SIS203

SAP Runs SAP – Remote Function Call: Gateway Hacking and Defense

This presentation describes experiences gained in real-life implementation of RFC gateway* protection at SAP

Bjoern Brencher / SAP Global IT – Security & Risk Office

SAP TechEd 2012

* RFC gateway is a technical component in the SAP kernel. It is not the product SAP NetWeaver Gateway.

Disclaimer

This presentation outlines our general product direction and should not be relied on in making a purchase decision. This presentation is not subject to your license agreement or any other agreement with SAP. SAP has no obligation to pursue any course of business outlined in this presentation or to develop or release any functionality mentioned in this presentation. This presentation and SAP's strategy and possible future developments are subject to change and may be changed by SAP at any time for any reason without notice. This document is provided without a warranty of any kind, either express or implied, including but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement. SAP assumes no responsibility for errors or omissions in this document, except if such damages were caused by SAP intentionally or grossly negligent.

This presentation describes and reflects experiences gathered during the real-life implementation of the RFC gateway protection in systems at the company SAP. Some information presented is simplified. Implementation in systems at other companies may require additional steps.

Abstract

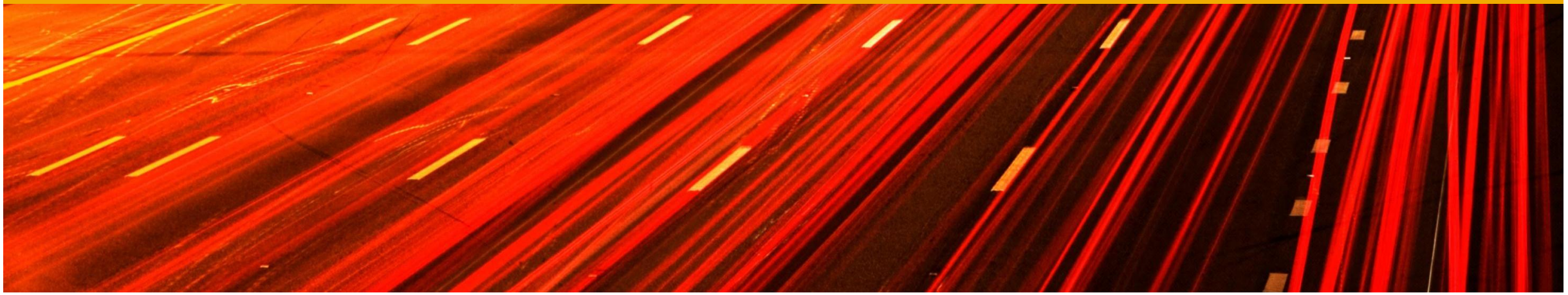
For the first time, SAP's own internal security department will provide insight into the SAP internal project of how to secure remote function call (RFC) communication via the "gateway" component. RFC is one of the main communication technologies for SAP NetWeaver-based systems. RFC is handled by gateway, which is a technical component running on every SAP NetWeaver Application Server – ABAP and Java. Gateway access control is one of the most crucial security configurations in SAP NetWeaver systems. After demonstrating how to break into SAP systems that lack gateway access control, you will learn how to design access control for highly integrated and connected SAP landscapes and how to implement it without business disruption. In addition, a monitoring strategy for gateway security will be presented.

Agenda

Hackers & RFC gateway

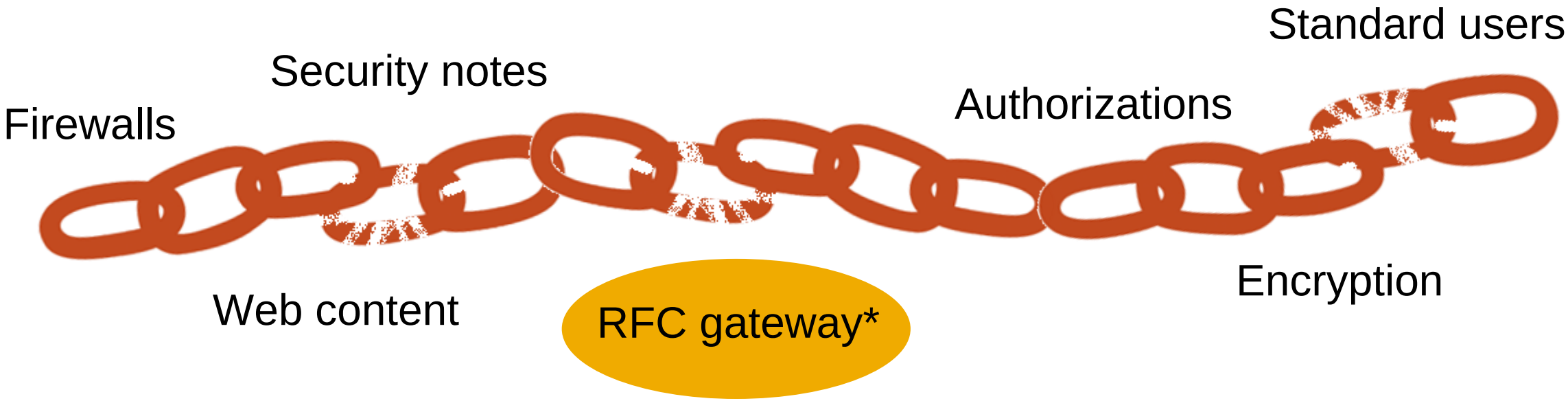
Live hacking demo – exploiting insecure RFC gateway configurations

SAP Runs SAP: How do we secure the RFC gateway?



Hackers & RFC gateway

Is your SAP environment secure?



* RFC gateway is a technical component in the SAP kernel. It is not the product SAP NetWeaver Gateway.

Vulnerabilities of RFC gateway disclosed on security conference

2007

Security conference – Blackhat USA

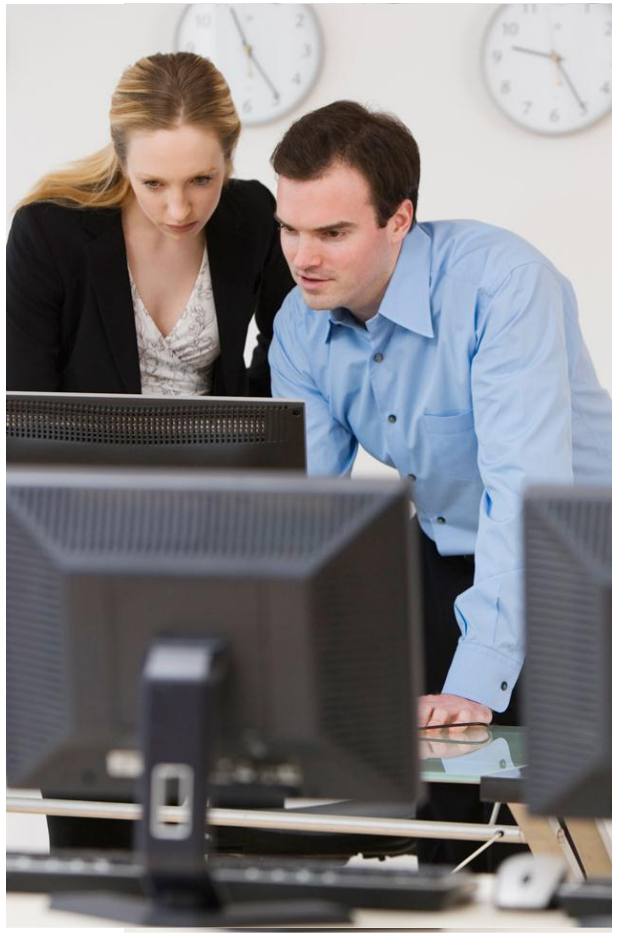
- Mariano Nuñez Di Croce –
  Attacking the Giants: Exploiting SAP Internals

SAP Runs SAP: What we did to protect our own systems at SAP

2007

Task force initiated with SAP Product Development

- Evaluate the security issue with SAP Product Development and the external researcher
- Analyze and discuss protection possibilities as protection is only possible by configuration



2008

SAP internal project started

- Define protection of the RFC gateway for our own SAP business systems
- Run pilot implementation for 1 system landscape
- Rollout to all critical landscapes
- Define monitoring procedure

More presentations about the same RFC gateway vulnerabilities

2007

Security conference – Blackhat USA

- Mariano Nuñez Di Croce –
  Attacking the Giants: Exploiting SAP Internals

2010

Security conference – 27C3, the 27th. Chaos Communication Congress

- Ertunga Arsal – Rootkits and Trojans On Your SAP Landscape

2012

Security conference – CRESTCon

- Dave Hartley – SAP Slapping

Security conference – Troopers

- Mariano Nuñez Di Croce – Real-World Cyber Threats to SAP Systems
- Ralf Kempf – SAP Solution Manager from the hackers point of view

Protection of RFC gateways at SAP customers

Challenges for SAP Customers

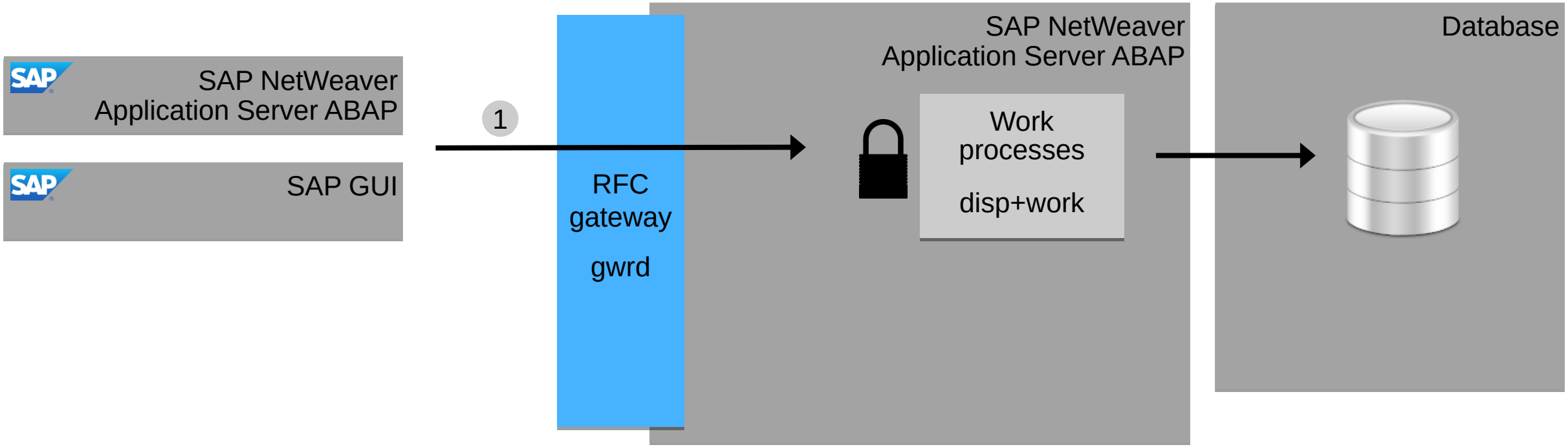
- Protection requires configuration on customer side
- Very technical topic with high complexity
- Elaborate implementation of security measures

Improvements by SAP (supported by our implementation experience)

- Reduced implementation times of security measures
- Improved documentation on vulnerability and security measures
- Secure default configuration of RFC gateways as of SAP NetWeaver Application Server ABAP 7.31

SAP customers need to secure their RFC gateways

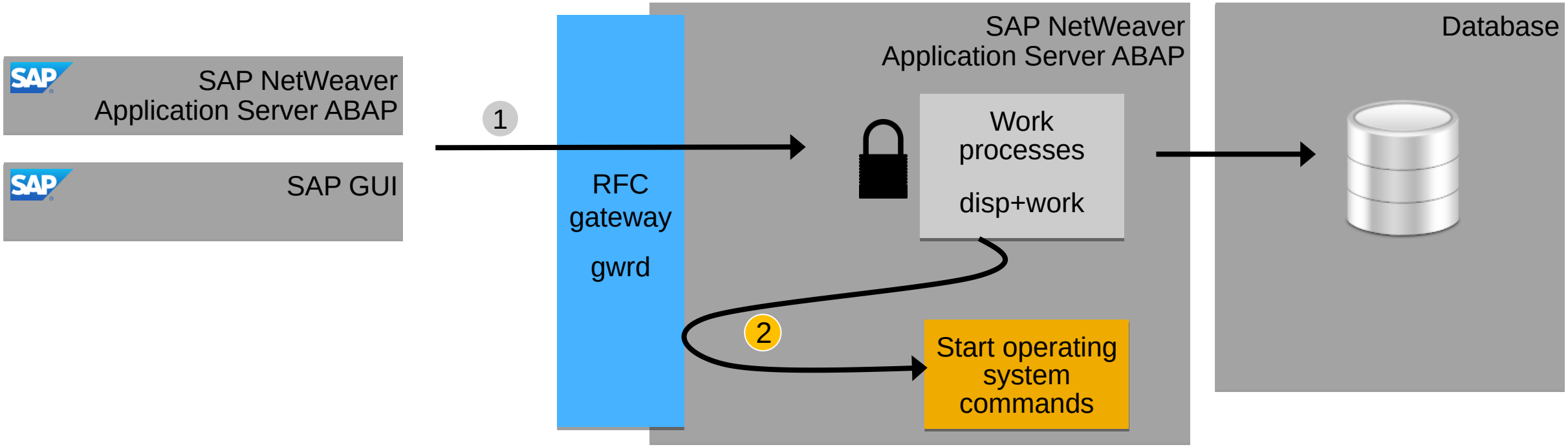
What is the RFC gateway? – Quick introduction – Part 1



Scenarios of RFC communication

1 Call to ABAP function modules

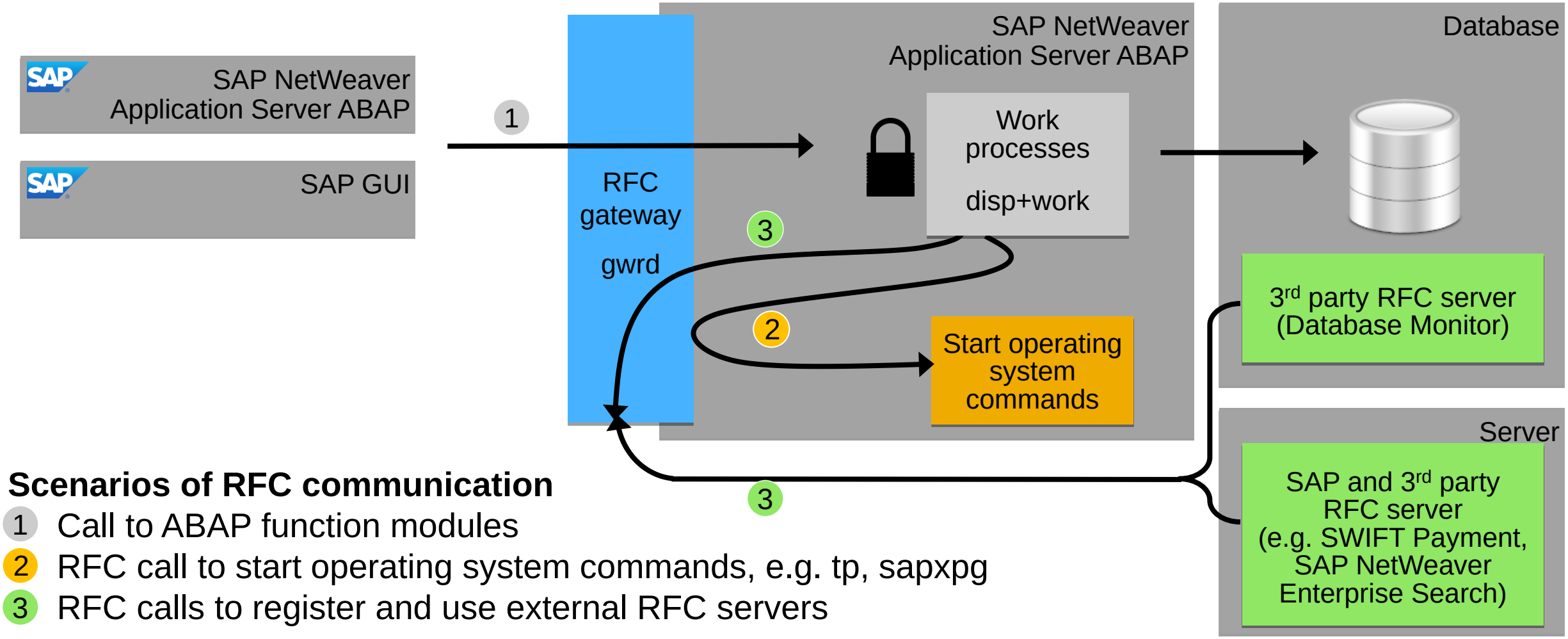
What is the RFC gateway? – Quick introduction – Part 2



Scenarios of RFC communication

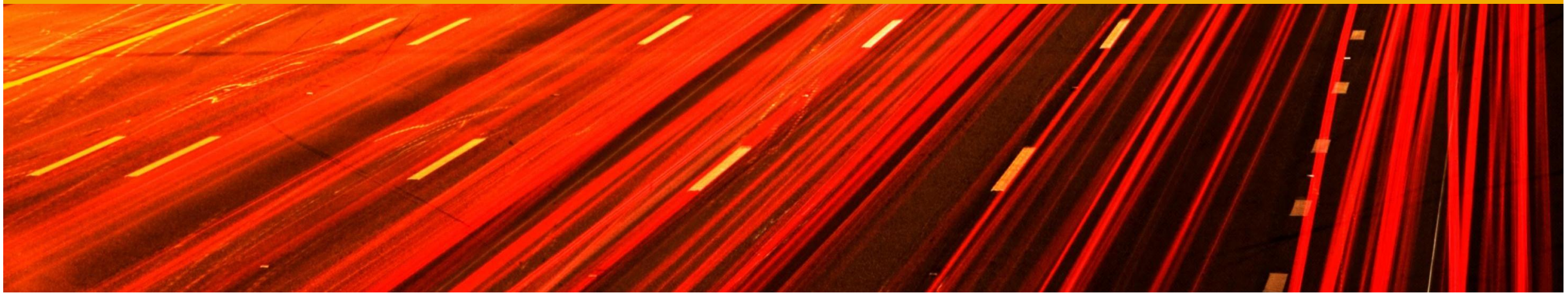
1. Call to ABAP function modules
2. RFC call to start operating system commands, e.g. tp, sapxpg

What is the RFC gateway? – Quick introduction – Part 3



Scenarios of RFC communication

1. Call to ABAP function modules
2. RFC call to start operating system commands, e.g. tp, sapxpg
3. RFC calls to register and use external RFC servers

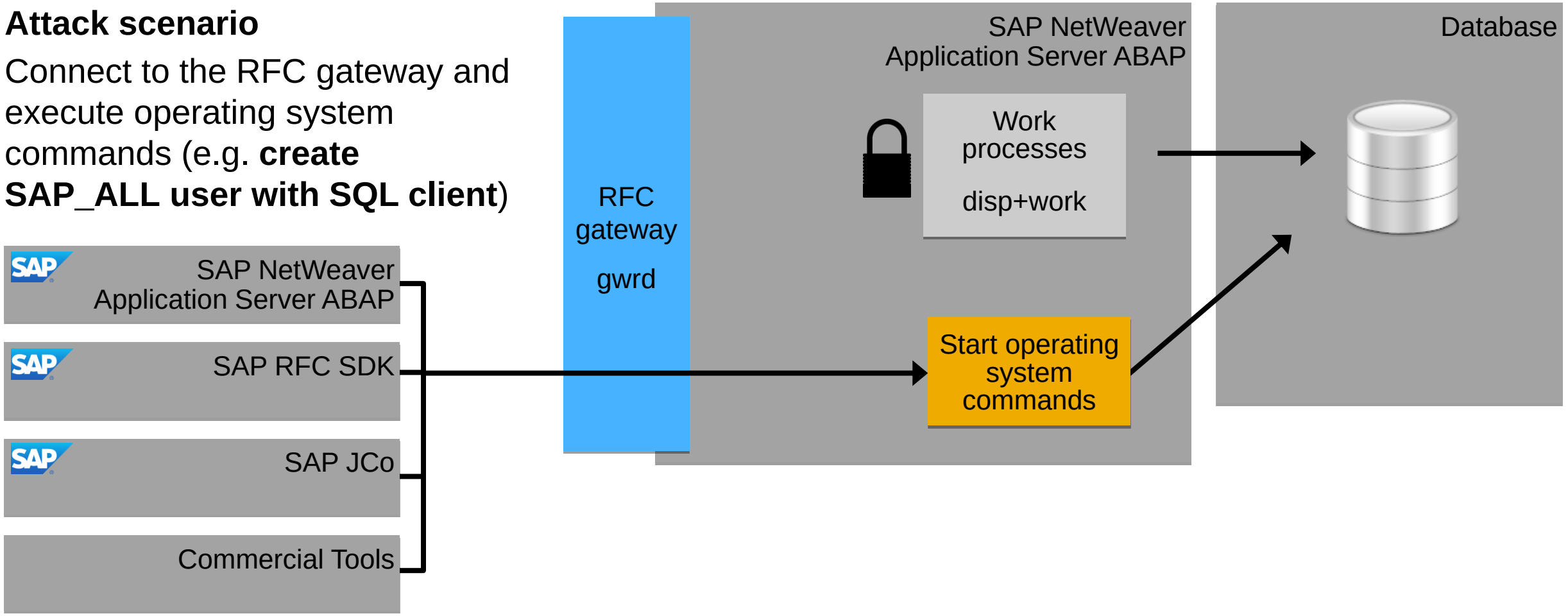


Live hacking demo – exploiting insecure RFC gateway configurations

Let’s hack the SAP system misusing the RFC gateway

Attack scenario

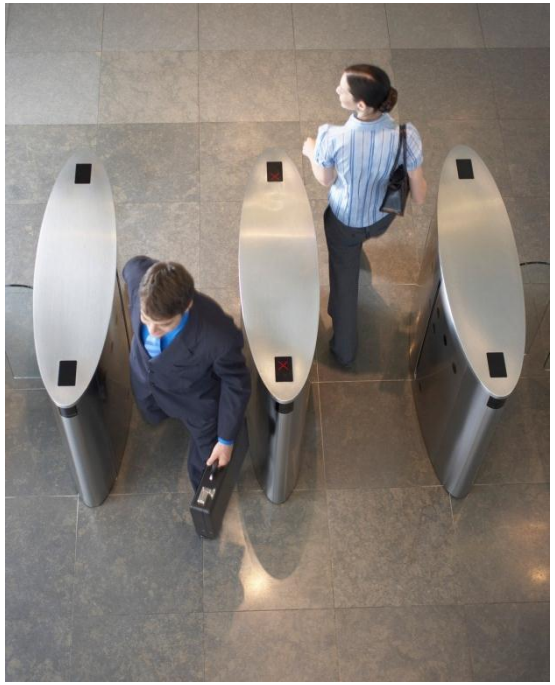
Connect to the RFC gateway and execute operating system commands (e.g. **create SAP_ALL user with SQL client**)



Impact of unprotected RFC gateway

Risk and impact of an unprotected RFC gateway

- Full control over SAP systems bypassing any other SAP security controls
- Manipulation of data which endangers legal compliance
- Data theft
- No traceability due to missing audit trail
- Unavailability of data and systems

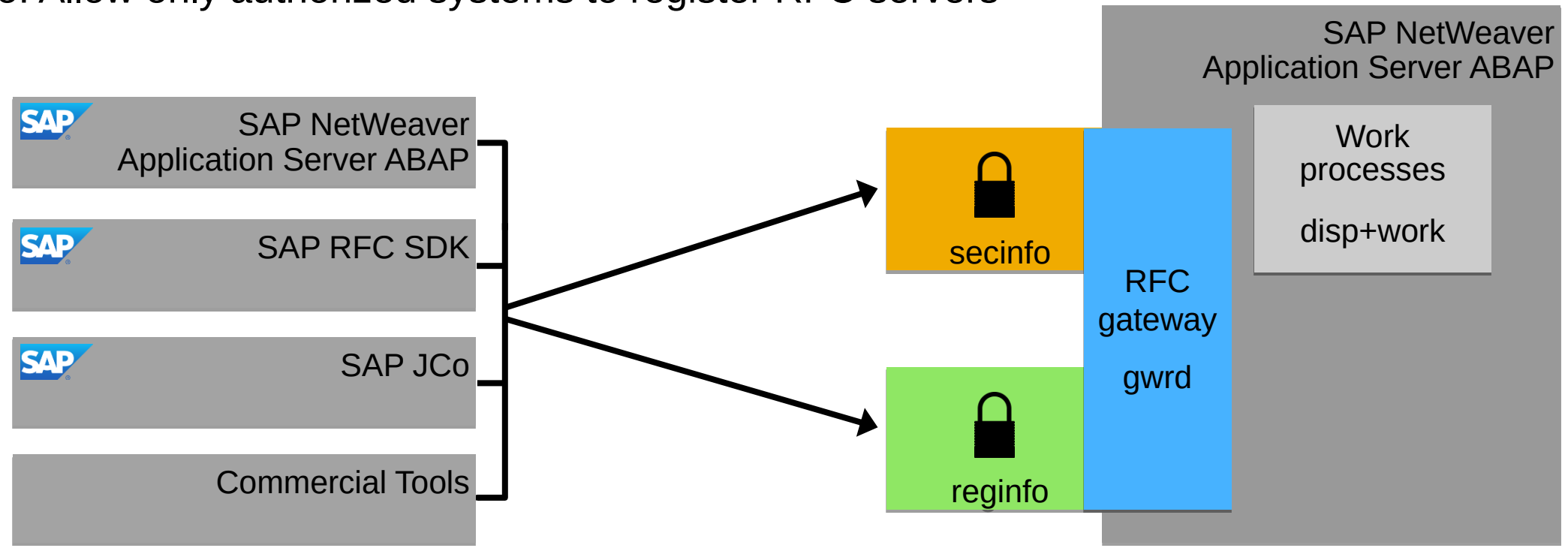


Unprotected RFC gateways allow manipulation of business processes in SAP systems

Protection of the RFC gateway – secinfo and reginfo

RFC gateway protection

- Secinfo: Allow only authorized systems to execute operating system commands
- Reginfo: Allow only authorized systems to register RFC servers



Protection in detail – started RFC server (secinfo)

File on operating system (defined by gw/sec_info) with a list of entries like

USER=*, ***USER-HOST*=<source>, *HOST*=<destination>**, *TP*=*

- User that wants to start the program
- System that wants to start the program (source system)
- System where the program should be started (destination system)
- Name of the program to be started

Useful variables for USER-HOST and HOST

- *local* – All local interfaces of 1 application server
- *internal* – All interfaces of all application / database servers belonging to the same SAP system

Protection in detail – registered RFC server (reginfo)

File on operating system (defined by gw/reg_info) with a list of entries like

TP=*, ***HOST*=<source>**

Name of the program to be started

System that wants to start the program (source system)

Useful variables for HOST

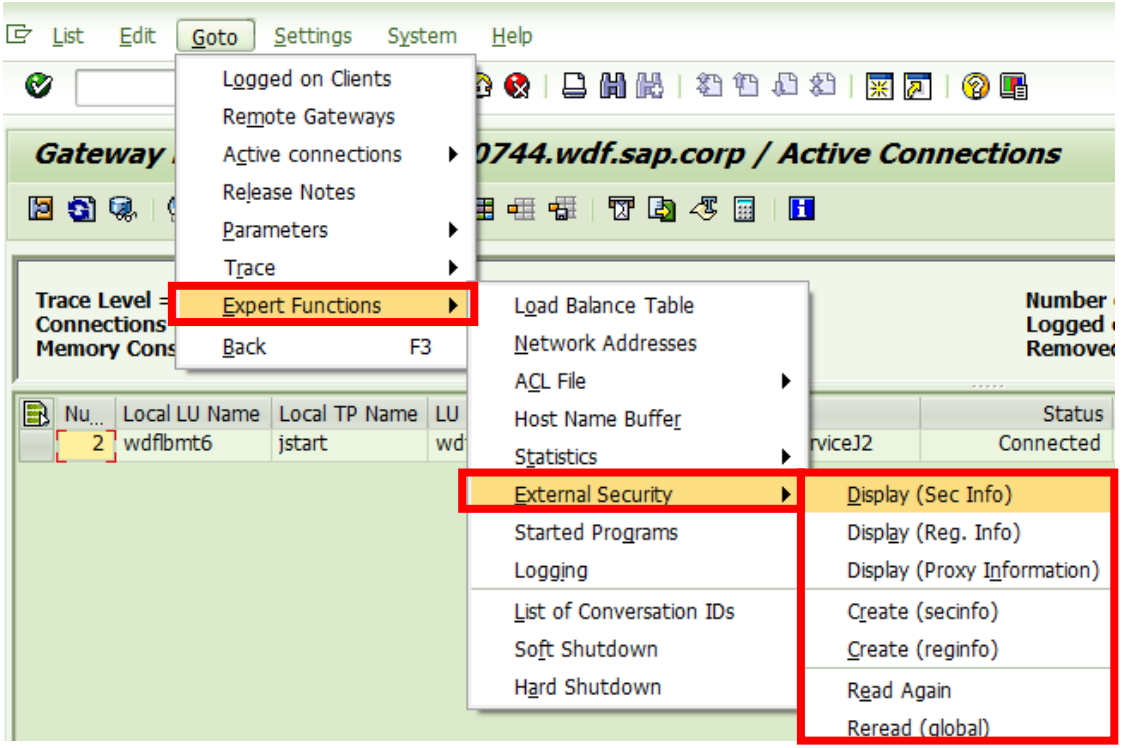
- *local* – All local interfaces of 1 application server
- *internal* – All interfaces of all application / database servers belonging to the same SAP system

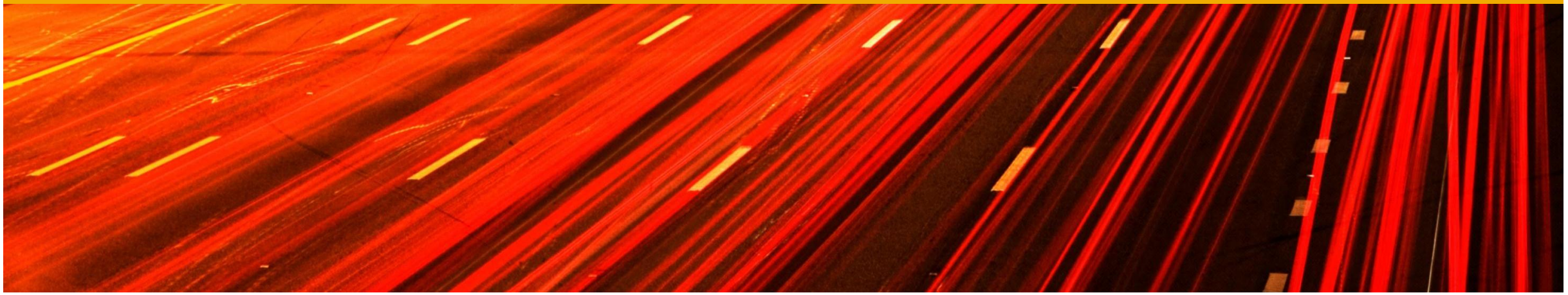
RFC gateway protection – Where to find the settings?

In SAP NetWeaver Application Server ABAP, display settings of RFC gateway protection

- Transaction SMGW – Expert Functions External Security
  - Display (Sec Info)
  - Display (Reg. Info)
  - Create (secinfo)
  - Create(reginfo)
  - Read Again
  - Reread (global)

- Change of secinfo & reginfo content has to be done on operating system level

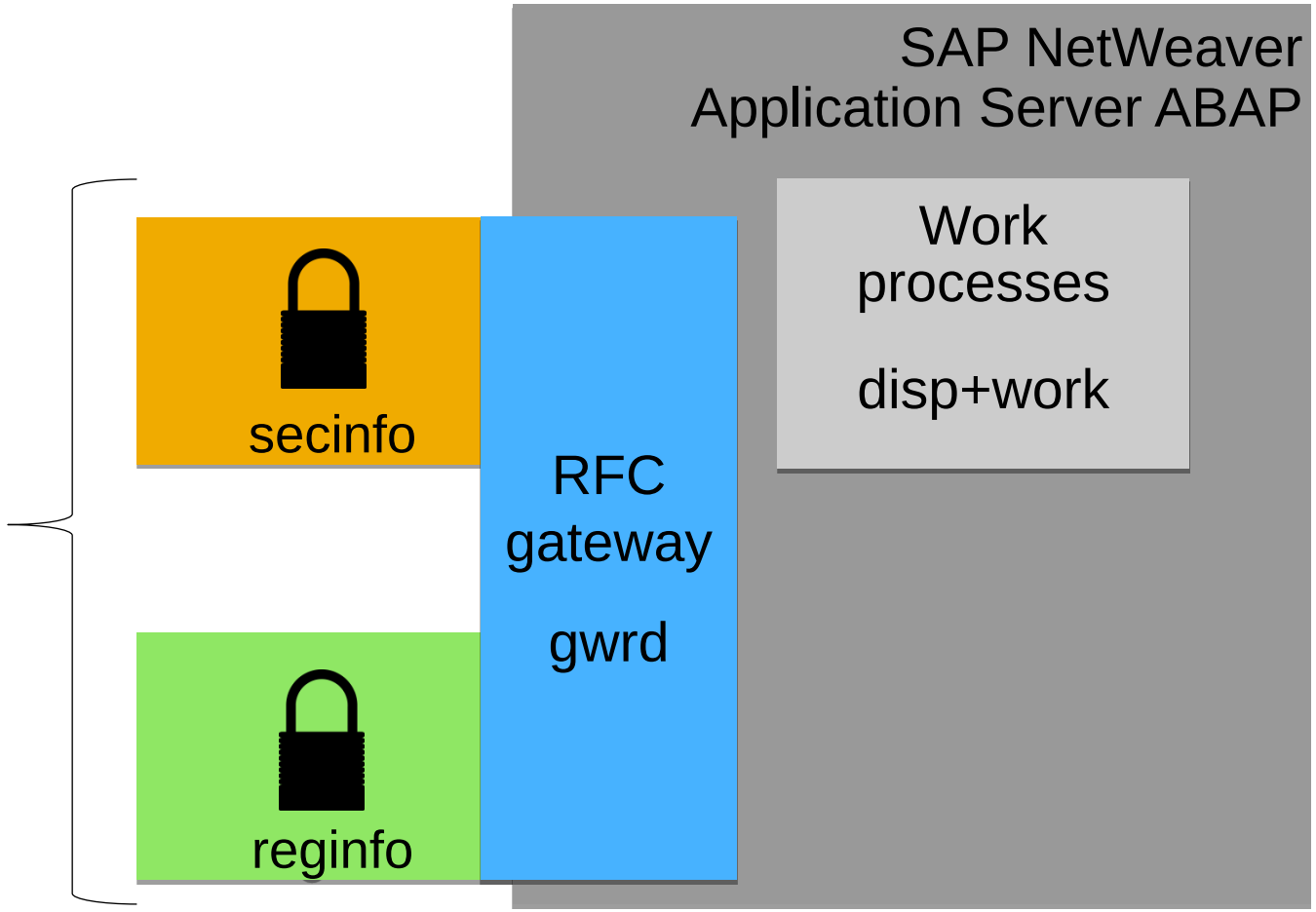




SAP Runs SAP: How do we secure the RFC gateway?

The Challenge! – Find the right entries

How to identify systems that need to be added?

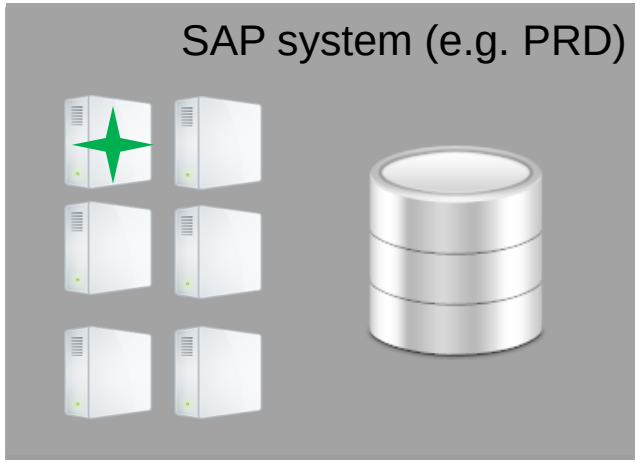


SAP Runs SAP: Protection in detail – started RFC server (secinfo)

Recommended entries

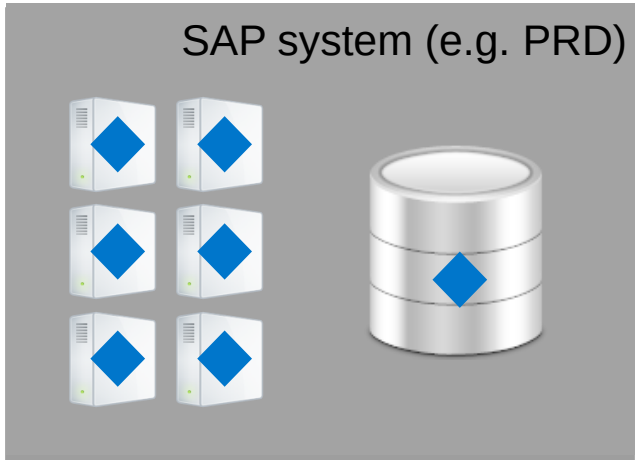
Allow local application server traffic

USER=* USER-HOST=**local** HOST=**local** TP=*



Allow traffic between all application servers and the database server of an SAP system

USER=* USER-HOST=**internal** HOST=**internal** TP=*



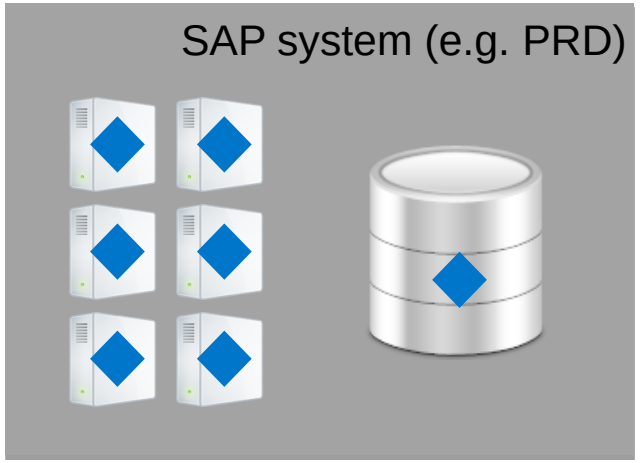
According to our experience at SAP this covers about 99% of all secinfo traffic!

SAP Runs SAP: Protection in detail – registered RFC server (reginfo)

Recommended entries

Allow registration of RFC servers between all application servers and the database server

TP=*, HOST=local
TP=*, HOST=internal



reginfo

The Challenge! Additional customer specific entries

Allow registration of RFC servers from required systems for 3rd party software integration, e.g.

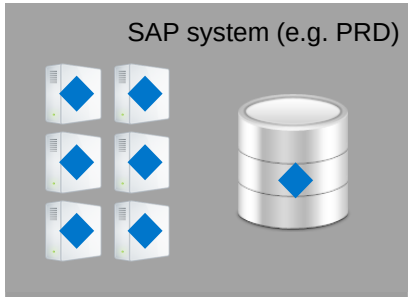
TP=*, HOST=search.demo.sap.corp
TP=*, HOST=payment.demo.sap.corp
TP=*, HOST=10.2.4.2
TP=*, HOST=<Unknown system>

SAP NetWeaver Enterprise Search

Unknown system

SAP NetWeaver Portal

3rd Party SWIFT Payment



SAP Runs SAP: How to implement RFC gateway protection?

Prerequisite: Use the highest SAP kernel patch level as lots of things were improved and bugs fixed

Original way:
Low business risk, but huge effort

- Activate logging of RFC gateway
- Analyze logs
- Create secinfo & reginfo files manually
- Activate secinfo & reginfo

Additional way:
More business risk, but less effort

- Use creation reports for initial secinfo & reginfo
- Activate proposed secinfo & reginfo
- Monitor logs for rejected connections closely
- Add rejected entries to secinfo & reginfo manually

With SAP kernel 7.21: Introduction of simulation mode

SAP Runs SAP: Internal implementation of RFC gateway protection

Scope of our SAP internal implementation

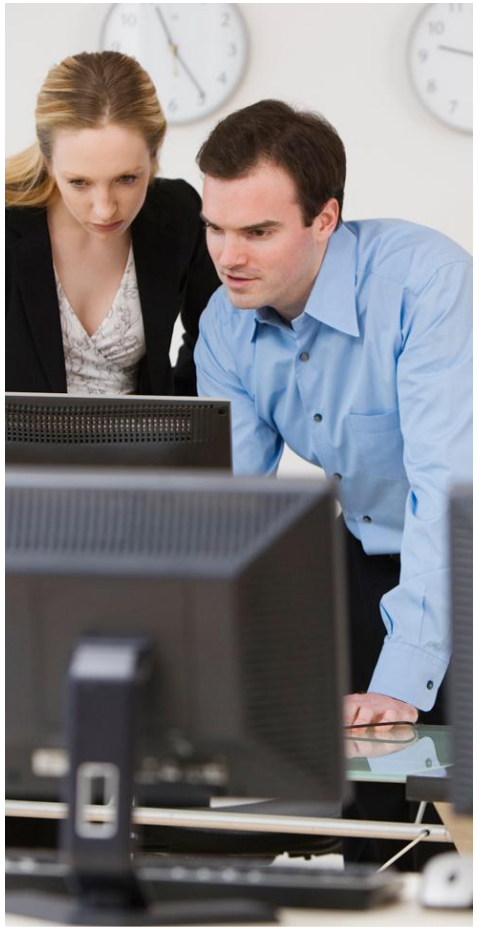
- Business critical systems of SAP (e.g. SAP's own SAP ERP system)
- About 40 productive landscapes with roughly 200 single systems

Timelines of our SAP internal implementation

- In 2007, start with first analysis of RFC gateway protection
- In 2008, first pilot implementation
- By end of 2009, rollout completed to productive landscapes

Further Details of our SAP internal implementation

- Our project staffing: SAP Global IT Security & Risk Office with Basis Administrators and a close link to SAP Product Development
- Our implementation was done with log analysis, as other ways were not available
- Implementation effort for rollout: ~200 person days (~5 person days per landscape)
- Estimated ongoing maintenance effort: ~0.25 person day per year per landscape



SAP Runs SAP: Internal implementation of RFC gateway protection

Issues faced during implementation

- Limited knowledge about RFC gateway and its use
- No references how to implement RFC gateway protection in a real-life environment with productive SAP NetWeaver systems
- Adjustment of implementation approach after pilot
- RFC gateway logging only available in latest SAP NetWeaver release
- No tools / scripts available to analyze generated RFC gateway log files
- Some bugs caused delays, e.g.
  - RFC gateway logging not complete
  - Network masks not supported in secinfo / reginfo for older SAP kernel releases
  - RFC gateway protection can be circumvented under special circumstances

SAP Runs SAP: Importance of RFC gateway monitoring

RFC gateway protection depends on several independent settings

- Profile parameter (gw/reg_no_conn_info, gw/sec_info, gw_reginfo)
- Content of files secinfo and reginfo on operating system
- Successful load of content into RFC gateway memory

Usage of SAP Solution Manager – Configuration Validation for RFC gateway protection at SAP

Configuration Items

		Compliant (1=Yes, 0=No, ''=Not valuated)				
ConfigStore Name	Compliance System	ABC 12345678	DEF 12345678	GHI 12345678	JKL 12345678	MNO 12345678
ABAP_INSTANCE_PAHI	No		0			0
	Yes	1	1	1	1	1
GW_REGINFO	No					
	Yes	1	1	1	1	1
GW_SECINFO	No					
	Yes	1	1	1	1	1

Summary

Three key messages as take away!

RFC gateway is one of the **common points to attack** in an SAP NetWeaver system

Implementation of **RFC gateway protection** is not easy but **manageable**

SAP customers need to **take action** and secure RFC gateways of their SAP systems

- Do it yourself
- Use SAP offered services

Feedback

Please complete your session evaluation for SIS203.

Bjoern Brencher, SAP Global IT Security & Risk Office
bjoern.brencher@sap.com

Thanks for attending this SAP TechEd session.

Further Information

RFC gateway documentation

Security Settings in the SAP Gateway
http://help.sap.com/saphelp_nw73ehp1/helpdata/en/48/b2096e7895307be10000000a42189b/frameset.htm

SAP Security Note 1408081 – Basic settings for reg_info and sec_info
https://service.sap.com/sap/support/notes/1408081

SAP Note 1425765 – Generating sec_info reg_info
https://service.sap.com/sap/support/notes/1425765

SAP Security Note 1444282 – gw/reg_no_conn_info settings
https://service.sap.com/sap/support/notes/1444282

SAP Note 1689663 – GW: Simulation mode for reg_info and sec_info
https://service.sap.com/sap/support/notes/1689663

Further Information

SAP offered services to support RFC gateway protection

SAP Global IT Security & Risk Office
Contact ralph.salomon@sap.com

SAP Consulting – SAP Note 1504652 – Consulting: Secure Configuration of Application Server ABAP https://service.sap.com/sap/support/notes/1504652

SAP Active Global Support – Security Services
Contact securitycheck@sap.com

SAP Public Web

SCN Security Community
http://scn.sap.com/community/security

SCN Security Forum
http://scn.sap.com/community/security/content

Further Information

SAP Public Web

SAP System Recommendations “Secure Configuration SAP NetWeaver Application Server ABAP”:
http://scn.sap.com/docs/DOC-17149

SAP Solution Manager Configuration Validation
https://service.sap.com/changecontrol

SAP Education and Certification Opportunities

www.sap.com/education

ADM960 – SAP NetWeaver AS – Security
P_ADM_SEC_70 – SAP Certified Technology Professional – Security with SAP NetWeaver 7.0

SAP Runs SAP: Some advice on gw/reg_no_conn_info

RFC gateway protection and gw/reg_no_conn_info

- Due to a bug, RFC gateway protection can be circumvented under special circumstances
- Set gw/reg_no_conn_info to **1 or an odd value** (1,3,5,…127) to disable this security bypass
  gw/reg_no_conn_info is used to activate different RFC gateway functionalities by binary addition

Note	Description	Binary value	Example #1	Example #2
1298433	**Bypassing security in reginfo & secinfo**	**1**	**X**	**X**
1434117	Bypassing sec_info without reg_info	2		X
1465129	CANCEL registered programs	4	X	
1473017	Uppercase/lowercase in the files reg_info and sec_info	8	X	X
….	...			
	Calculated value for gw/reg_no_conn_info		13	11

© 2012 SAP AG. All rights reserved.