Attacking the Giants: Exploiting SAP Internals

Mariano Nuñez Di Croce

mnunez [at] cybsec [dot] com
March 30, 2007
Blackhat Europe 07
Agenda

• SAP Connectivity
• SAP RFC Interface
• The RFC Library
• Security Review of the RFC Interface Implementation
• Advanced Attacks
• Tool Release: sapyto
• Conclusions
• Questions & Answers
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:
  - ALE
  - EDI
  - HTTP
  - RFC
  - FTP
  - XML
  - ...
SAP RFC Interface
A 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.
SAP Systems Layout
RFC Between SAP Systems

- 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...`

```abap
... 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
...```
RFC Between SAP Systems

- The DESTINATION parameter notifies the AS that it is a remote call.
- Specifically, DESTINATION is an index key to a RFC Destinations table (RFCDES), maintained through transaction SM59.
The Gateway Server

- Communication is done through the Gateway Server.
- Handles communications between SAP systems and between SAP systems and External systems.
- Logically, it consists of three different services.
RFC Between SAP and External Systems

- **External RFC Client**
  - External System
  - Client Program
  - Values
  - Result
  - SAP R/3 System
  - ABAP Function Module
  - Result

- **External RFC Server**
  - SAP R/3 System
  - ABAP Program
  - Values
  - Result
  - External System
  - Server Function 1
  - Server Function 2
External RFC Servers

- By "default", client doesn't need to supply logon information.
- 2 Ways of "attaching" External RFC Servers:
  - **Started Mode**
    - Application Server starts them remotely on-demand.
    - Commonly via Remote Shell or Remote Exec (!)
    - External Server is closed after operation.
  - **Registered Mode**
    - External Server registers 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 clients/servers.
- Available for all SAP supported platforms.
- Forward, backward and sideward compatible.
- An upper layer: JCo, .Net, ...
- Very good documentation.
- Delivered with examples.
External RFC Server Internals

• First of all, the server install available functions:

\[
\text{RfcInstallFunction}(\text{RFC\_FUNCTIONNAME} \ functionname, \\
\text{RFC\_ONCALL} \ f\_ptr, \\
\text{rfc\_char\_t} \ *\text{docu});
\]

• Listen and dispatch requests with \text{RfcDispatch()} loop.
• Requested function (\text{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
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.
  • Called Function Name.
  • Parameters Information and Content.
  • Tables Information and Content (may be compressed).
  • Client and Server information.
  • ...
## Traffic Analysis

| 01a0 | 00 00 00 00 00 00 00 06 05 14 00 10 5f 22 ea 45 5e |
| 01b0 | 22 c5 10 e1 00 00 00 c0 a8 02 8b 05 14 01 30 00 |
| 01c0 | 0a 72 66 63 5f 73 65 72 76 65 72 01 30 01 11 00 |
| 01d0 | 06 42 43 55 53 45 52 01 11 01 17 00 0b 81 bb 89 |
| 01e0 | 62 fc b5 3e 70 07 6e 79 01 17 01 14 00 03 30 30 |
| 01f0 | 30 01 14 01 15 00 01 45 01 15 05 01 00 01 01 05 |
| 0200 | 01 05 02 00 00 05 02 00 0b 00 03 36 34 30 00 0b |
| 0210 | 01 02 00 0e 5a 43 55 53 54 47 45 54 0d 4f 4e |
| 0220 | 45 59 01 02 05 14 00 10 5f 22 ea 45 5e 22 c5 10 |
| 0230 | e1 00 00 00 c0 a8 02 8b 05 14 02 01 00 09 43 4c |
| 0240 | 49 45 4e 54 5f 49 44 02 01 02 03 00 08 43 55 53 |
| 0250 | 54 30 30 31 00 02 03 ff ff 00 00 ff ff 00 00 01 |
| 0260 | c7 00 00 3e 80 |

...
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.

\[
\text{for each CHAR in CLEAR\_TEXT\_PASS} \\
\quad \text{OBFUSCATED\_PASS}[i] = \text{CHAR} \oplus \text{KEY}[i]
\]

\[
\text{KEY\_TO\_THE\_KINGDOM} = [0x96, 0xde, 0x51, 0x1e, 0x74, 0xe, \\
0x9, 0x9, 0x4, 0x1b, 0xd9, 0x46, 0x3c, 0x35, 0x4d, 0xe5, \\
0x55, 0xc5, 0xe5, 0xd4, 0xb, 0xa0, 0xdd, 0xd6, 0xf5, \\
0x21, 0x32, 0xf, 0xe2, 0xcd, 0x68, 0x4f, 0x1a, 0x50, \\
0x8f, 0x75, 0x54, 0x86, 0x3a, 0xbb]
\]
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.
Function Analysis: RFC_PING

• A RFC ping
• Connects to the target system, analyzing its availability.
• No need for valid logon data.
• Available in External Systems and R/3.

This function can be used to check for availability of remote RFC Server.
Function Analysis: RFC_SYSTEM_INFO

- Obtain RFC server system information.
- No need for logon data!
- Available in External Systems and R/3.

What can we get?
- SAP Kernel Version
- Hostname
- Timezone
- Database Engine
- Database Host
- SAP System ID
- Operating System
- ...
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

Any of this functions can be called, just as regular installed functions...
Function Analysis: RFC_TRUSTED_SYSTEM_SECURITY

- Designed for internal use by SAP only.
- Available in External Systems.

**Impact:**
This function can be used to check existence of users and groups in an External system, its domain and trusted domains.
Function Analysis: RFC_SET_REG_SERVERPROPERTY

- Enables the definition of properties of External Registered Servers.
- Available in External Systems.

Impact:
Calling this function with a special parameter would render an External Registered Server unavailable to other clients (Denial of Service).
Function Analysis: RFC_START_GUI

• Starts SAPGUI on FrontEnd systems.
• Available in External Systems.

Impact:
Calling this function with a specially crafted parameter would result in the ability to run remote arbitrary commands over the External Server system.
Function Analysis: SYSTEM_CREATE_INSTANCE

- Enables the creation of remote objects, where an object adapter is available.
- Available in External Systems.

Impact:
Calling this function with a specially crafted parameter would result in the ability to run remote arbitrary commands over the External Server system.
Function Analysis: RFC_START_PROGRAM

- Enables the execution of programs on External Servers.
- Commands are restricted by the RfcAllowStartProgram() function:

  - No RfcAllowStartProgram() => Remote execution disabled

  - RfcAllowStartProgram("foo.exe") => Execution of "foo.exe" is authorized.

  - RfcAllowStartProgram(NULL) => All commands are authorized.
Function Analysis: RFC_START_PROGRAM (cont.)

**Impact:**
Calling the functions with specially crafted parameters would allow an attacker to:

- Obtain information about configuration of the remote server.
- Execute remote arbitrary commands, exploiting a buffer overflow vulnerability.
**Function Analysis: RFC_START_PROGRAM (cont.)**

What happens if `RfcAllowStartProgram("dumbprogram.exe")`?

- **Analysis** of `RfcAllowStartProgram()` revealed that only the first N bytes of incoming program are verified, where N is the length of the allowed program.

- **You know** an allowed program, you can execute another:
  
  "dumbProgram.exe../../../../../path/to/evil/program.exe"

- **According to SAP**, external server developers should validate against this type of attacks...
**RFCEXEC**

- Bundled with the RFCSDK.
- Released as an example.
- Not intended for productive use.
- Installs the following functions:
  - RFC_RAISE_ERROR
  - RFC_MAIL
  - RFC_REMOTEPIPE
  - RFCREMOTEFILE
  - RFCREMOTEEXEC

- Protected through `rfceexec.sec` file directives.
**SAPXPG**

- Executable shipped with SAP R/3 Application Server.
- Used for execution of external commands and programs.
- Installs the following functions:
  - `SAPXPG_END_XPG`
  - `SAPXPG_START_XPG_LONG`
  - `SAPXPG_START_XPG`
Advanced Attacks
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 ABAP developer. (No step-by-step demonstration)
The Gateway Monitor

• The **Gateway Server** has a configuration parameter for controlling Gateway Monitor access.

<table>
<thead>
<tr>
<th>gw/monitor</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Monitor is disabled.</td>
</tr>
<tr>
<td>1</td>
<td>Local access only.</td>
</tr>
<tr>
<td>2</td>
<td>Remote access enabled.</td>
</tr>
</tbody>
</table>

• 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 `reginfo` 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...
**Evil Twin illustrated...**

- Legitimate External RFC Server registers at SAP R/3 Gateway.
Evil Twin illustrated...

- Legitimate External RFC Server registers at SAP R/3 Gateway.
- Innocent lamb connection establishment...
Evil Twin illustrated...

- Legitimate External RFC Server registers at SAP R/3 Gateway.
- Innocent lamb connection establishment...
- Client performs RFC call and Server answers politely.
- An external RFC malicious client/server appears in scene... (don’t be afraid, it’s controlled)
- The attacker connects with the original RFC server, preventing him from serving requests from other clients.
- Now, the same malicious client/server connects with the SAP R/3 Gateway, registering itself with the same ID as the original external server.
- Now, the same malicious client/server connects with the SAP R/3 Gateway, registering itself with the same ID as the original external server.
- All future connections to the REG1 server will be attended 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.
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.
A Wiser (and Stealth) Evil Twin: MITM Attacks

- So we have the same scenario, legitimate client and External RFC Server, the SAP R/3 Server and the SAP Gateway.
A Wiser (and Stealth) Evil Twin: MITM Attacks

- Here we go again, blocking valid connections to the innocent External RFC Server
- Here we go again, blocking valid connections to the innocent External RCF Server
- Now, the same malicious client/server connects with the SAP R/3 Gateway, and register itself with the same ID as the original external server.
- This time, every RFC call received is Logged/Modified, and forwarded to the original external server.
A Wiser (and Stealth) Evil Twin: MITM Attacks

- This time, every RFC call received is Logged/Modified, and forwarded to the original external server.
Attacking the R/3 with a Registered Server

- RFC Interface allows client / servers to perform "callbacks".

![Diagram showing RFC Client and RFC Server interacting through RFC Calls and sending data and results](image_url)
Attacking the R/3 with a Registered Server (cont.)

• We can perform "callbacks" to R/3 systems.
• The RFC Call is executed under 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.
  4. Perform RFC callback.
  5. If user has SAP_ALL...Bingo!
- Yes, again the same scenario: the valid client, the valid External RFC Server, the SAP R/3 Server and the SAP Gateway
- Again, the same malicious client/server connects with the SAP R/3 server, and register itself with the ID of the original external server.
Attacking the R/3 with a Registered Server (cont.)

- But now, when a RFC call is received...
But now, when a RFC call is received, we perform a callback...
- But now, when a RFC call is received, we perform a callback...
- **SAP R/3 Application Server OWNED!!**
Tool Release:
sapyto
sapyto

• First public framework for performing SAP Penetration Tests.
• Core dependencies: SAP RFC Library and saprfc module.
• Plugin based.
• Audit & Attack Plugins.
• Shipped with plugins for exploiting RFC vulnerabilities, auditing SAP R/3 configuration, launching described attacks, etc..
• Developed in Python and C.
Available Plugins in Beta Version

• Audit:
  • RFC Ping.
  • Registration of External Servers.
  • Detection of RFCEEXEC.
  • Detection of SAPXPG.
  • Get system information.
  • Get server documentation.
Available Plugins in Beta Version (cont.)

• **Attack:**
  - RFC_START_PROGRAM Directory Transversal.
  - Run commands through RFCEXC.
  - Run commands through SAPXPG.
  - StickShell.
  - Evil Twin Attack.
  - Get remote RFCShell.

• **Tools:**
sapyto Demonstration
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.
• Network must be properly segmented.
• Advanced attacks described can be avoided with proper configuration + patches.
Coming soon...

- Attacking SAP clients.
- SAP Backdoors.
- ABAP Worms.
- Exploiting Trusted Systems.
- RFC Fuzzer.
- ...

Stay tunned!
Questions?
Thank you!