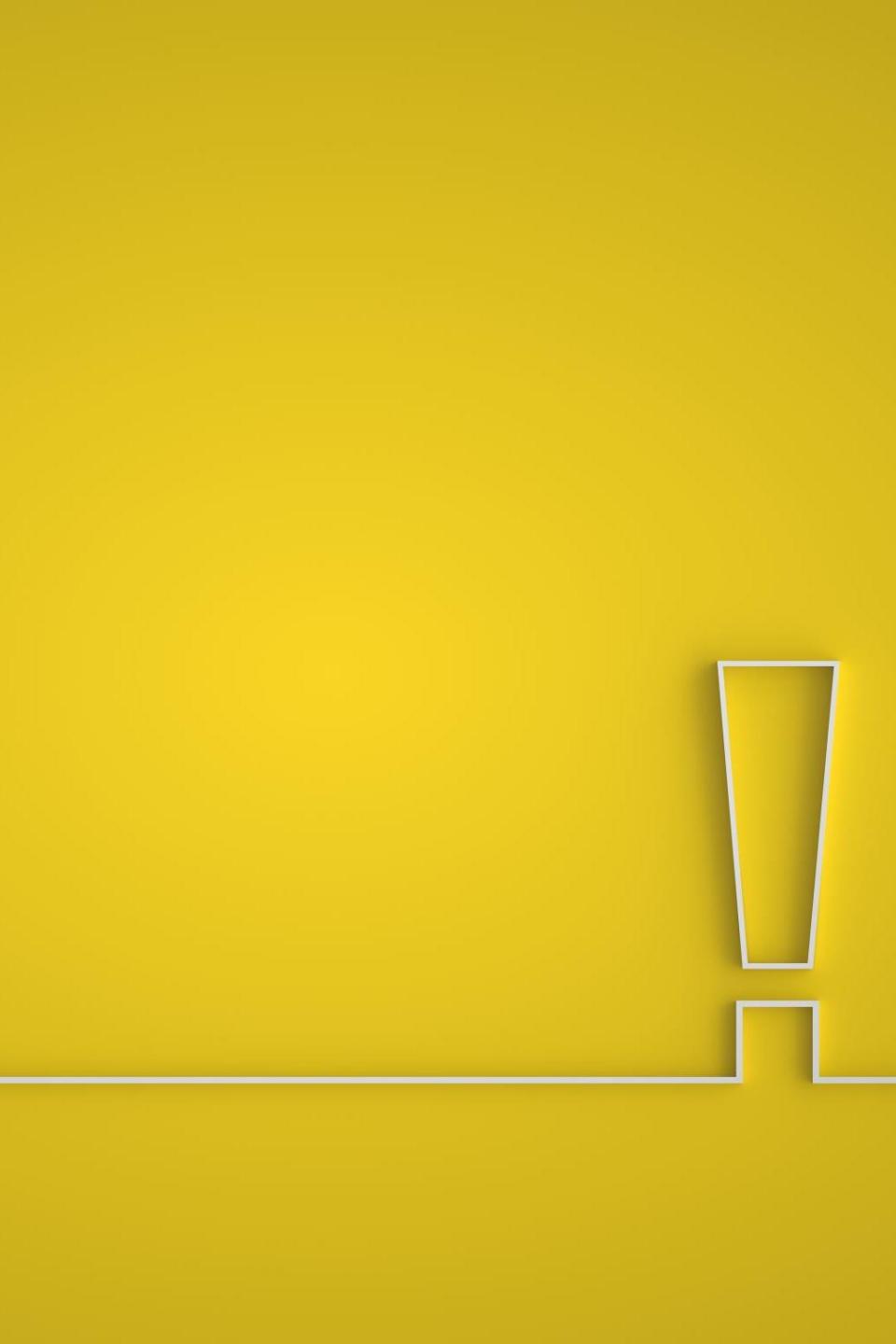
- ❖ Discretionary Access Control (DAC)
 - ❖ A method of access control provisioned by an administrator
- ❖ Mandatory Access Control (MAC)
 - ❖ Access control provisioned by data labeling
- ❖ Authentication
 - ❖ Refers to the process of verifying a user's identity.
- ❖ Denial of Service
 - ❖ A forced 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)

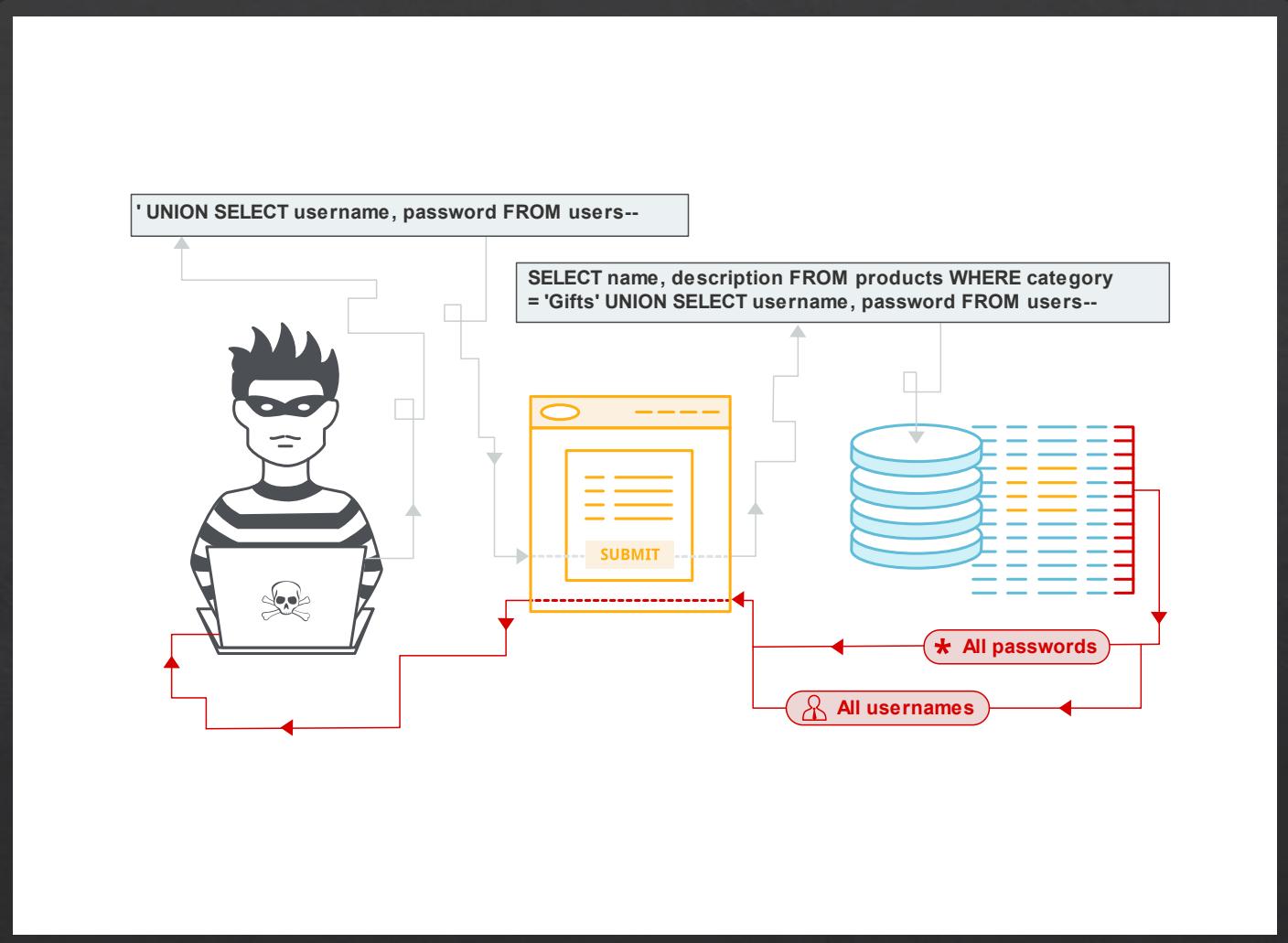


Missing Data Encryption

Readable traffic!

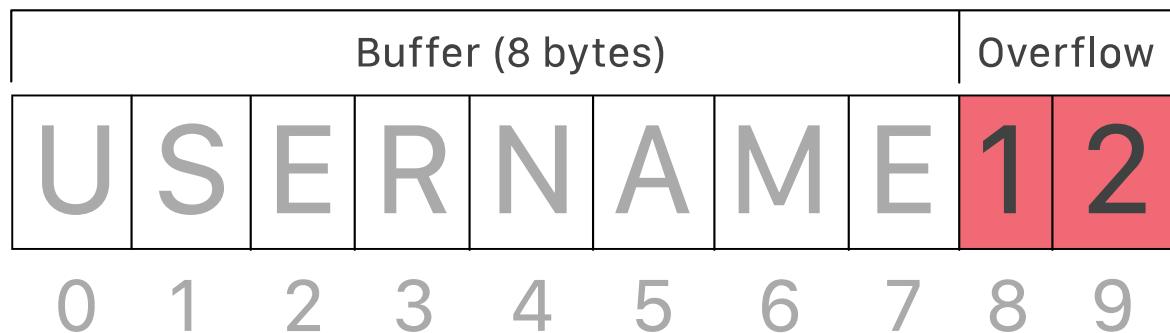
SQL Injection

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



Buffer Overflow

Buffer overflow example



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?

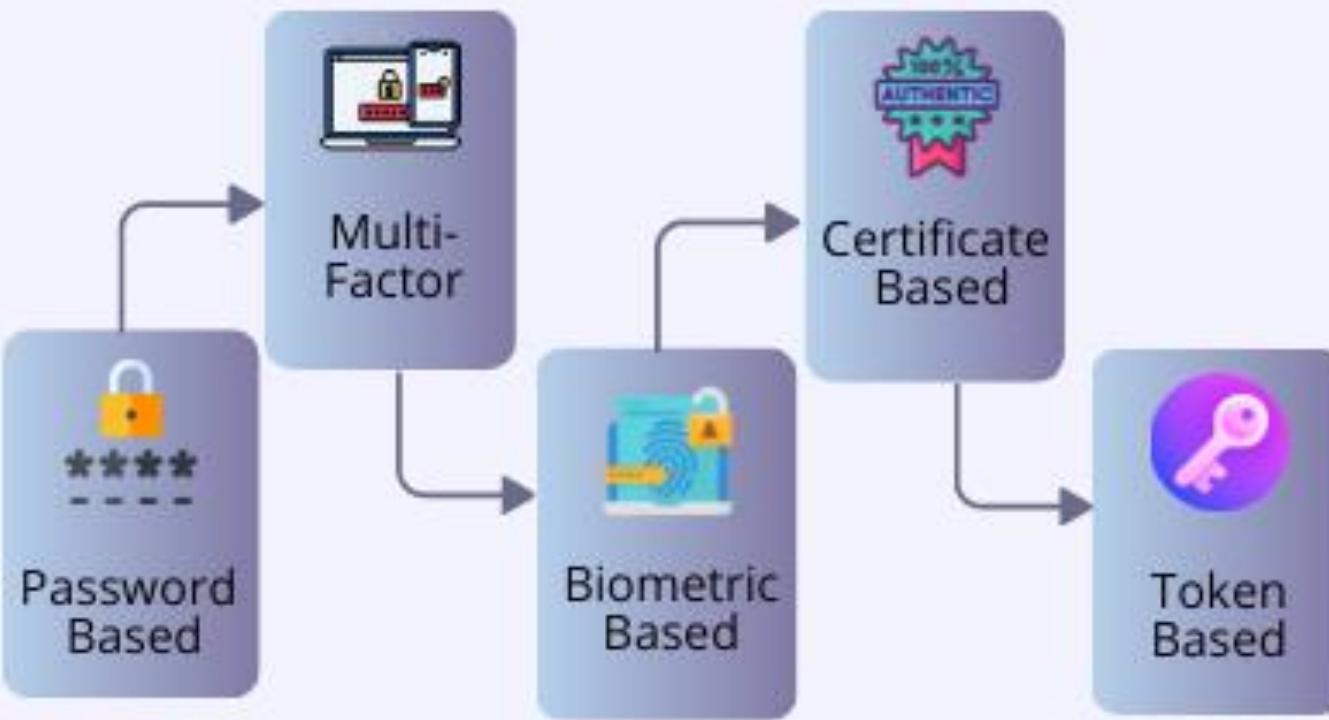
Common Vulnerabilities and Exposures (CVEs)

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	
<small>Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.</small>	
<ul style="list-style-type: none">• 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	

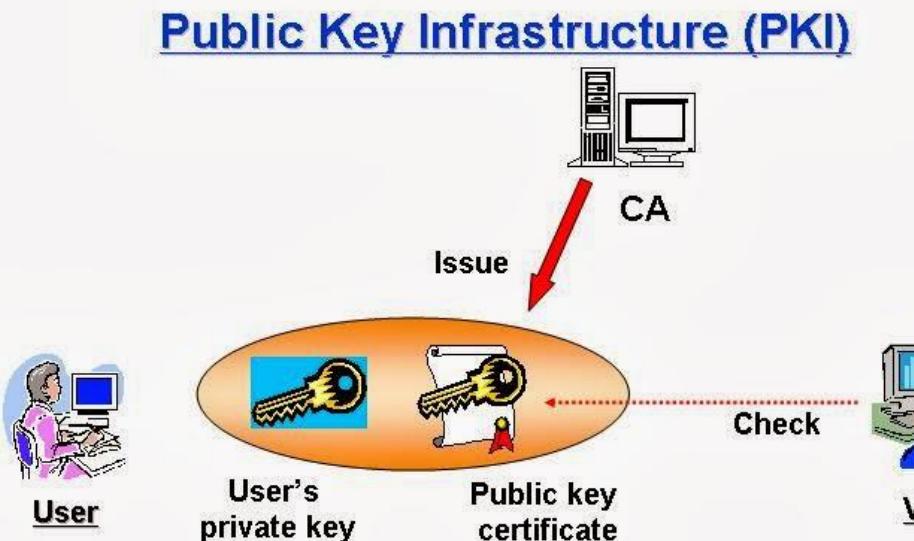


Authentication

Different types of Authentication



Public Key Infrastructure (PKI)



10-minute
break



Access Control

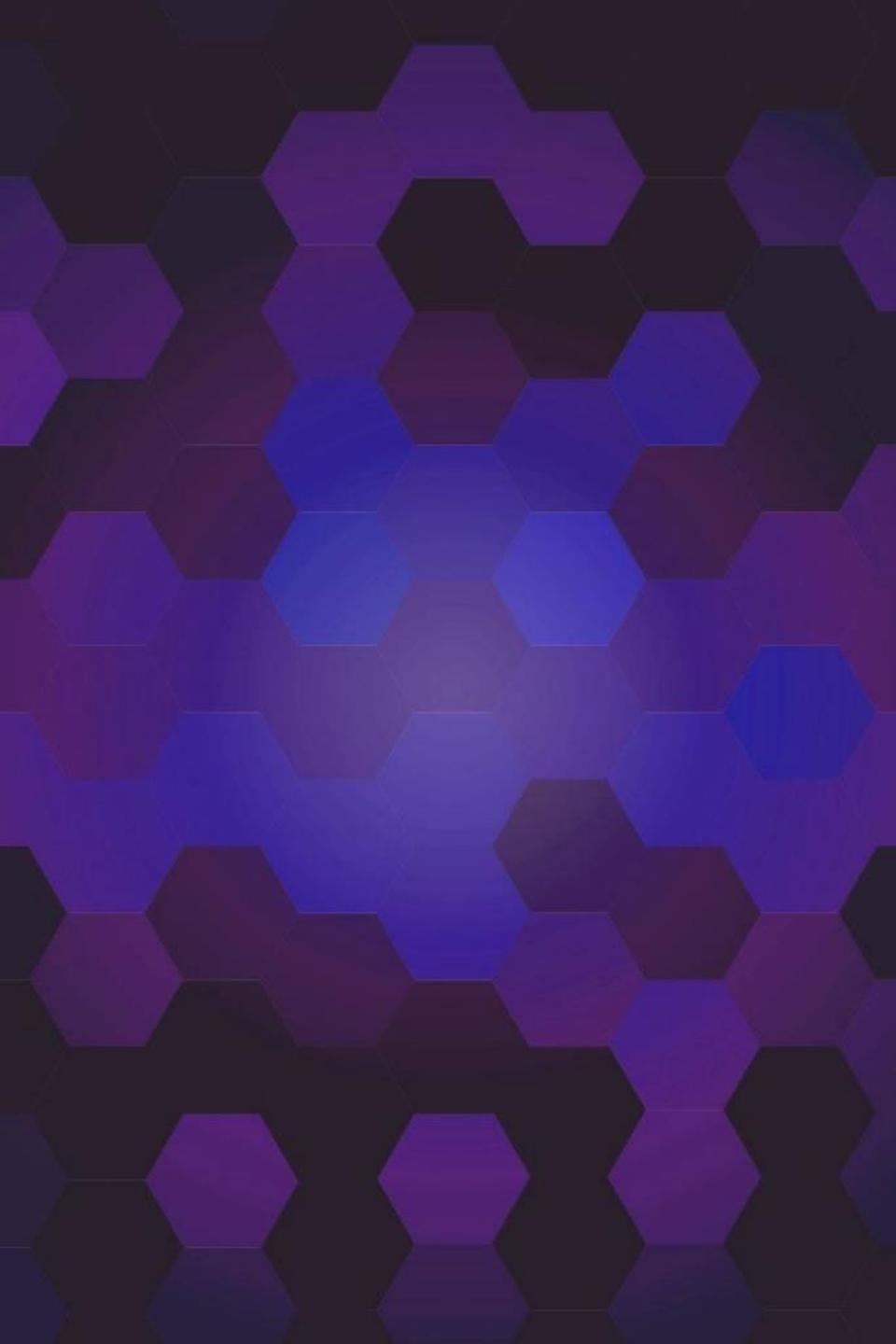
MAC, DAC, and RBAC



Mandatory Access Control



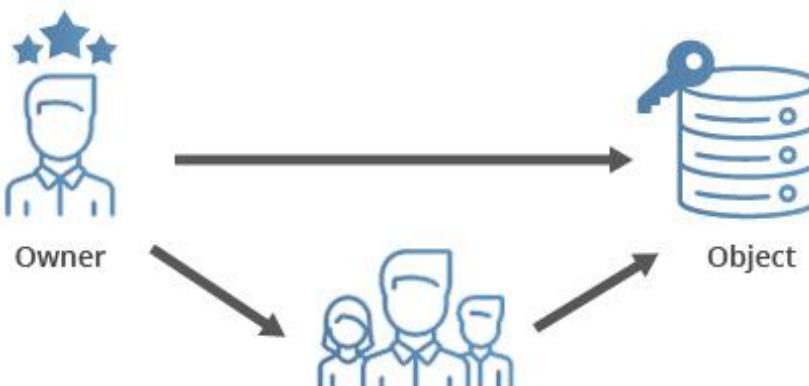
Mandatory Access Control (MAC)



Discretionary Access Control (DAC)

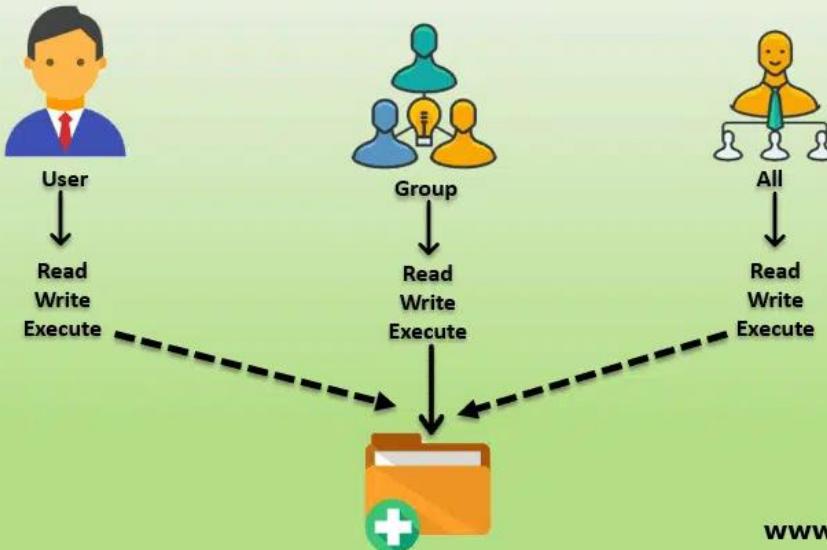
DAC

Discretionary Access Control (DAC)



Specifies users/groups who can access

Unix File Permissions



www.educba.com

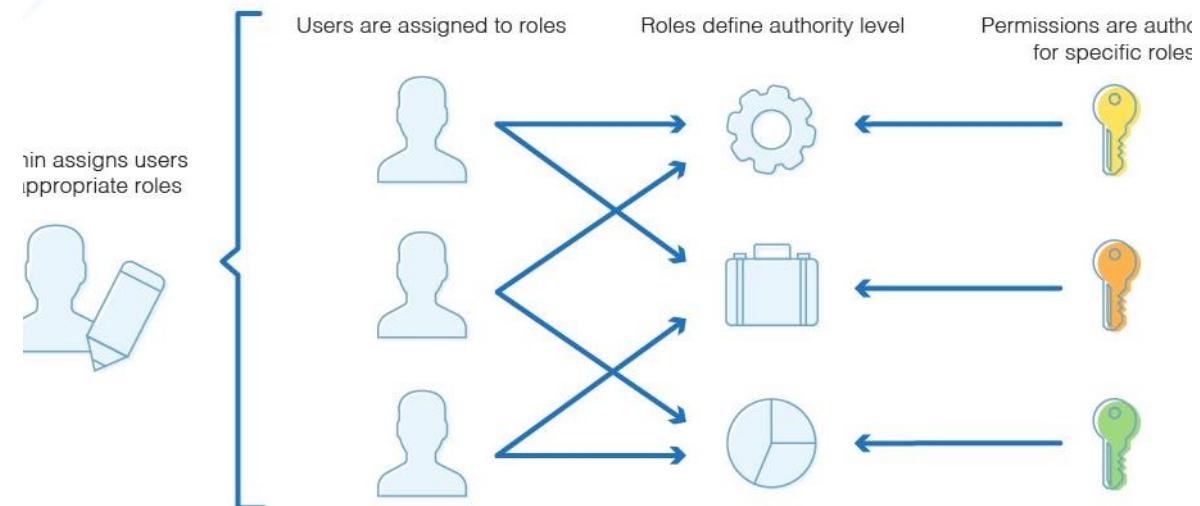
DAC In
Action

Linux permissions in practice

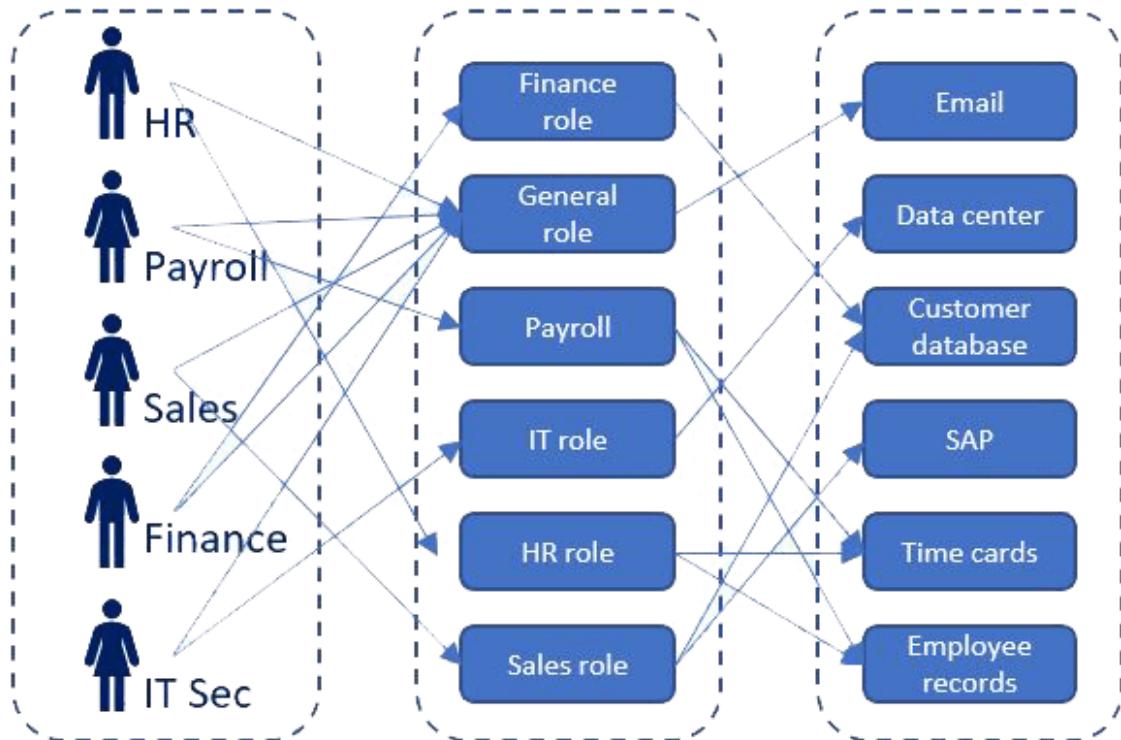
```
jpp@jpp:/boot$ ls -la
total 39132
drwxr-xr-x  3 root root    4096 2011-05-13 08:52 .
drwxr-xr-x 23 root root    4096 2011-05-04 09:27 ..
-rw-r--r--  1 root root  700761 2011-03-18 16:33 abi-2.6.35-28-generic
-rw-r--r--  1 root root  730039 2011-04-11 01:24 abi-2.6.38-8-generic
-rw-r--r--  1 root root 122616 2011-03-18 16:33 config-2.6.35-28-generic
-rw-r--r--  1 root root 130313 2011-04-11 01:24 config-2.6.38-8-generic
drwxr-xr-x  3 root root   12288 2011-05-04 09:32 grub
-rw-r--r--  1 root root 11008098 2011-04-15 08:58 initrd.img-2.6.35-28-generic
-rw-r--r--  1 root root 13134896 2011-05-13 08:52 initrd.img-2.6.38-8-generic
-rw-r--r--  1 root root 160988 2010-10-22 09:08 memtest86+.bin
-rw-r--r--  1 root root 163168 2010-10-22 09:08 memtest86+_multiboot.bin
-rw-r--r--  1 root root 2344143 2011-03-18 16:33 System.map-2.6.35-28-generic
-rw-----  1 root root 2654256 2011-04-11 01:24 System.map-2.6.38-8-generic
-rw-r--r--  1 root root   1336 2011-03-18 16:35 vmcoreinfo-2.6.35-28-generic
-rw-----  1 root root   1368 2011-04-11 01:26 vmcoreinfo-2.6.38-8-generic
-rw-r--r--  1 root root 4342384 2011-03-18 16:33 vmlinuz-2.6.35-28-generic
-rw-----  1 root root 4523936 2011-04-11 01:24 vmlinuz-2.6.38-8-generic
jpp@jpp:/boot$
```

Role Based Access Control (RBAC)

Role-Based Access Control



RBAC In Action



Pentesting Methodology



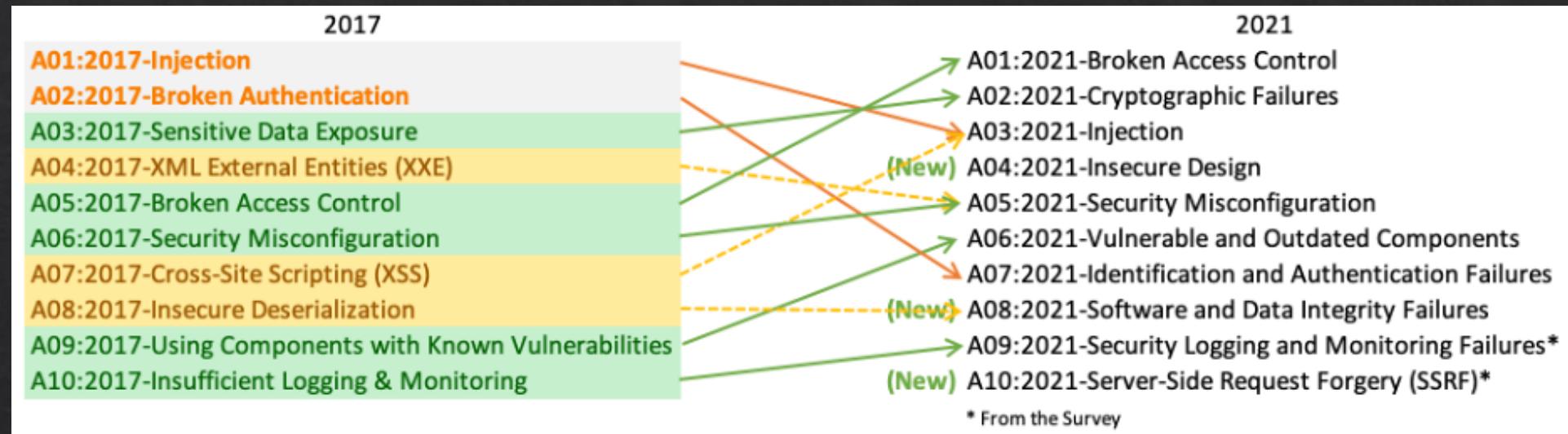
Standards



OWASP

Open Web Application
Security Project

OWASP



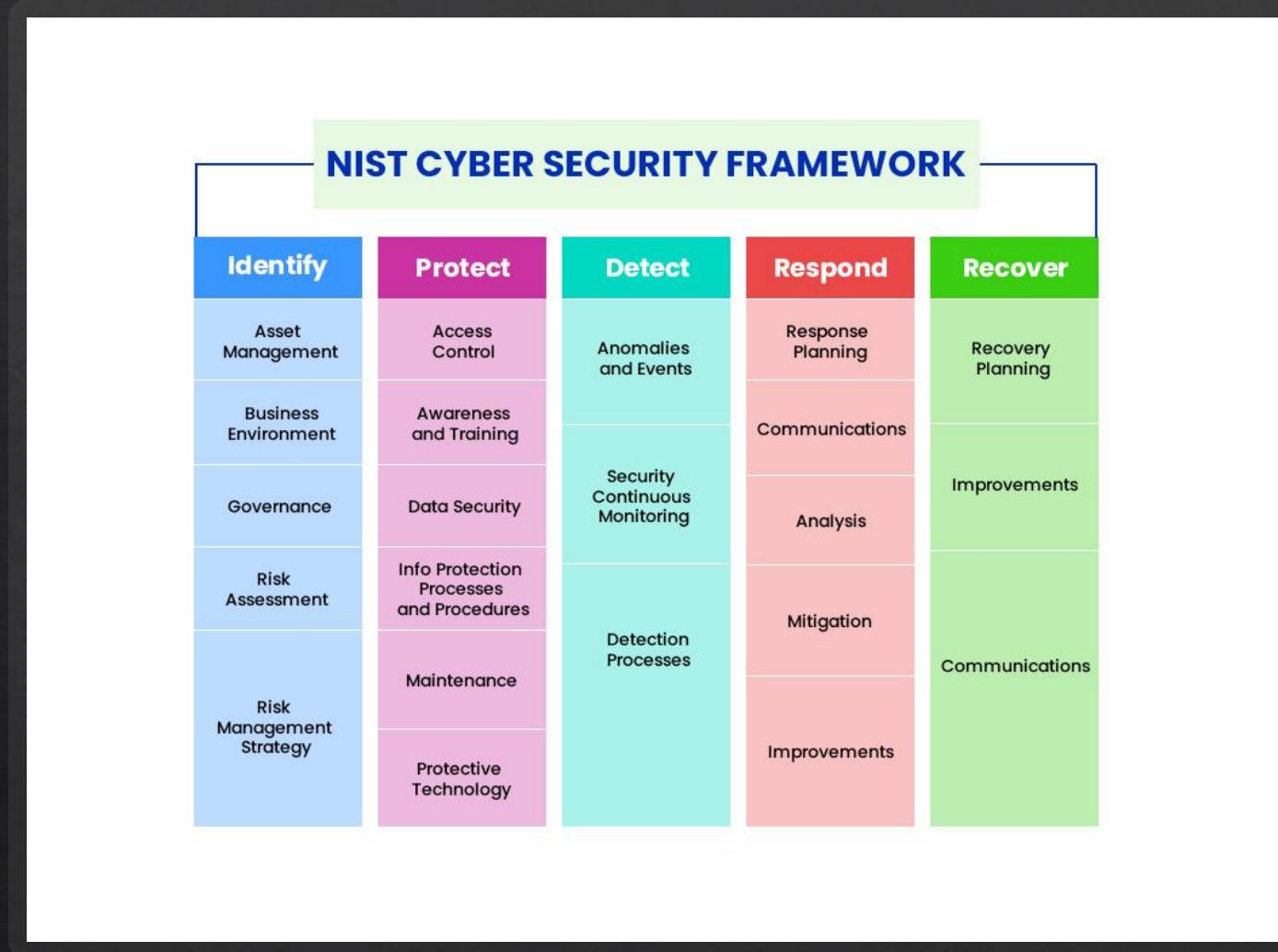
OWASP Top 10



Mobile Application Security Verification Standard (MASVS)

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





NIST Cybersecurity Framework

Application Programming Interface (APIs)

Application Programming Interfaces (APIs)

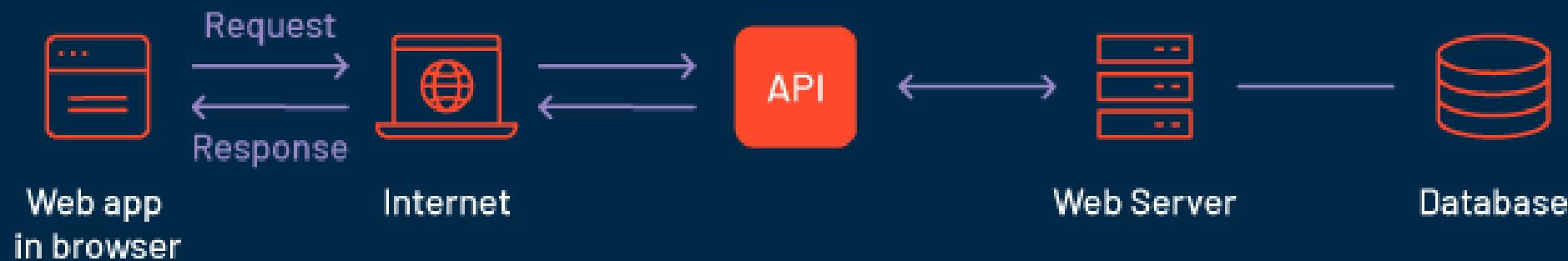


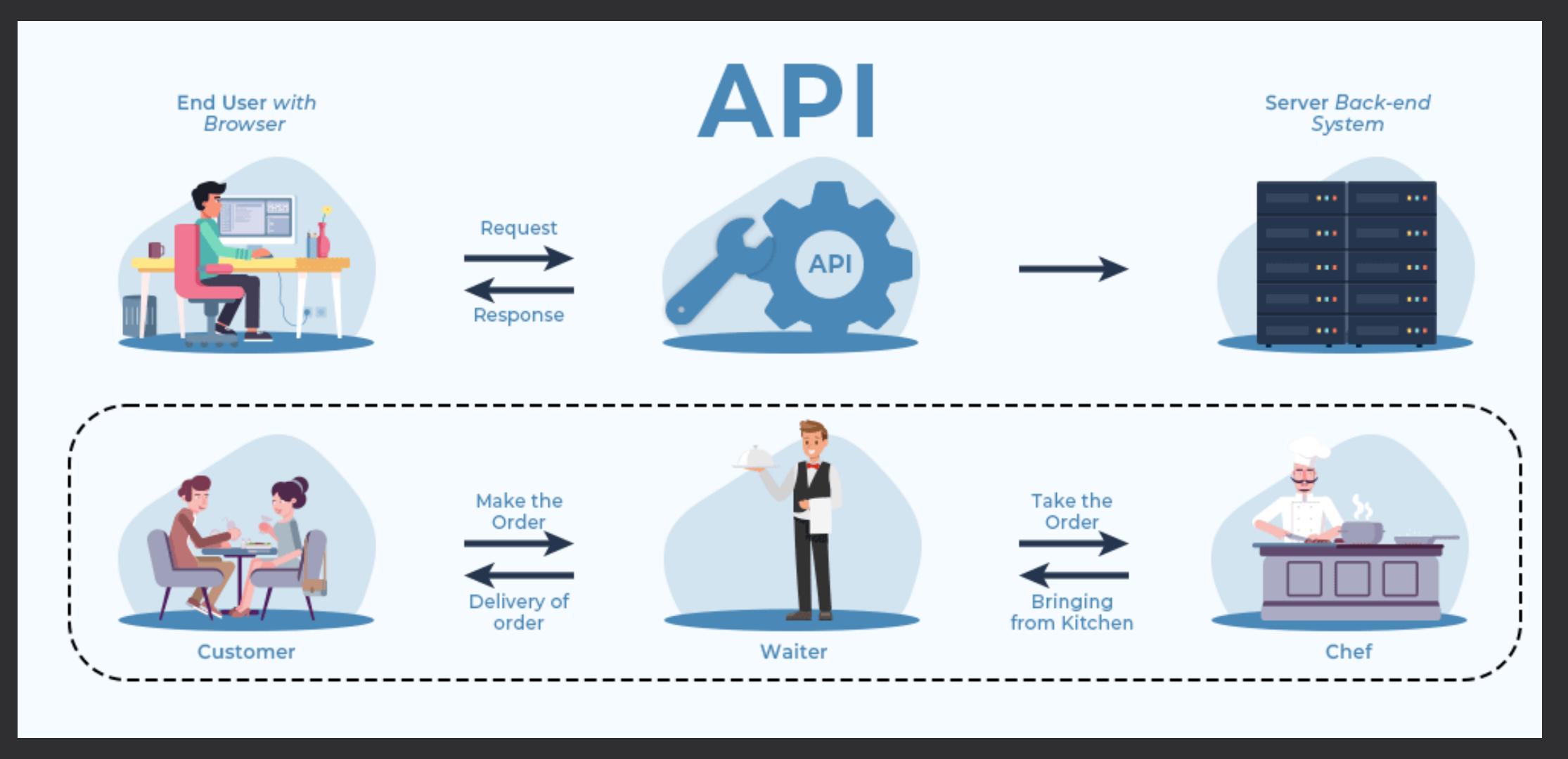
What do they do for
applications?



When would we want to use an
API?

How Do APIs Work





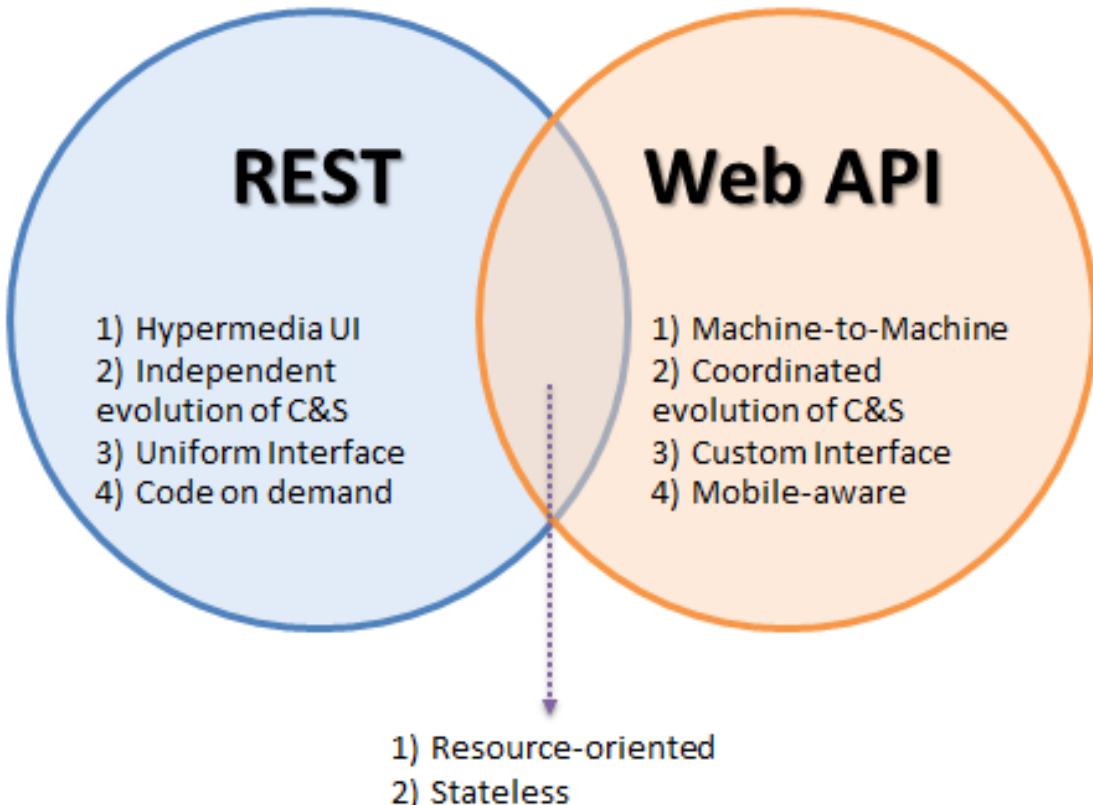
Common API Protocols



Representational State
Transfer (REST or RESTful)
API

```
{  
  "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



The background of the image is a close-up, slightly blurred view of a computer keyboard and a white document with text.

HTTP/Web API

HTTP API Verbs

- ❖ HTTP
 - ❖ GET
 - ❖ POST
 - ❖ PUT
 - ❖ DELETE

HTTP GET Header

method	path	protocol
GET	/tutorials/other/top-20-mysql-best-practices/	HTTP/1.1
Host: net.tutsplus.com		
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.1		
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=		
Accept-Language: en-us,en;q=0.5		
Accept-Encoding: gzip,deflate		
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7		
Keep-Alive: 300		
Connection: keep-alive		
Cookie: PHPSESSID=r2t5uvjq435r4q7ib3vtdjq120		
Pragma: no-cache		
Cache-Control: no-cache		

HTTP headers as Name: Value

HTTP POST Header

The Request line:

The HTTP Method.

The path to the resource on the web server.

The protocol version that the web browser is requesting.

POST /advisor/selectBeerTaste.do HTTP/1.1

The Request headers:

Host: www.wickedlysmart.com

User-Agent: Mozilla/5.0 (Macintosh; U; PPC Mac OS X Mach-O; en-US; 20030624 Netscape/7.1

Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.8,application/xhtml+xml;q=0.8,application/xml;q=0.8,application/xml;q=0.8,video/x-mng,image/png,image/jpeg,image/gif;q=0.2,*/*

Accept-Language: en-us,en;q=0.5

Accept-Encoding: gzip,deflate

Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7

Keep-Alive: 300

Connection: keep-alive

The message body, sometimes called the "payload".

{ color=dark&taste=malty }

This time, the parameters are down here in the body, so they aren't limited the way they are if you use a GET and have to put them in the Request line.

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!

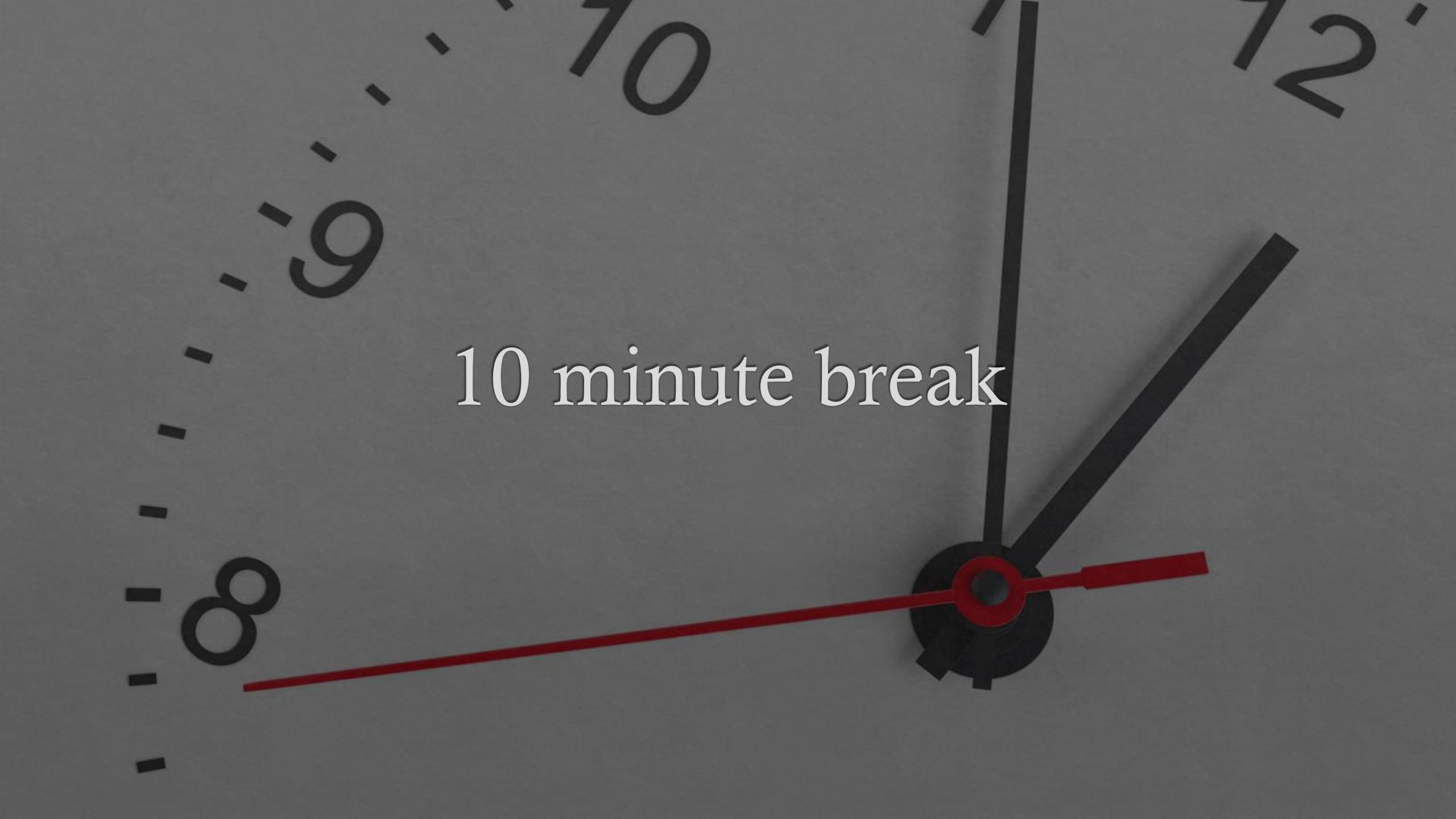
Mobile APIs vs. Web APIs



- 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

A close-up view of a clock face, likely a kitchen timer, set to 10 minutes. The clock has black numbers and hands on a light gray background. A red second hand is positioned at the 7 o'clock position. The text "10 minute break" is overlaid in white font.

10 minute break



Securing APIs

SAML vs. Oauth

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

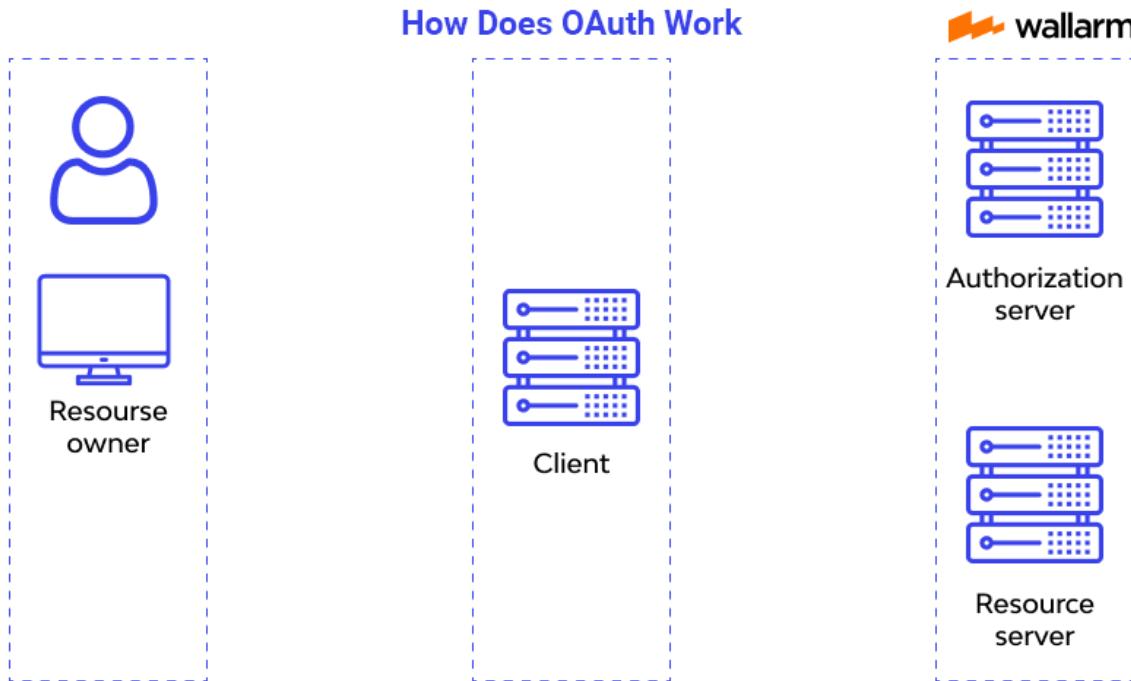
Copy

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



A large, abstract graphic in the background consists of numerous overlapping triangles in shades of orange, yellow, and light brown, creating a sense of depth and motion.

Preview Week 3