



**CYBSEC**<sub>SA</sub>  
Security Systems

# Attacking the Giants: Exploiting SAP Internals

Mariano Nuñez Di Croce  
mnunez [at] cybsec [dot] com

30 November, 2007  
EKOPARTY, Buenos Aires



## Agenda

- SAP Connectivity
- SAP RFC Interface
- The RFC Library
- Security Review of the RFC Interface Implementation
- PenTesting with sapyto
- Going After the Low-Hanging-Fruit
- Advanced Attacks
- Conclusions
- Questions & Answers



# SAP Connectivity

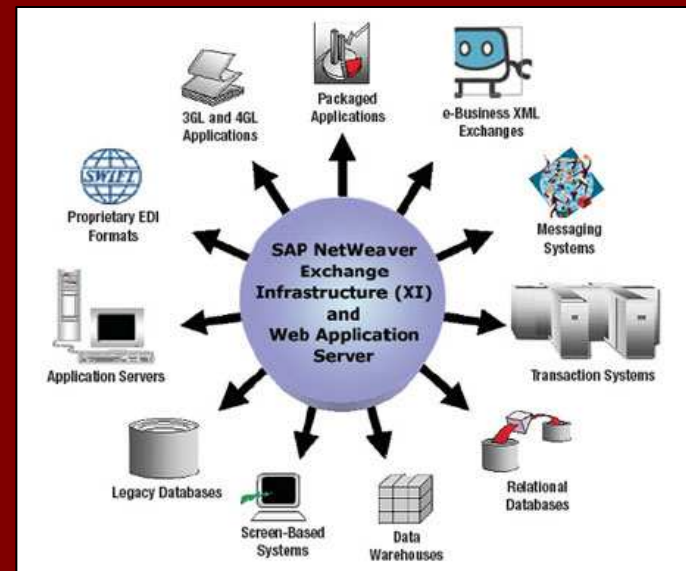
# Attacking the Giants: Exploiting SAP Internals

## SAP Connectivity



## SAP Connectivity

- SAP is designed to be able to interact with many **external systems**.
- This way you can **integrate** and centralize information under a unique architecture.
- Communicating with other systems:
  - HTTP
  - FTP
  - ALE
  - EDI
  - **RFC**
  - XML
  - SMTP
  - ...





# SAP RFC Interface

# Attacking the Giants: Exploiting SAP Internals

## SAP RFC Interface



### A Little Bit of History...

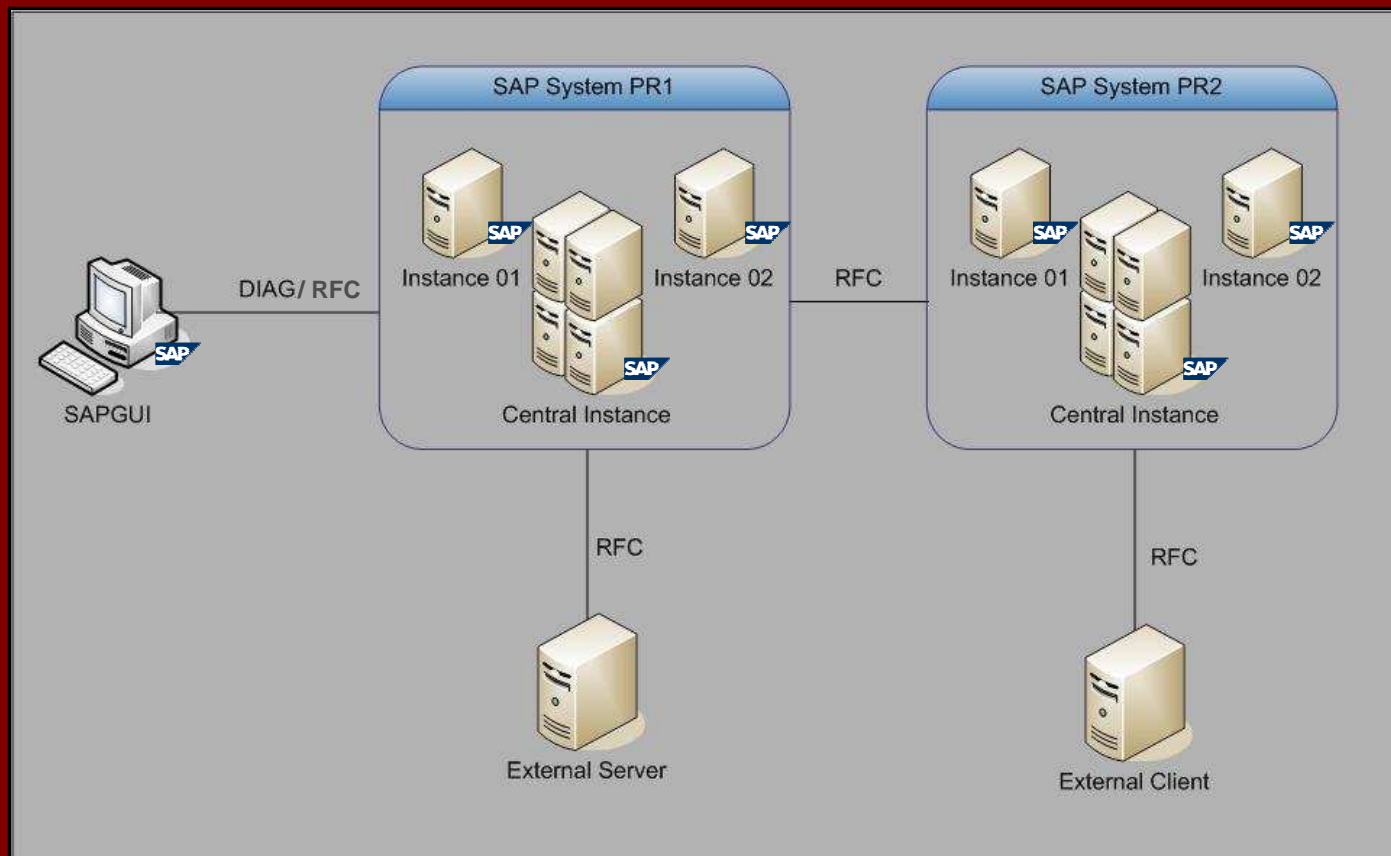
- In the beginning, SAP implemented IBM's CPI-C interface to communicate with other systems.
- CPI-C was developed to allow data transfer.
- Complex applications needed to be able to call functions on other servers.
- Result: SAP Remote Function Call (RFC) Interface.
- Developed in the 1980s, based on CPI-C.
- Today, the RFC Interface is a key component of the SAP Application Server.

# Attacking the Giants: Exploiting SAP Internals

## SAP RFC Interface



## SAP Systems Layout





## RFC Function Modules

- For a **Function Module** to be remotely-callable, it must be flagged as "Remote-enabled".
- ABAP Programs call a remote Function Module using the command **CALL FUNCTION...DESTINATION..**

```
...  
CALL FUNCTION 'ZCUST_GETMONEY' DESTINATION 'PROD2'  
  EXPORTING  
    ZCUST_ID = 100  
  IMPORTING  
    MONEY = cust_money  
  TABLES  
    TABINFO = table1  
  EXCEPTIONS  
    CUST_NOT_FOUND = 0  
    TABLE_EMPTY = 1  
...
```

# Attacking the Giants: Exploiting SAP Internals

## SAP RFC Interface



## RFC Destinations

DESTINATION argument is a **index key** to an RFC Destinations table (RFCDES), maintained through transaction **SM59**.

The screenshot shows the SAP SM59 transaction window titled "Configuration of RFC Connections". The table displays various RFC connections categorized into folders: ABAP Connections, Internal Connections, SNA/CPI-C connections, and TCP/IP connections. The TCP/IP connections folder is expanded, showing a list of connections with their respective types and comments.

RFC Connections	Type	Comment
ABAP Connections	3	
Internal Connections	I	
SNA/CPI-C connections	S	
TCP/IP connections	T	
CALLTP_WindowsNT	T	Transport Tools: tp Interface *generated*
DOCUMENTATION_HELP	T	Call WinHelp and WinWord from R/3
EU_SCRP_MF	T	Graphical Screen Painter (Unix/Motif)
EU_SCRP_TEST	T	Graphical Screen Painter (local Test for A.Herrmann)
EU_SCRP_WN32	T	Graphical Screen Painter (WindowsNT / Windows95)
F1_HELP_SERVER	T	Windows RFC server for F1 help on fields, messages and comm
F1_HELP_SERVER_32	T	Windows RFC server for F1 help on fields, messages and comm
F1_HELP_SERVER_40	T	Windows RFC server for F1 help on fields, messages and comm
GFW_ITS_RFC_DEST	T	Generated RFC destination for IGS
IGS_RFC_DEST	T	Generated RFC destination for IGS
LOCAL_CALLSCREEN	T	RFC of local C program call screen
LOCAL_EXEC	T	Starts the Program 'RFCEXEC' on Front End Machine
LOCAL_EXEX	T	Runs rfcexec for X terminals
LOCAL_PRINT	T	

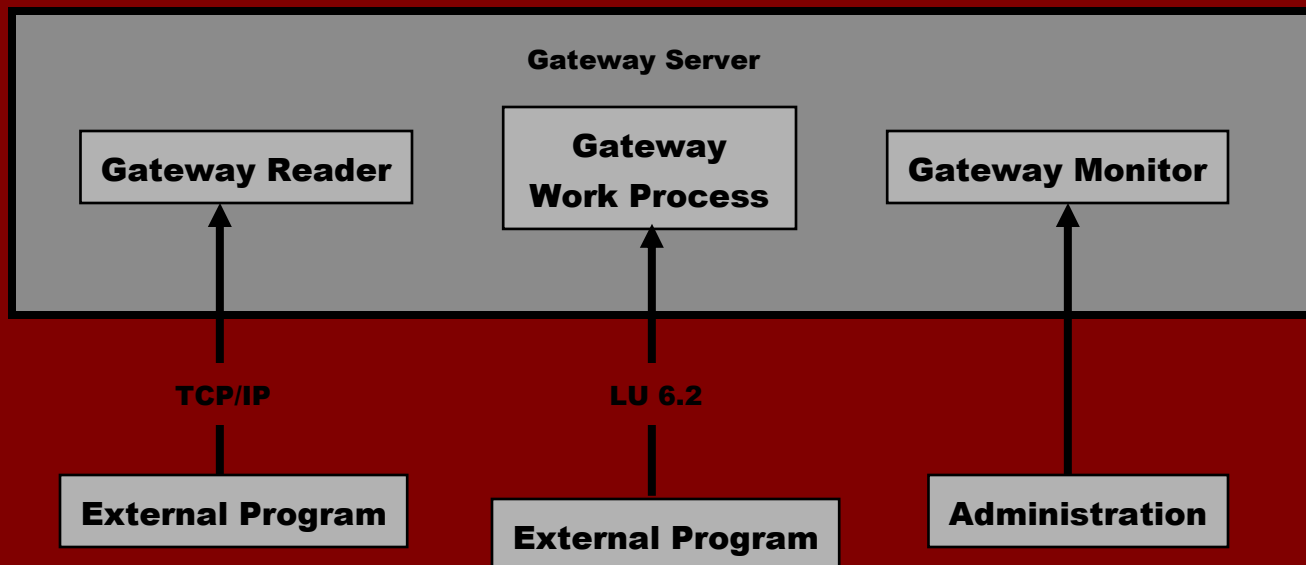
# Attacking the Giants: Exploiting SAP Internals

## SAP RFC Interface



## The Gateway Service

- CPIC/RFC communication is done through the **Gateway Service**.
- **Handles communications** between SAP systems and between SAP systems and External systems.
- Logically, it consists of **three** different services.



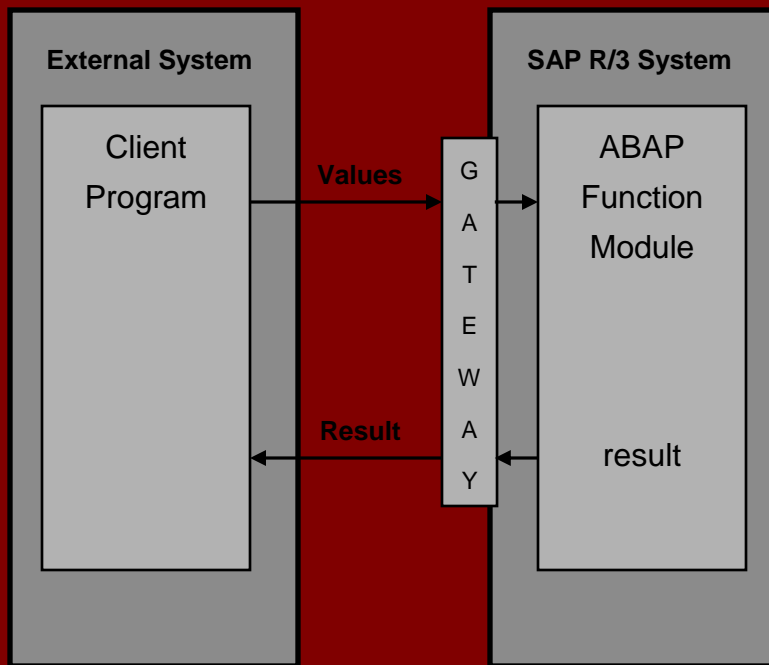
# Attacking the Giants: Exploiting SAP Internals

## SAP RFC Interface

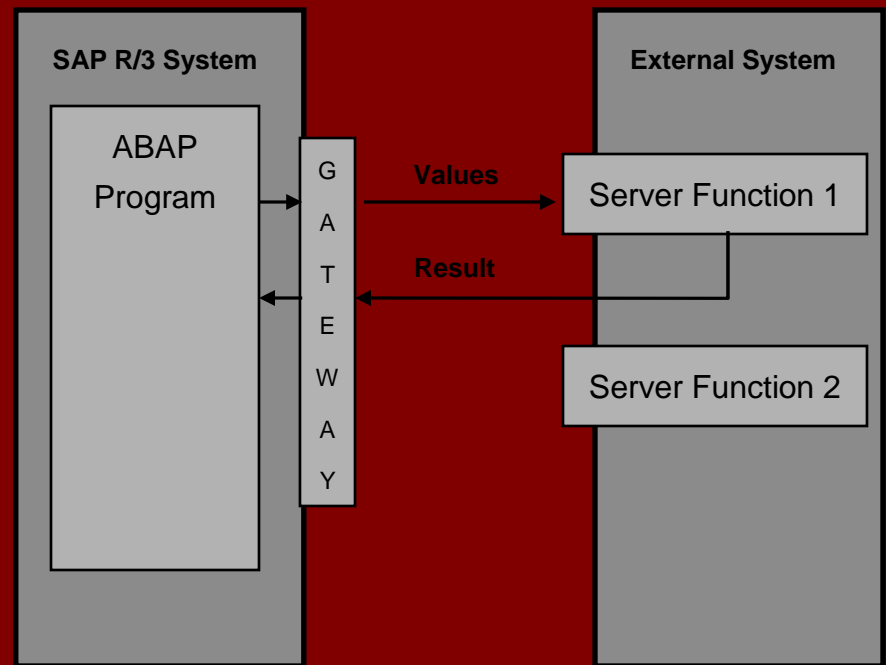


### RFC Between SAP and External Systems

- External RFC Client



- External RFC Server





## External RFC Servers

- 2 Ways of "attaching" External RFC Servers:
  - **Started Mode**
    - Application Server (the GW, really) starts them remotely on-demand.
    - Commonly via Remote Shell or Remote Exec (!)
    - External Server is closed after operation.
  - **Registered Mode**
    - External Server registers *itself* at the Gateway Server.
    - Identified by a **Program ID**.
    - External Server is not closed.

**But ... How do you develop an external client / server ??**



# The RFC Library



## The RFC Library

"The RFC Library is the most commonly used and installed component of existing SAP software"

*SAP RFCSDK Guide*

- **API** released by SAP to allow development of external RFC clients/servers.
- Available for all SAP supported platforms.
- An upper layer: **JCo**, **.Net**, ...
- Delivered with examples.



## External RFC Server Internals

- First of all, the server install available functions:

```
RfcInstallFunction(RFC_FUNCTIONNAME functionname,  
                  RFC_ONCALL f_ptr,  
                  rfc_char_t *docu);
```

- Listen and dispatch requests with **RfcDispatch()** loop.
- Requested function (*f\_ptr*) is executed.
- Results are sent back to client.
- Three functions installed by default:
  - RFC\_DOCU
  - RFC\_PING
  - RFC\_SYSTEM\_INFO



# Security Review of the RFC Interface Implementation

(version 6.40)

# Attacking the Giants: Exploiting SAP Internals

## Security Review of the RFC Interface...



## Traffic Analysis

- Information is sent in **clear-text** by default.
- SAP provides **SNC** (Secure Network Communications) for encryption of traffic.
- What can we get?
  - **Logon** information (client, user ID, password).
  - Called Function Name.
  - Parameters Information and **Content**.
  - Tables Information and **Content** (may be compressed).
  - Client and Server information.
  - ...

# Attacking the Giants: Exploiting SAP Internals

## Security Review of the RFC Interface...



## Traffic Analysis

```
...
01a0 00 00 00 00 00 06 05 14 00 10 5f 22 ea 45 5e ....._".E^
01b0 22 c5 10 e1 00 00 00 c0 a8 02 8b 05 14 01 30 00 .....0.
01c0 0a 72 66 63 5f 73 65 72 76 65 72 01 30 01 11 00 .rfc_server.0...
01d0 06 42 43 55 53 45 52 01 11 01 17 00 0b 81 bb 89 .BCUSER.....
01e0 62 fc b5 3e 70 07 6e 79 01 17 01 14 00 03 30 30 b..?w.oy.....00
01f0 30 01 14 01 15 00 01 45 01 15 05 01 00 01 01 05 0.....E.....
0200 01 05 02 00 00 05 02 00 0b 00 03 36 34 30 00 0b .....640..
0210 01 02 00 0e 5a 43 55 53 54 5f 47 45 54 4d 4f 4e ....ZCUST_GETMON
0220 45 59 01 02 05 14 00 10 5f 22 ea 45 5e 22 c5 10 EY....._".E^"..
0230 e1 00 00 00 c0 a8 02 8b 05 14 02 01 00 09 43 4c .....CL
0240 49 45 4e 54 5f 49 44 02 01 02 03 00 08 43 55 53 IENT_ID.....CUS
0250 54 30 30 31 00 02 03 ff ff 00 00 ff ff 00 00 01 T001.....
0260 c7 00 00 3e 80 ...>.
```

# Attacking the Giants: Exploiting SAP Internals

## Security Review of the RFC Interface...



### Traffic Analysis: Show me the Password!

- You said that data is clear-text... but I can't see a single password!
- Reason: Password is obfuscated.

```
for each CHAR in CLEAR_TEXT_PASS
```

```
    OBFUSCATED_PASS[i] = CHAR XOR KEY[i]
```

```
KEY_TO_THE_KINGDOM = [0x96, 0xde, 0x51, 0x1e, 0x74, 0xe,  
0x9, 0x9, 0x4, 0x1b, 0xd9, 0x46, 0x3c, 0x35, 0x4d, 0x8e,  
0x55, 0xc5, 0xe5, 0xd4, 0xb, 0xa0, 0xdd, 0xd6, 0xf5,  
0x21, 0x32, 0xf, 0xe2, 0xcd, 0x68, 0x4f, 0x1a, 0x50,  
0x8f, 0x75, 0x54, 0x86, 0x3a, 0xbb]
```

# Attacking the Giants: Exploiting SAP Internals

## Security Review of the RFC Interface...



CYBSEC<sup>SA</sup>  
Security Systems

© 2007

### Function Analysis: RFC\_DOCU

- Retrieves **documentation** about installed functions on External Server.
- Specifically, it outputs strings defined in the *rfc\_docu* parameter of *RfcInstallFunction()* calls.
- **No need for valid logon data.**
- Available in External Systems.

This function can be used to **discover installed functions** and their structure.

# Attacking the Giants: Exploiting SAP Internals

## Security Review of the RFC Interface...



### Function Analysis: RFC\_PING

- An RFC ping
- Connects to the target system, analyzing its **availability**.
- **No need for valid logon data.**
- Available in External Systems and SAP Application Servers.

This function can be used to **check for availability** of a remote RFC Server.



## Function Analysis: RFC\_SYSTEM\_INFO

- Obtain RFC server system information.
- No need for logon data!
- Available in External Systems and SAP Application Servers (!).

What can we get?

- SAP Kernel Version
- Hostname
- Timezone
- Database Engine
- Database Host
- SAP System ID
- Operating System
- ...

# Attacking the Giants: Exploiting SAP Internals

## Security Review of the RFC Interface...



## Some Other Functions

There are **other functions** installed **by default** in every external RFC server. We have discovered security vulnerabilities in some of them:

- RFC\_TRUSTED\_SYSTEM\_SECURITY
- RFC\_SET\_REG\_SERVER\_PROPERTY
- RFC\_START\_GUI
- SYSTEM\_CREATE\_INSTANCE
- RFC\_START\_PROGRAM

The thing is that...any of this functions **can be called**, just as regular installed functions...



## Abusing Default Functions

- **RFC\_TRUSTED\_SYSTEM\_SECURITY**

Check existence of users and groups in an External system, its domain and trusted domains.

- **RFC\_SET\_REG\_SERVER\_PROPERTY**

Denial Of Service of *Registered Servers*.

- **RFC\_START\_GUI**

Remote Command Execution (buffer overflow).



## Abusing Default Functions (cont.)

- **SYSTEM\_CREATE\_INSTANCE**

Remote Command Execution (buffer overflow).

- **RFC\_START\_PROGRAM**

Restricted through *RfcAllowStartProgram("progrname")*

Remote Command Execution (buffer overflow).

Determine Applied Restrictions through *RfcAllowStartProgram()*.

Path Traversal Attacks (c:\path\IamAllowed.exe\..\..\..\butIamNot.exe).



# PenTesting with sapyto



# Attacking the Giants: Exploiting SAP Internals

## PenTesting with sapyto



### sapyto

- First public framework for performing SAP Penetration Tests.
- Plugin based.
- Shipped with plugins for analyzing RFC vulnerabilities, auditing SAP R/3 configuration, perform the actual penetration, etc..
- Developed in Python and C.

**Download ->** <http://www.cybsec.com/en/research/default.php>

# Attacking the Giants: Exploiting SAP Internals

## PenTesting with sapyto



### Available Plugins



- Audit:
  - RFC Ping.
  - Registration of External Servers.
  - Detection of RFCEXEC.
  - Detection of SAPXPG.
  - Get system information.
  - Get server documentation.

# Attacking the Giants: Exploiting SAP Internals

## PenTesting with sapyto



## Available Plugins

- Attack:
  - RFC\_START\_PROGRAM Directory Traversal.
  - Run commands through RFCEXEC.
  - Run commands through SAPXPG.
  - StickShell.
  - Evil Twin Attack.
  - Get remote RFCShell.
- Tools:
  - RFC Password Obfuscator / De-obfuscator.



# Going After the Low-Hanging Fruit



# Attacking the Giants: Exploiting SAP Internals

## Going After the Low-Hanging Fruit



### RFCEXEC

- Bundled with the RFCSDK.
- Works in *registered mode*.
- Released as an example, not intended for productive use.
- Provides the following functions:
  - RFC\_RAISE\_ERROR
  - RFC\_MAIL
  - RFC\_REMOTE\_PIPE
  - RFC\_REMOTE\_FILE
  - RFC\_REMOTE\_EXEC
- Protected through *rfcexec.sec* file directives.

# Attacking the Giants: Exploiting SAP Internals

## Going After the Low-Hanging Fruit



## SAPXPG

- Executable shipped with SAP Application Server.
- Works in *started mode*.
- Used for (legitimate) execution of external commands and programs in SAP systems.
- Installs the following functions:
  - SAPXPG\_END\_XPG
  - SAPXPG\_START\_XPG\_LONG
  - SAPXPG\_START\_XPG

**So...what if we tell the Gateway to start *sapxpg*?**



# Advanced Attacks

# Attacking the Giants: Exploiting SAP Internals

## Advanced Attacks

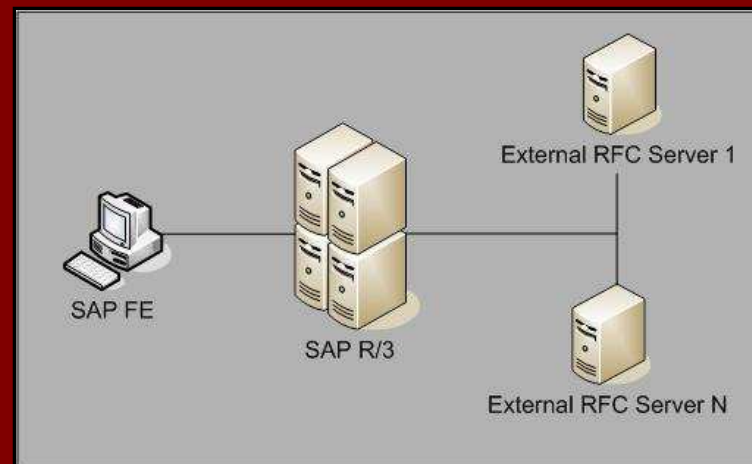


CYBSEC<sup>SA</sup>  
Security Systems

© 2007

## Attacks Setup

- Scenario:



- We need some information about current deployment.
- How do we get it?
  - Network sniffing (RFC is clear-text!).
  - The Gateway Monitor.
  - Kidnapping an SAP administrator. (No step-by-step demonstration )



## Getting the Information: The Gateway Monitor

- The **Gateway Server** has a configuration parameter for restricting Gateway Monitor access.

```
gw/monitor = 0    Monitor is disabled.  
gw/monitor = 1    Local access only.  
gw/monitor = 2    Remote access enabled.
```

- Up to SAP Kernels 6.20, **default value for this parameter is: 2.**
- Remote access to the Gateway Monitor would provide **any information needed** for the attacks.



## Evil Twin

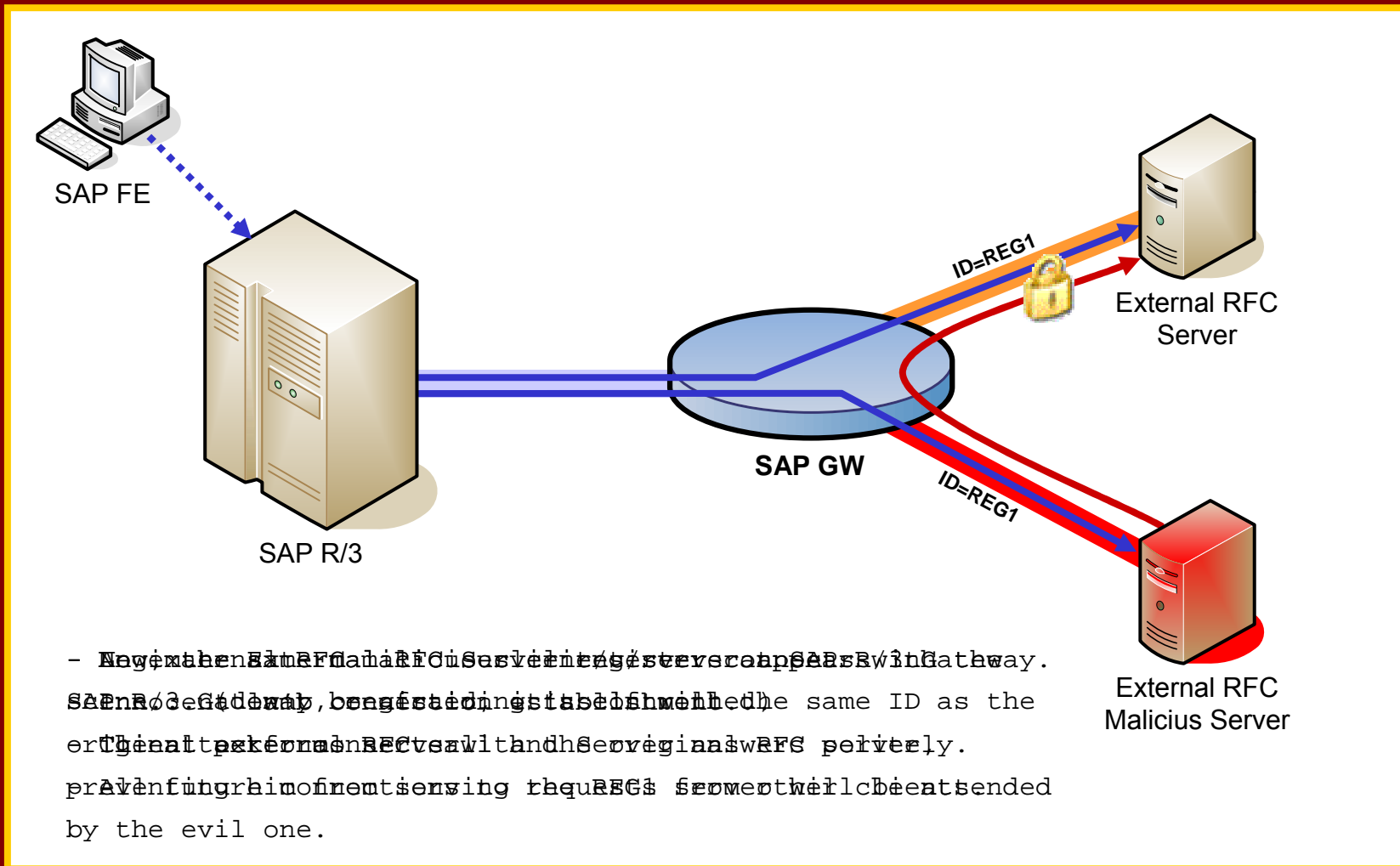
- Registration of External Servers can be done remotely.
- ACL for registration process is implemented through the *reg\_info* file.
- By default, registration for everyone is allowed. (Registration Party!)
  
- External Servers can register several times with the same Program ID.
- ANY External Server can register with that ID!
  
- Attack:
  1. Connect to licit Registered Server, ID=REG1 (blocking connections).
  2. Register External Server with ID=REG1.
  3. Drink some beer while watching calls arriving to our Evil Twin Server...

# Attacking the Giants: Exploiting SAP Internals

## Advanced Attacks



### Evil Twin illustrated...



- New external RFC Malicious Server is registered over SAP Gateway.  
SAP Gateway, being a distributed system, has the same ID as the  
original external RFC server with the same ID as the original  
server. This prevents the original server from receiving the  
requests sent to the malicious server. The requests are sent  
by the evil one.



## A Wiser (and Stealth) Evil Twin: MITM Attacks

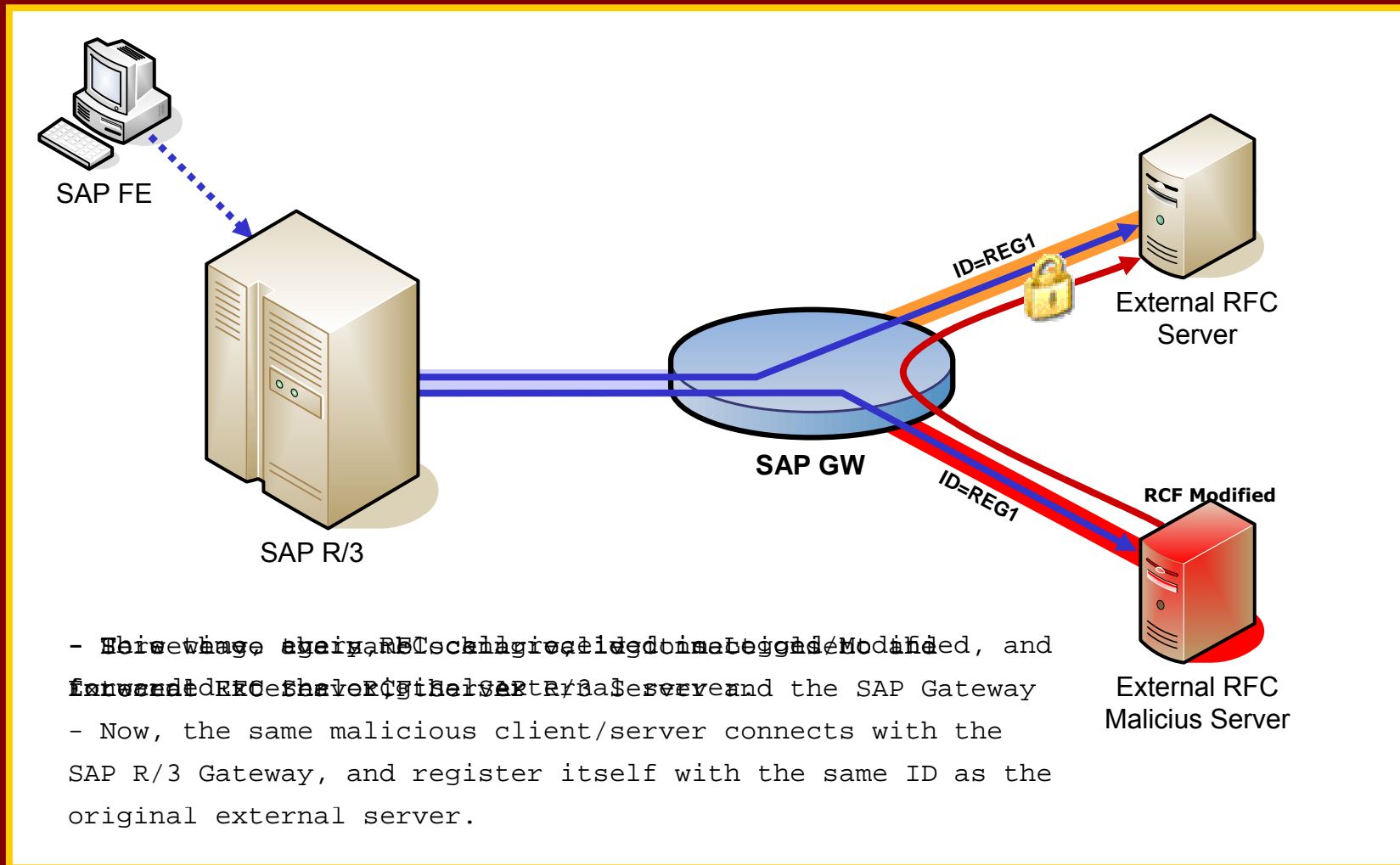
- Proof of Concept.
- Attack:
  1. Connect to licit Registered Server, ID=REG1 (blocking connections).
  2. Register External Server with ID=REG1.
  3. Receive RFC call.
  4. Log / Modify Parameters values.
  5. Use established connection with licit Registered Server to forward the (possible modified) RFC call.
  6. Get results and send them to the original client.
  7. Disconnect from the licit Registered Server.
  8. Back to Step 1.

# Attacking the Giants: Exploiting SAP Internals

## Advanced Attacks



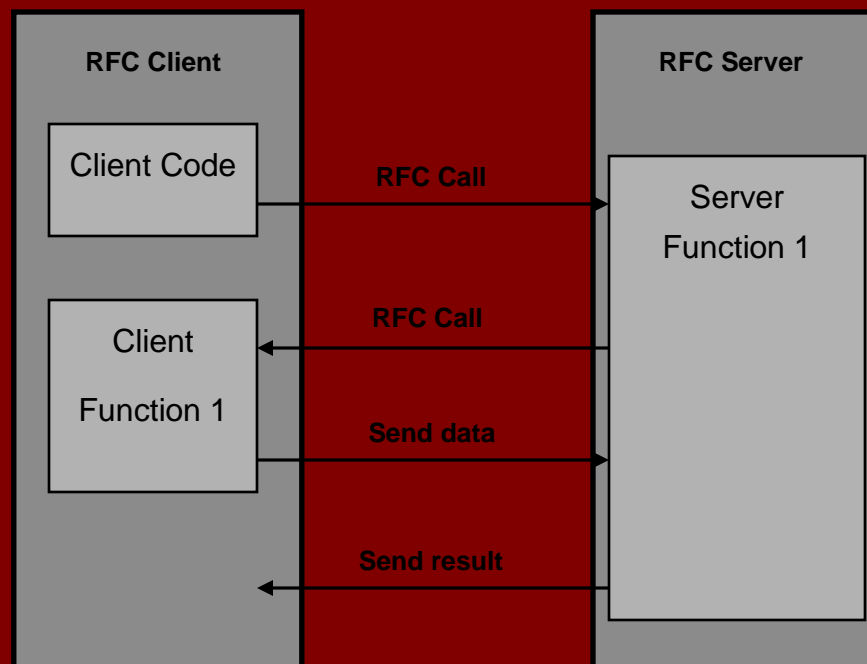
### A Wiser (and Stealth) Evil Twin: MITM Attacks





## Attacking the Application Server with a Registered Server

- RFC Interface allows client / servers to perform “callbacks”.





## Attacking the Application Server with a Registered Server (cont.)

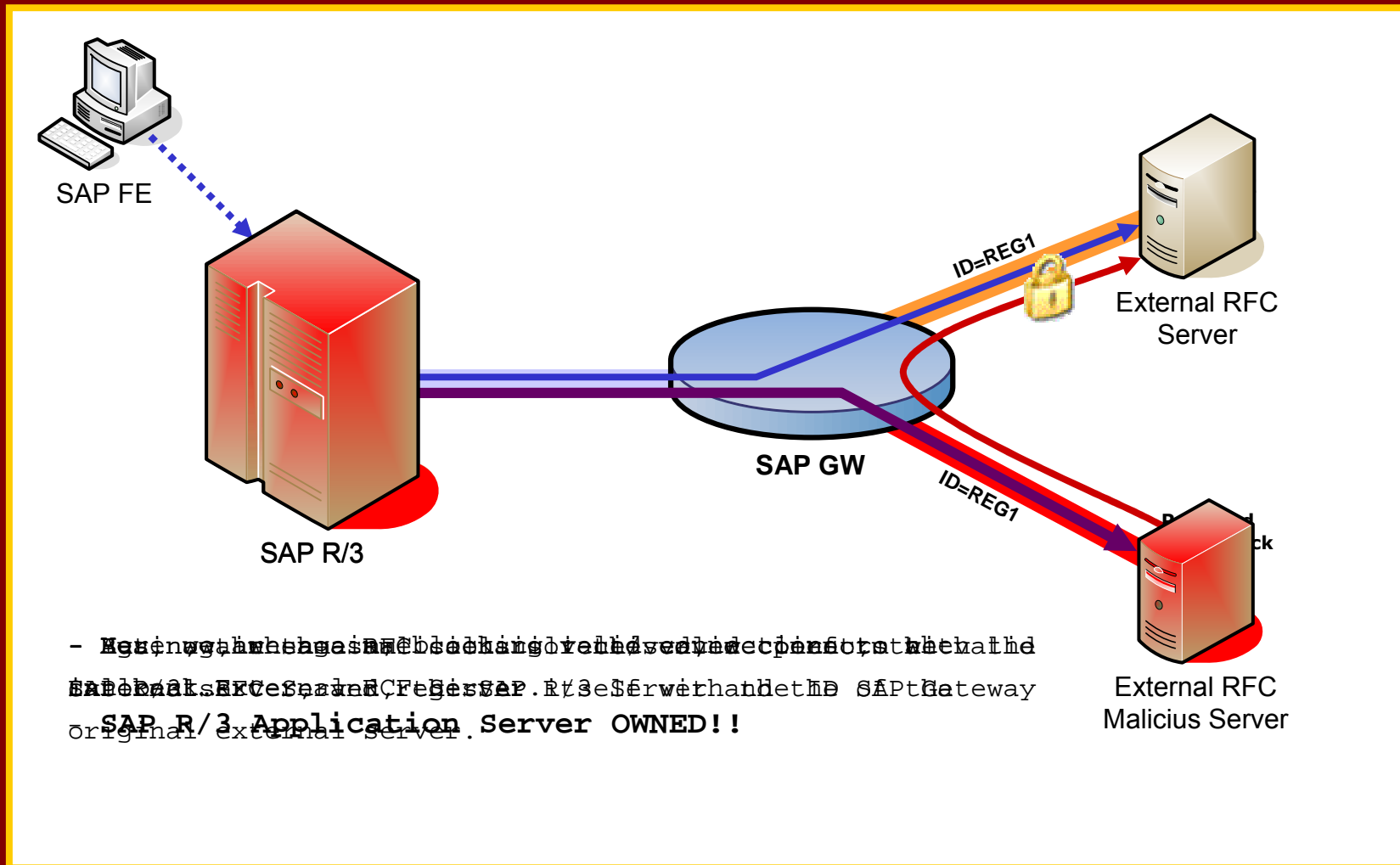
- We can perform “callbacks” to the RFC partner (in this case, SAP App. Server)
- The RFC Call is executed in the **context** of the original R/3 call.
- Impact depends on **authorizations** of the R/3 user (*SAP\_ALL?*).
- Attack:
  1. Connect to licit Registered Server, ID=REG1 (blocking connections).
  2. Start an Evil Twin.
  3. Receive RFC call.
  4. Perform RFC callback.
  5. If user has SAP\_ALL...Bingo!

# Attacking the Giants: Exploiting SAP Internals

## Advanced Attacks



### Attacking the R/3 with a Registered Server (cont.)



- Registering the malicious server as a registered server for the SAP R/3 Application Server. The SAP Gateway will then forward all RFC requests to the malicious server, effectively taking control of the SAP R/3 Application Server.



## Closing the Holes...

- Your SAP administrator already has the protection mechanisms available.
- By default, these attacks are possible.
- Protecting from *started servers attacks*: `gw/sec_info`

```
USER=<user>, [PWD=<pwd>,] [USER-HOST=<user_host>,] HOST=<host>,TP=<tp>;
```

- Protecting from *registered servers attacks*: `gw/reg_info`

```
TP=<tp> [HOST=<host name>,...] [NO=<n>] [ACCESS=<host name,....>] [CANCEL=<host name,....>]
```



## Conclusions & Comments

- The RFC Interface is a wide door into SAP Systems. It has to be locked!
- SAP has responded quickly and provided solutions with SAP notes 1003908, 1003910, 1004084, and 1005397.
- SAP Administrators must **apply patches**.
- **SNC prevents credential and information sniffing**. It is included in SAP systems and must be activated.
- Attacks and caveats described **can be avoided** with proper configuration + patches (don' t forget to use *sec\_info* and *reg\_info!!*)



# Questions?

[mnunez@cybsec.com](mailto:mnunez@cybsec.com)





# Thank you!

