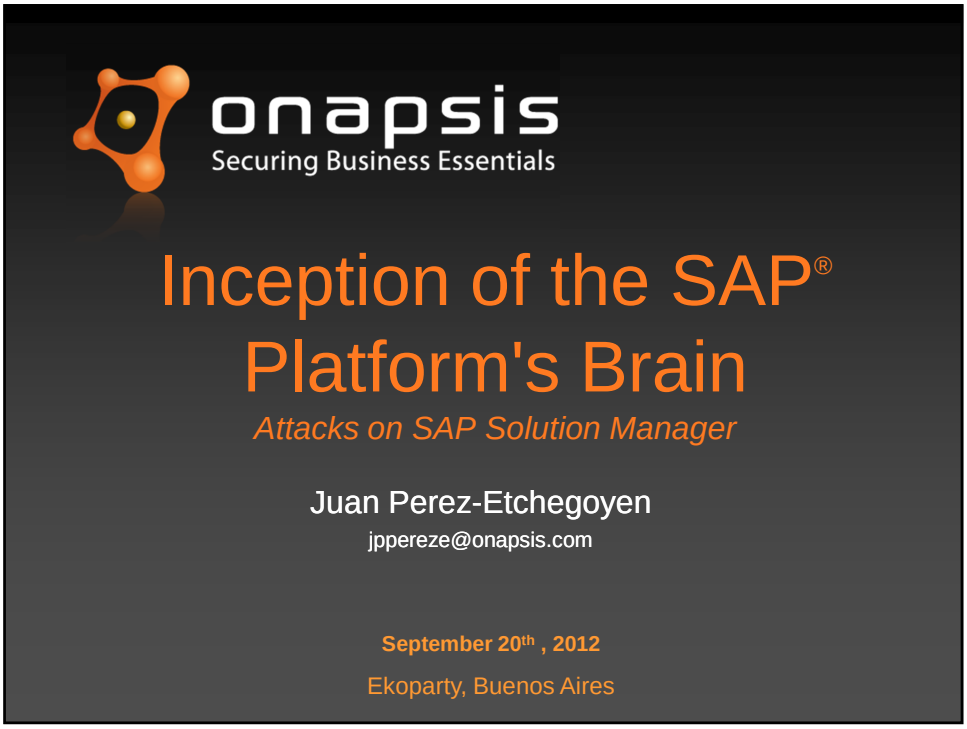
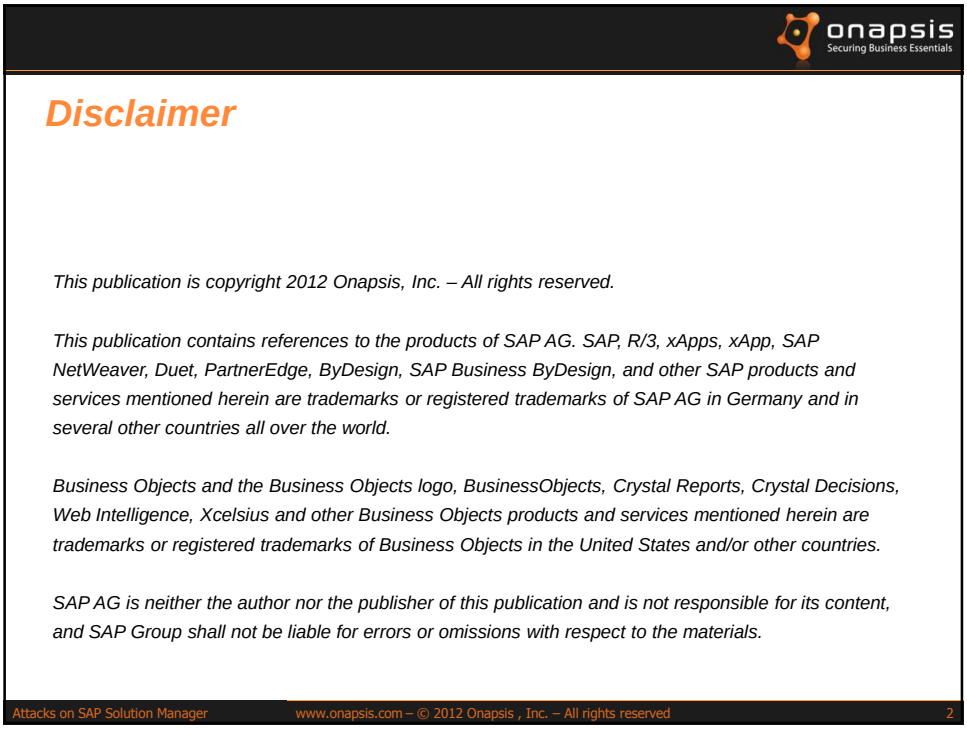

onapsis
Securing Business Essentials
Inception of the SAP® Platform's Brain
Attacks on SAP Solution Manager
Juan Perez-Etchegoyen
jppereze@onapsis.com
September 20th , 2012
Ekoparty, Buenos Aires


onapsis
Securing Business Essentials
Disclaimer
This publication is copyright 2012 Onapsis, Inc. – All rights reserved.
This publication contains references to the products of SAP AG. SAP, R/3, xApps, xApp, SAP NetWeaver, Duet, PartnerEdge, ByDesign, SAP Business ByDesign, and other SAP products and services mentioned herein are trademarks or registered trademarks of SAP AG in Germany and in several other countries all over the world.
Business Objects and the Business Objects logo, BusinessObjects, Crystal Reports, Crystal Decisions, Web Intelligence, Xcelsius and other Business Objects products and services mentioned herein are trademarks or registered trademarks of Business Objects in the United States and/or other countries.
SAP AG is neither the author nor the publisher of this publication and is not responsible for its content, and SAP Group shall not be liable for errors or omissions with respect to the materials.
Attacks on SAP Solution Manager
www.onapsis.com – © 2012 Onapsis , Inc. – All rights reserved
2

Who is Onapsis, Inc.?

- Company focused in the **security of ERP systems and business-critical infrastructure** (SAP®, Siebel®, Oracle® E-Business Suite™, PeopleSoft®, JD Edwards® …).
- Working with Global Fortune-100 and large governmental organizations.
- What does Onapsis do?
  - Innovative ERP security software (Onapsis X1, Onapsis Bizploit, Onapsis IA).
  - ERP security consulting services.
  - Trainings on business-critical infrastructure security.

Who am I?

- **Juan Pablo Perez Etchegoyen, CTO** at **Onapsis.**
- Discovered several **vulnerabilities** in SAP and Oracle ERPs...
- **Speakers/Trainers** at BlackHat, HITB, Ekoparty, Source, ...
- Collaborator in the “SAP Security In-Depth” publication.

Agenda

- Introduction
- The SAP Solution Manager (SolMan)
- Central User Administration (CUA)
- Computing Center Management System (CCMS)
- Solution Manager Diagnostics (SMD)
- Conclusions

Introduction

What is SAP?

- **Largest** provider of **business management solutions** in the world.
  - More than 140.000 implementations around the globe.
  - More than 90.000 customers in 120 countries.

- Used by **Global Fortune-1000 companies**, **governmental organizations** and **defense agencies** to **run their every-day business processes.**
  - Such as Revenue / Production / Expenditure business cycles.

FINANCIAL PLANNING TREASURY PAYROLL
SALES **INVOICING** **LOGISTICS**
BILLING
PRODUCTION PROCUREMENT

A Business-Critical Infrastructure

- **ERP systems store and process the most critical business information in the Organization.**
- **If the SAP platform is breached**, an intruder would be able to perform different attacks such as:
  - **ESPIONAGE:** Obtain customers/vendors/human resources data, financial planning information, balances, profits, sales information, manufacturing recipes, etc.
  - **SABOTAGE:** Paralyze the operation of the organization by shutting down the SAP system, disrupting interfaces with other systems and deleting critical information, etc.
  - **FRAUD:** Modify financial information, tamper sales and purchase orders, create new vendors, modify vendor bank account numbers, etc.

Over 95% of the SAP systems we evaluated were exposed to espionage, sabotage and fraud cyber attacks.

Attackers do not need access credentials to perform these attacks!

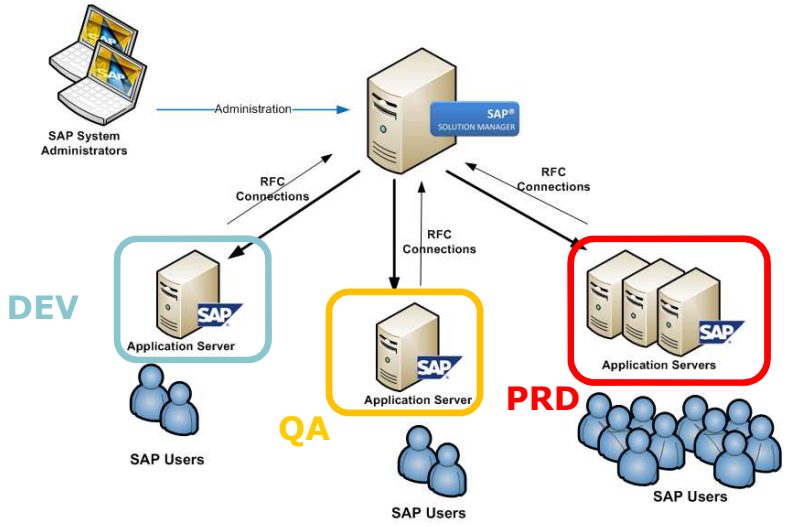
The SAP Solution Manager

What is the SAP Solution Manager?

- SAP component **required** in every SAP implementation.
- **Central** point for the administration of SAP systems.
- Typically, it is connected to several customer's SAP systems
- Does not hold any business data, but technical **information** about customer's SAP systems.
- Administrators connect to it to manage users, incidents, download and apply patches, among other activities.

If an attacker breaks into the SolMan, all the connected systems can be ultimately compromised!

SAP SolMan Infrastructure



The Initial Compromise

If not *compliant* with BIZEC TEC/11, an anonymous attacker could easily compromise a satellite SAP system.

- **BIZEC TEC-01: Vulnerable Software in Use**
- **BIZEC TEC-02: Standard Users with Default Passwords**
- **BIZEC TEC-03: Unsecured SAP Gateway**
- **BIZEC TEC-04: Unsecured SAP/Oracle authentication**
- **BIZEC TEC-05: Insecure RFC interfaces**
- **BIZEC TEC-06: Insufficient Security Audit Logging**
- **BIZEC TEC-07: Unsecured SAP Message Server**
- **BIZEC TEC-08: Dangerous SAP Web Applications**
- **BIZEC TEC-09: Unprotected Access to Administration Services**
- **BIZEC TEC-10: Insecure Network Environment**
- **BIZEC TEC-11: Unencrypted Communications**

The Initial Compromise

If not *compliant* with BIZEC TEC/11, an anonymous attacker could easily compromise a satellite SAP system.

- **BIZEC TEC-01: Vulnerable Software in Use**
- **BIZEC TEC-02: Standard Users with Default Passwords**
- **BIZEC TEC-03: Unsecured SAP Gateway**
- **BIZEC TEC-04: Unsecured SAP/Oracle authentication**
- **BIZEC TEC-05: Insecure RFC interfaces**
- **BIZEC TEC-06: Insufficient Security Audit Logging**
- **BIZEC TEC-07: Unsecured SAP Message Server**
- **BIZEC TEC-08: Dangerous SAP Web Applications**
- **BIZEC TEC-09: Unprotected Access to Administration Services**
- **BIZEC TEC-10: Insecure Network Environment**
- **BIZEC TEC-11: Unencrypted Communications**

SAP SolMan RFC Connections

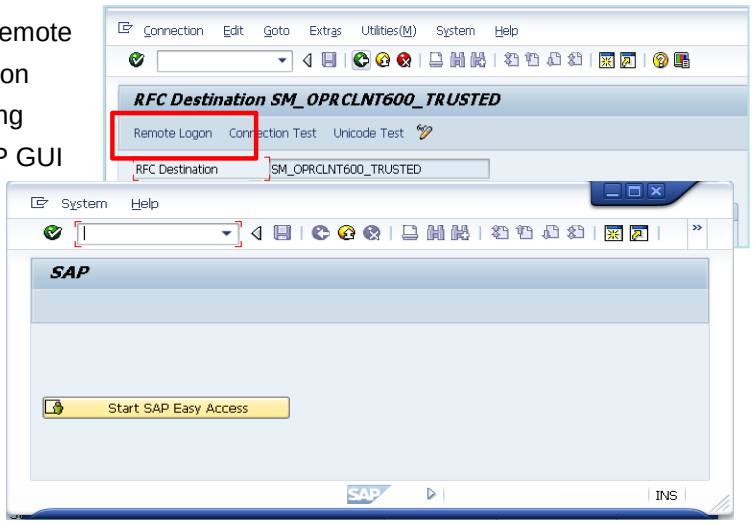
- RFC connections **to and from** the Solution Manager created by default

RFC Destination
SM_<SID>CLNT<Client>_LOGIN
SM_<SID>CLNT<Client>_READ
SM_<SID>CLNT<Client>_TRUSTED
SM_<SID>CLNT<Client>_TMW
SM_<SID>CLNT<Client>_BACK

- TRUSTED connections imply a trust relationship (a user with S_RFCACL authorization is required)
- BACK connections imply access from satellite systems to Solution Manager.
- Connections with stored password can be used to do remote logons or remotely execute RFC-enabled function modules.

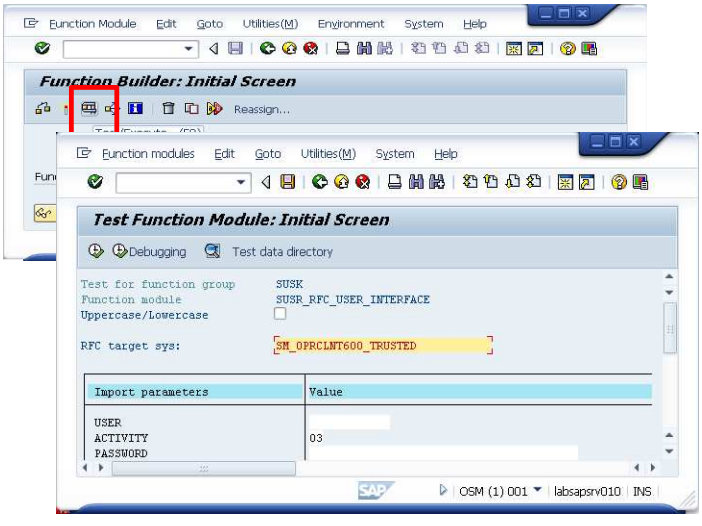
Abuse of default RFC connections

- Remote Logon Using SAP GUI



Abuse of default RFC connections

- Remote Execution of RFC Function Modules



SAP SolMan and Gateway attacks

- SAP Solution Manager is highly dependent on the Gateway: several external servers are registered by default.

- If the attacker knows/can guess the TPNAME, and the Gateway is not protected (by default), then all the well-known **Gateway attacks** can be triggered:
  - RFC callback attacks.
  - Cancellation of required external servers (DoS).
  - Man-in-the-middle attacks through RFC. No sensitive business data, but technical information, useful for other attacks, can be intercepted (and modified).

SAP SolMan and Gateway attacks

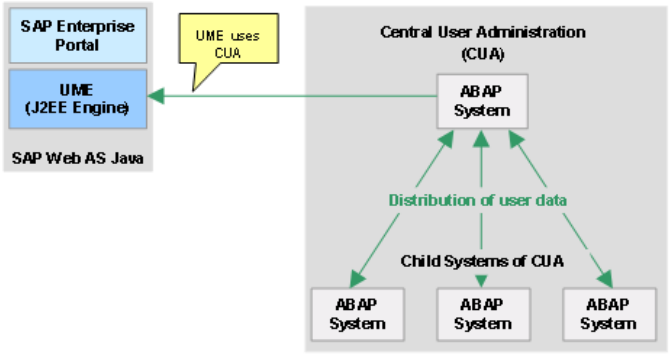
Protection / Countermeasure

- Restrict the assignment of user authorizations to logon from trusted systems (S_RFCACL and S_RFC).
- Use authorization object S_ICF on calling systems, controlling who can use which RFC destination.
- Restrict who can access RFC destinations by transaction (SM59), by table (RFCDES) and by authorization object (S_RFC_ADM).
- Restrict authorization object S_DEVELOP with activity 16 (execute) to control who can test function modules using SE37.
- *Check the "References" slide for more information!*

SAP Central User Administration (CUA)

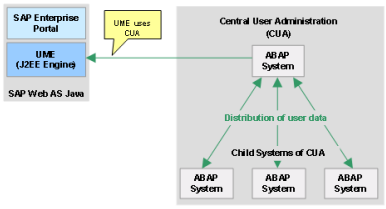
Central User Administration (CUA)

CUA enables the administration of users from a central SAP system (usually the SolMan).



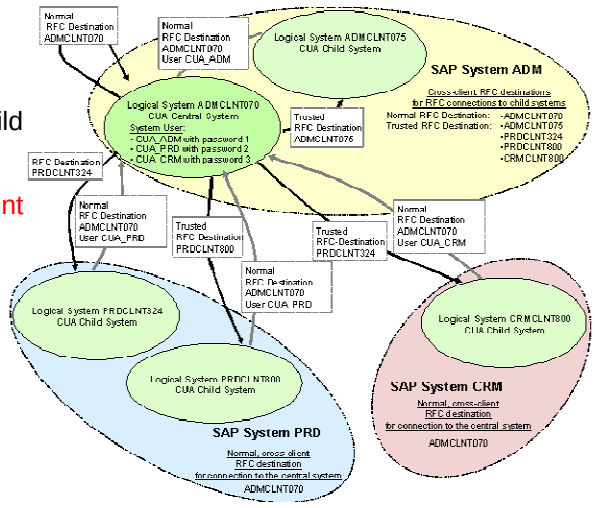
Central User Administration (CUA)

- The CUA Parent system needs to be allowed to create and administrate users on every Child system.
- It allows SAP administrators to easily manage users of ALL the SAP systems from a single point.
- Useful for ABAP and J2EE systems integration.



Central User Administration (CUA)

- RFC Connections are created:
  - From Parent to Child system (Trusted)
  - From Child to Parent system (Normal)



http://help.sap.com/saphelp_nw73/helpdata/en/a9/1a1ba3db9343beb2723452255003c5/content.htm

Attacks on Central User Administration

- **If the CUA Parent (usually the SolMan) is compromised, arbitrary users with any profiles can be created in all satellite systems.**

- *Note: Common RFC function modules used to create users do not work neither on child or parent systems when CUA is enabled → Other set of functions need to be used (**the ones used by CUA itself**).*

Attacks on Central User Administration

- If the CUA Parent (usually the SolMan) is compromised, arbitrary users with any profiles can be created in all satellite systems.

- *Note: Con... not work neither... Other set of functi...*

Protection / Countermeasure

- Restrict the usage of CUA RFC destinations for user administrators only, by using authorization object S_ICF on the CUA master.
- Use a special client within the SolMan to run the CUA master.

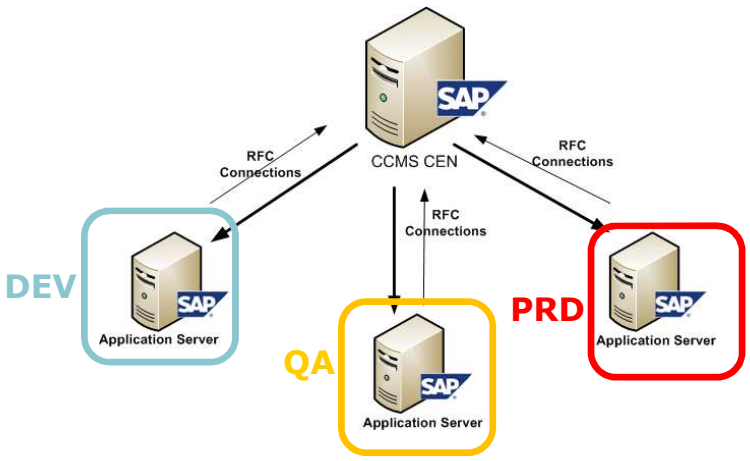
SAP Computing Center Management System (CCMS)

SAP CCMS

- Monitoring infrastructure provided by SAP to monitor SAP Application Servers. It can be configured centrally, using a central server (CEN) defined to receive all alerts.

- An **AGENT** is required to be executed on each monitored server. The agent :
  - Is implemented as an RFC server, which exposes several functions.
  - Registers itself as an **EXTERNAL SERVER** in the CEN, with a specific TPNAME (following a well-known pattern).
  - Is running as **<SID>adm** → Any abuse or exploitation would imply a full compromise of the SAP system information.

SAP CCMS Infrastructure



In many cases the Solution Manager is used as the CCMS Central Server (CEN), receiving information from all managed systems.

SAP CCMS RFC Connections

- RFC Connections from the CEN are created by default

RFC Destination
<SID>_RZ20_COLLECT
<SID>_RZ20_ANALYZE

  - The *COLLECT* destination has stored logon data and can be used to remotely execute function modules in the monitored systems.
  - The *ANALYZE* destination is typically used with a highly-privileged user, but has no stored logon information.

- Additionally, the agent connects back to the CEN using the CMSREG user, whose credentials are stored in a local file in the agent system (*/usr/sap/SID/INSTANCE/log/sapccm4x/passwd*).

Attacks on the SAP CCMS Agent

- One of the functions exposed by the CCMS agent can be used to execute OS commands remotely without authentication.

- As the agent is executed with SIDadm privileges → An attacker could get full compromise of the monitored SAP System going through the CEN's gateway.

Attacks on the SAP CCMS Agent

- One of the functions exposed by the CCMS agent can be used to execute OS commands remotely without authentication.

Protection / Countermeasure

- Secure the SAP Gateway, only allowing connections from authorized systems to the CCMS agents working as registered servers.

SAP Solution Manager Diagnostics (SMD)

SAP SMD

- *"**Solution Manager Diagnostics** provides all functionality to centrally analyze and monitor a complete NetWeaver system landscape".*

- An **AGENT** is required to be executed on each monitored server. The agent :
  - Is developed in JAVA and installed as a new SAP system (typically using a high system number like 97 or 98).
  - Exposes an **anonymous** P4 interface with a reduced set of methods.
  - Connects back to the Solution Manager, using a highly-privileged user account.

Abuse of SMD stored credentials

- **If a monitored system is compromised, the credentials of the user used for the connection can be decrypted *(kudos to Jordan Santarsieri @Onapsis).***

- Using these credentials, an attacker can connect back to the Solution Manager with high privileges.

- Once logged to the Solution Manager, the compromise can be extended by using default RFC connections to all managed/satellite systems.

Abuse of SMD stored credentials

- If a monitored system is compromised, the credentials of the user used for the connection can be decrypted *(kudos to Jordan Santarsieri @Onapsis).*

- Using these credentials, an attacker can connect back to the Solution Manager with high privileges.

- Once logged to the Solution Manager, the compromise can be extended by using default RFC connections to all managed/satellite systems.

Protection / Countermeasure

- Avoid the initial compromise of SAP system running the SDM agent.
- Restrict access to the secure storage file at the file-system level.

Abuse of SMD P4 interface

- Once the SMD agent is installed, the P4 interface is exposed on TCP service 5XX04 (instance num. XX).
- The P4 interface configured in the SMD agent is exposing a method that allows the installation of an application in the SMD agent, leading to remote OS command execution.
- Commands are executed as the <SID>adm user (daaadm, smdadm…)
- This leads to a full compromise of any SAP system configured on the Application Server.

Abuse of SMD P4 interface

- Once the SMD agent is installed, the P4 interface is exposed on TCP service 5XX04 (instance num. XX).
- The P4 interface configured in the SMD agent is exposing a method that allows t ding to remote OS
- Comman adm…)
- This lead on the Application Server.

Protection / Countermeasure

- Follow SAP recommendations and restrict access to P4 interface in SAP systems, as potentially insecure services might be exposed.

Conclusions

Conclusions

● **If an attacker breaks into the SAP Solution Manager, the game is over**: he would be able to compromise all managed satellite systems.

● **Trust relationships** are necessary in most SAP implementations. Extra caution:
- ● Which users can log-in using this feature (**S_RFCACL**).
- ● Which **authorizations** are being granted to these users.

● RFC connections are necessary in all SAP implementations. **Whenever possible:**
- ● Use **encryption** (SNC). It should be mandatory for business related communications.
- ● Avoid using connections with stored credentials.
- ● Avoid using connections from systems with lower security classification to systems with higher security classification (DEV → PRD!)

● **Monitor the creation/management of RFC connections**, as one single connection from DEV → PRD could result in a full system compromise if

Conclusions

- If possible, use **different Solution Manager/CEN systems** for Production environments.
- Secure the Solution Manager as **ANY** other Productive System

- Secure all satellite systems managed by an SAP Solution Manager:
  - Segregation of Duties (SoD) is really necessary, but not enough.
  - Implement a secure technical configuration of satellite systems.
  - Perform continuous/automated security monitoring.

- Do not expose the Solution Manager to the Internet!

- Restrict network access to the SAP Systems. Use firewalls/network filters to restrict potentially insecure interfaces.

- Update the systems, use the latest versions of all SAP solutions and apply all relevant SAP Security Notes.

References

1. Additional Information about Gateway and RFC security - Secure Configuration SAP NetWeaver Application Server ABAP" https://websmp109.sap-ag.de/~sapdownload/011000358700000968282010E/SAP-Sec-Rec.pdf
2. Best Practice - How to analyze and secure RFC connections http://wiki.sdn.sap.com/wiki/display/Security/Best+Practice+-+How+to+analyze+and+secure+RFC+connections
3. RFC/ICF Security Guide http://help.sap.com/saphelp_nw73ehp1/helpdata/en/48/92486caa6b17cee10000000a421937/frameset.htm
4. Security Settings in the SAP Gateway http://help.sap.com/saphelp_nw73ehp1/helpdata/en/48/b2096e7895307be10000000a42189b/frameset.htm
5. Securing RFC Connections http://scn.sap.com/docs/DOC-17089
6. Security Guide for Connectivity with the AS Java http://help.sap.com/saphelp_nw73ehp1/helpdata/en/b3/17d13fa69a4921e10000000a1550b0/frameset.htm
7. SolMan Security Guide: http://service.sap.com/~form/sapnet?_SHORTKEY=01100035870000735220&_OBJECT=011000358700000482312011E
8. Onapsis X1 http://www.onapsis.com/x1

Questions?

jppereze@onapsis.com

Follow us! ***@onapsis***
@jp_pereze

Thank you!