onapsis
Securing Business Essentials

Transporting evil code into the Business

Attacks on SAP TMS

Juan Perez-Etchegoyen
jppereze@onapsis.com

May 16th, 2013

NoSuchCon, Paris

NSC #1

Disclaimer

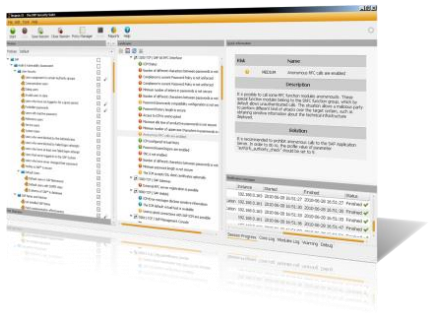
This publication contains references to the products of SAP AG. SAP, R/3, xApps, xApp, SAP NetWeaver, Duet, PartnerEdge, ByDesign, SAP Business ByDesign, and other SAP products and services mentioned herein are trademarks or registered trademarks of SAP AG in Germany and in several other countries all 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.

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

Agenda

- Introduction
- SAP TMS
- TMS Users and Connections
- Common Transport Directory
- Transport Files
- TP tool
- SAP TMS & Forensics
- 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!

Transport Management System

System ER6 System ER6
Transp. Domain DOMAIN_ER6 Transport domain ER6

SAP TMS

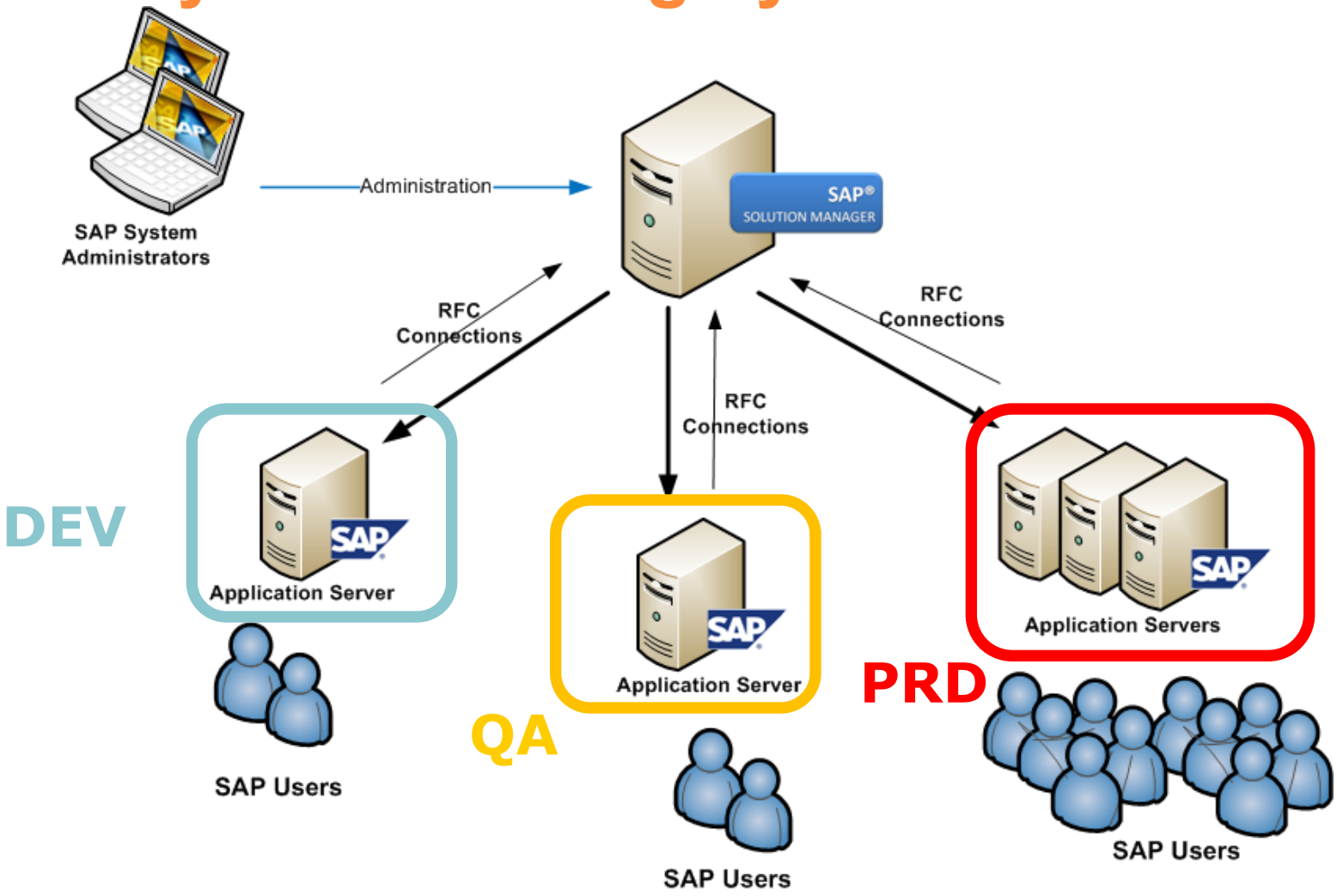
You are logged onto the domain controller

What is the SAP TMS?

- Set of tools, protocols and mechanisms aimed to manage and control **software customization** and **data changes** on SAP systems.
- Available for ABAP-based systems and also for non-ABAP (using CTS+)
- Configurable, as several “environments” can be included in the same domain (Training, Dev, QA, Prd) with their proper control procedures (ie QA Approval Procedure)

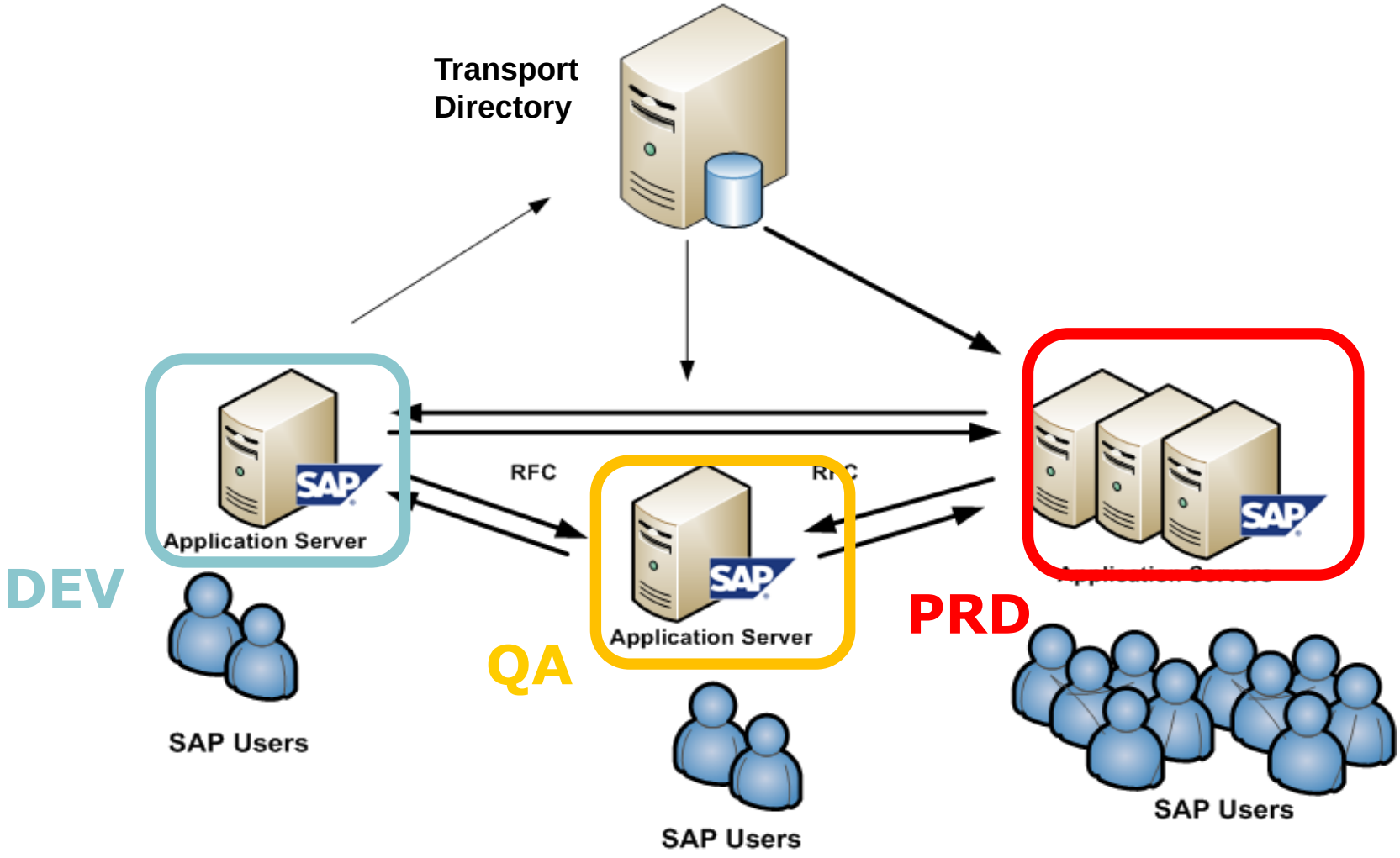
The final goal is to manage/control changes on the database

SAP Systems are highly connected…



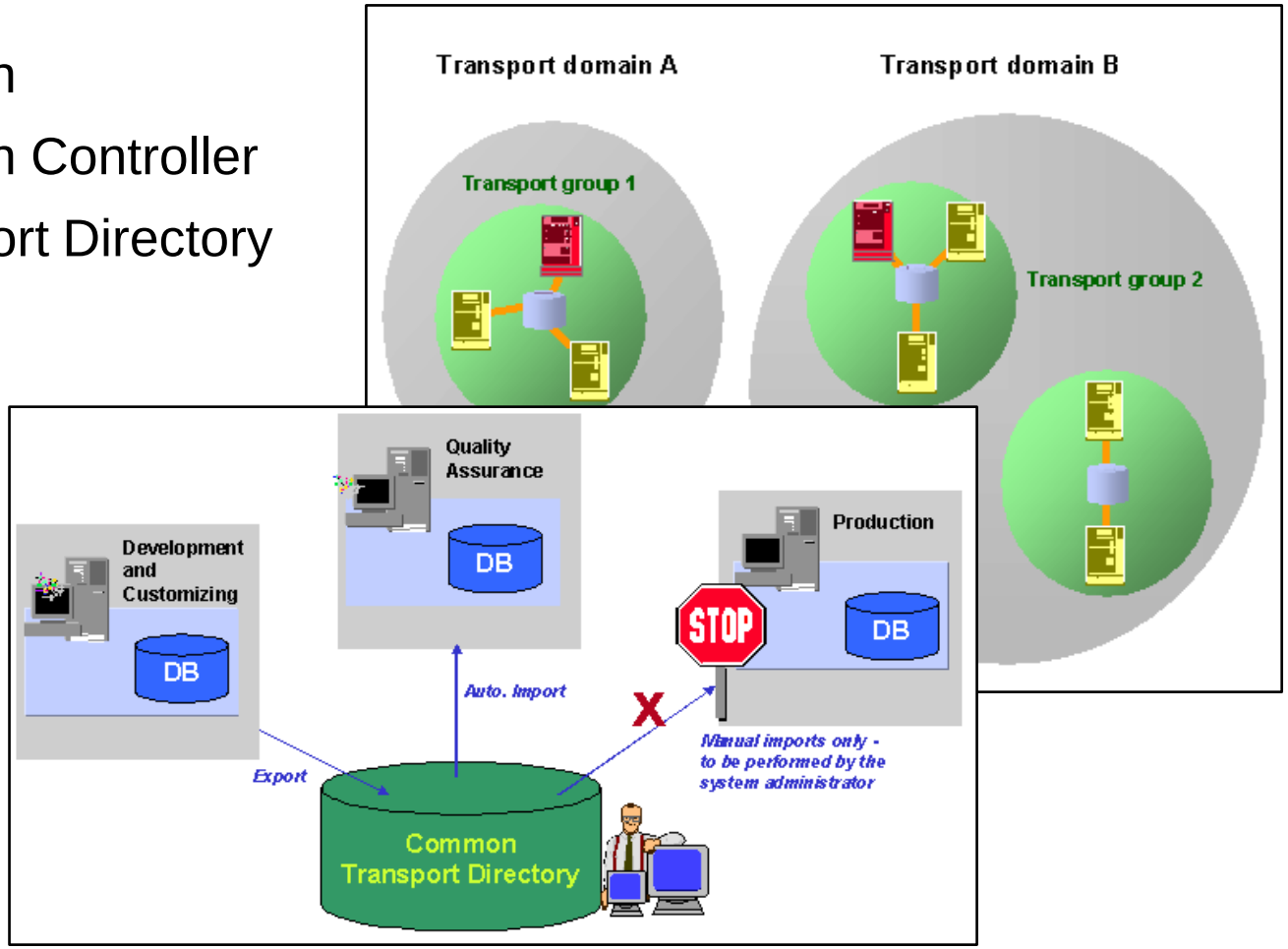
Attacks on SAP Solution Manager – 2012 Onapsis, Inc
http://www.onapsis.com/slides/ONAPSIS-HITB-Amsterdam-2012_Attacks_on_SAP_Solution_Manager.pdf.

SAP TMS Infrastructure



SAP TMS "concepts"

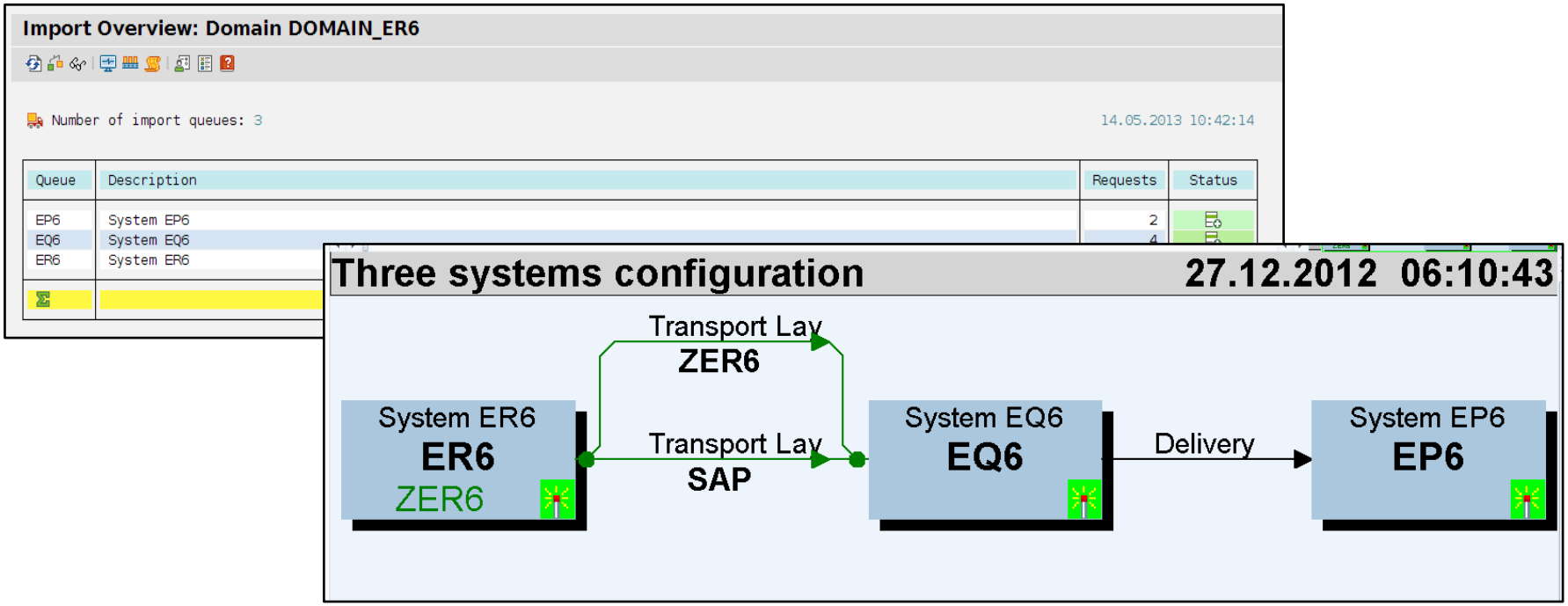
- Transport Domain
- Transport Domain Controller
- Common Transport Directory
- Transport Group
- SAP System
- SAP System role

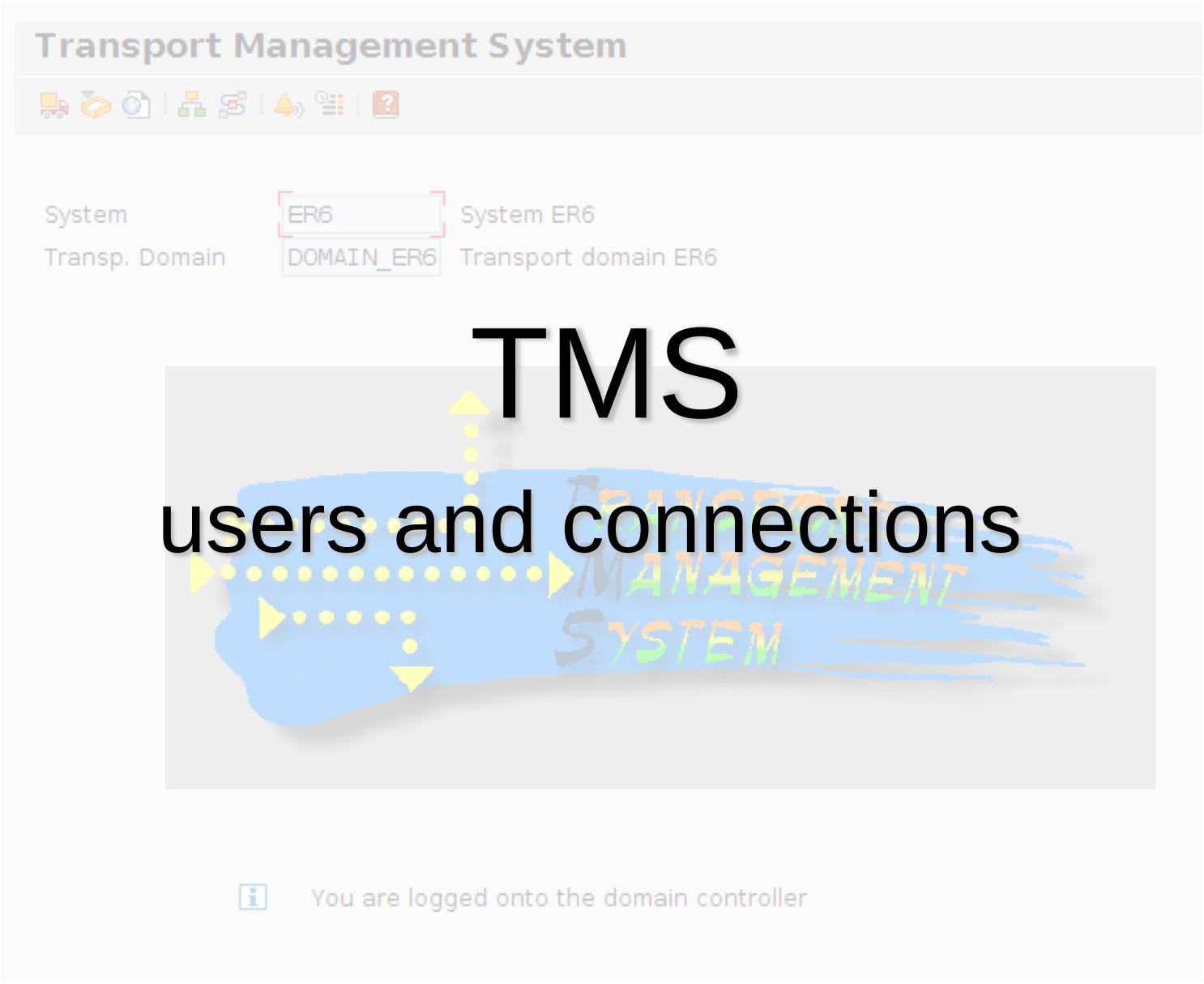


Transport Management System - http://help.sap.com/static/saphelp_nw70ehp1/en/c4/6045377b52253de10000009b38f889/Image1.gif
The SAP System Landscape - http://help.sap.com/saphelp_nw04s/helpdata/en/de/6b0d84f34d11d3a6510000e835363f/content.htm

SAP TMS “concepts” (cont.)

- Transport Routes
- Transport RFC Destinations
- TMS standard users
- TMS System queues





TMS

users and connections

SAP TMS RFC Connections

- After configuration, RFC connections are created connecting all the systems in the same transport domain (**full-mesh**).

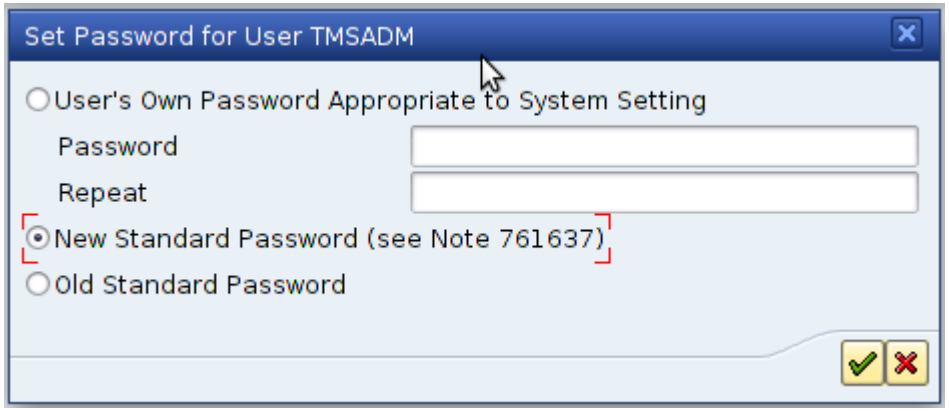
If the Transport Domain is configured with 3 systems, each system will have 6 “TMS” RFC Destinations.

RFC Destination
TMSADM@DOMAIN.SYSTEM
TMSSUP@DOMAIN.SYSTEM
CALLTP_<OS>

- TMSSUP connection does not represent any potential risk as user credentials are required in order to use it.
- TMSADM (configured with the S_A.TMSADM profile) connections are configured with stored TMSADM credentials meaning that anyone (with the proper authorizations) can use it to execute remote-enabled function modules.

TMSADM authentication

The standard user TMSADM (**system** type) is by default configured with a "shared" password for all the Transport Domain. This password is set on the installation. Initially it was arbitrarily configured to "PASSWORD", but now the user has more options.



- It is still very common to see TMSADM configured with password **PASSWORD**
- The new standard password is still a **fixed** password "$1Pawd2&"
- Choosing a non-standard password is the best option.

TMSADM authorizations

The standard user TMSADM is configured with a unique and standard profile S_A.TMSADM. This profile contains several authorization objects, many of them configured with '*' on the value.

Authorization objects
S_DEVELOP
S_DATASET, S_PATH
S_RFC, S_RFC_ADM
S_CTS_ADMI, S_TRANSPRT

- S_A.TMSADM is the minimum required set of authorization objects. Use this standard profile.
- No additional authorizations should be required.

Live Demonstration

TMSADM authorizations

The standard user TMSADM is configured with a unique and standard profile S_A.SYSTEM. This profile contains several authorization objects, ma

Protection / Countermeasure

- Use a strong and non-standard password for the user TMSADM
- Do not assign authorizations other than profile S_A.TMSADM, specially not SAP_ALL (we have seen this many times).
- Apply all SAP Security Notes. Keep the systems up-to-date.
- Implement SAP Security Notes 761637, 1414256, 1515926, 1657891, 1554030, 1488406, 1486759, 1445407, 1298160 and 1298160.
- *Check the "References" slide for more information!*

- S Use this standard profile.
- No additional authorizations should be required.

Common Transport Directory

CTD Security configuration

It's a **network location** shared by all systems in the same transport group. This directory will hold the TR (transport requests). This directory is implemented as **SMB or NFS** exported shares.

When implemented as NFS (most common) some configuration issues could arise:

- Exported to any IP address.
- Exported with insecure permissions (r/w, suid).
- Exported along with configuration and binary files.
- Implemented on the least secure system (usually DEV)

Where should I place the CTD

- **PRD** systems usually fall under the scope of internal/external audits → they are more “secure”.
- **DEV systems are not considered security-sensitive**.
  - Access controls and security settings are relaxed → high chances of exploiting SAP application-layer vulnerabilities.
  - No Security Auditing features enabled → low chances of being detected.
- **DEV,QA systems usually have explicit and implicit relationships with PRD systems (shared passwords, RFC connections)** → they are the perfect “pivot”.

Live Demonstration

Where should I place the CTD

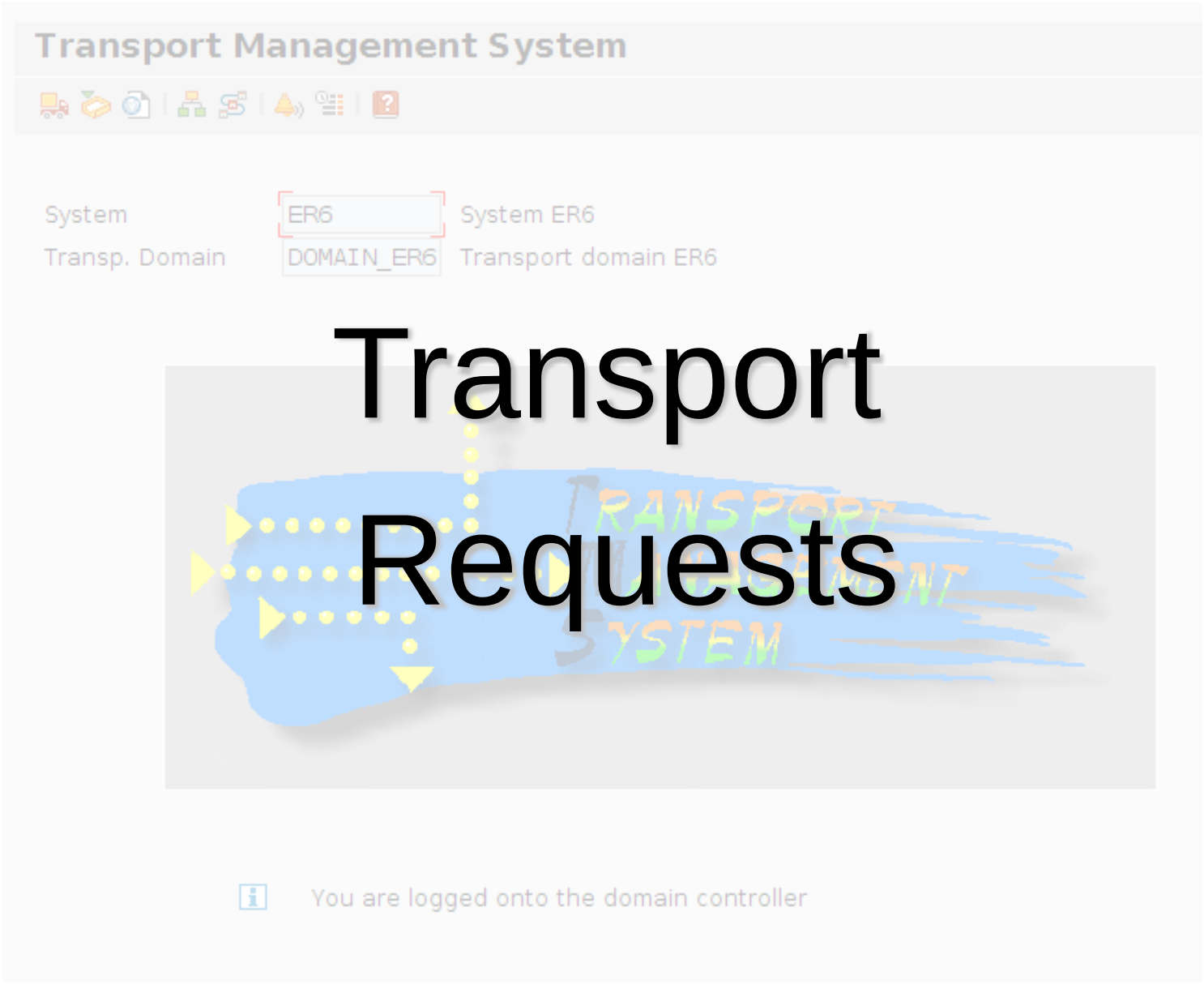
- **PRD** systems usually fall under the scope of internal/external audits → they are more "secure".
- **D**
- **D**

re

connections) → they are the perfect "pivot".

Protection / Countermeasure

- Configure the Common Transport Directory in a secure way.
- Restrict access to only the Application Servers of the SAP Systems on the same transport group.
- Use a secure system to hold the Common Transport Directory.
- Implement SAP Security Notes 1330776 and 633814.
- Secure every SAP system as the productive systems.
- *Check the "References" slide for more information!*



Transport Requests

TMS Transport requests

The transport request is the unit of data that is moved between SAP systems. All transport requests are stored in the CTD in two files, the "data" file and the "cofile" file. The default location is:

Default Location	
/usr/sap/trans/data/RXXXXXX.SYS	R900050.DEV
/usr/sap/trans/cofiles/KXXXXXX.SYS	K900050.DEV

The cofile keeps an "activity log" of the Transport Request.

```
ZONAPSIS  K EQ6    3 1 2 0 0 0 0 0 0 3  731   .  0   0   0   0   0 000
#□A
#/1/      A   G   D   -   R   C   T   -   Z RELE EX.  _   _   _   _   _ CLI
ER6 f 0000 20130511133715 labsapsrv030       er6adm
ER6 e 0000 20130511133717 labsapsrv030       er6adm
EQ6 < 0000 20130511133723 labsapsrv030       er6adm
ER6 E 0000 20130511133723 labsapsrv030       er6adm
EQ6 H 0004 20130511133819 labsapsrv019       eq6adm
EQ6 A 0004 20130511134836 labsapsrv019       eq6adm
```

Data File

An example Transport request analyzed. The header is an ascii-based portion while the rest is binary.

```
00000000  00 00 00 33 20 54 30 30  30 35 30 32 30 36 32 33  |...3 T0005020623|
00000010  32 30 31 33 30 35 31 31  31 36 33 37 32 33 65 72  |20130511163723er|
00000020  36 61 64 6d 20 20 20 20  20 20 37 33 31 20 00 00  |6adm      731 ..|
00000030  10 01 4c 00 00 06 d6 7c  9d 0c 23 00 40 00 00 12  |..L....|..#.@...|
00000040  1f 9d 02 bb 5c ab 5b 52  db 86 c2 ea 4d af 3a 9d  |....\.[R....M.:.|
00000050  b6 37 9d de e9 2a 49 99  65 23 ff ac 61 e9 a4 33  |.7...*I.e#..a..3|
00000060  06 cb e0 f5 0f c4 16 84  e5 66 87 ec d2 0d 33 89  |.........f....3.|
00000070  e9 2c 6c 9b f4 91 fa 00  7d 86 3e 53 af 7a 6c 7e  |.,l.....}.>S.zl~|
00000080  16 cb 18 0c d1 7a 5a f6  68 bc c1 46 9f f4 71 2c  |.....zZ.h..F..q,|
00000090  9d ef 48 0a 42 a8 84 4b  be 32 bb 1b 86 53 fc db  |..H.B..K.2...S..|
000000a0  e8 6e 3a 9e 84 35 ac 48  a7 12 39 95 64 5c c6 32  |.n:..5.H..9.d\.2|
000000b0  a9 49 72 8d 68 08 a1 77  b8 14 4c ee ef ae 47 38  |.Ir.h..w..L...G8|
000000c0  f8 34 9d 8d 3e e0 57 58  77 8d 97 56 38 1b bd c7  |.4..>.WXw..V8...|
000000d0  1f ab da 95 a6 e2 df c7  b3 77 d8 19 87 f7 1f f1  |.........w......|
000000e0  24 c4 46 dd 0d a2 5a 86  5e d7 03 6c e0 72 b9 0c  |$.F...Z.^..l.r..|
```

Date and time, user and version

Data File

After the header, there are blocks of compressed data of variable length.

```
00000000  00 00 00 33 20 54 30 30  30 35 30 32 30 36 32 33  |...3 T0005020623|
00000010  32 30 31 33 30 35 31 31  31 36 33 37 32 33 65 72  |20130511163723er|
00000020  36 61 64 6d 20 20 20 20  20 20 37 33 31 20 00 00  |6adm      731 ..|
00000030  10 01 4c 00 00 06 d6 7c  9d 0c 23 00 40 00 00 12  |..L....|..#.@...|
00000040  1f 9d 02 bb 5c ab 5b 52  db 86 c2 ea 4d af 3a 9d  |....\.[R....M.:.|
00000050  b6 37 9d de e9 2a 49 99  65 23 ff ac 61 e9 a4 33  |.7...*I.e#..a..3|
00000060  06 cb e0 f5 0f c4 16 84  e5 66 87 ec d2 0d 33 89  |.........f....3.|
00000070  e9 2c 6c 9b f4 91 fa 00  7d 86 3e 53 af 7a 6c 7e  |.,l.....}.>S.zl~|
00000080  16 cb 18 0c d1 7a 5a f6  68 bc c1 46 9f f4 71 2c  |.....zZ.h..F..q,|
00000090  9d ef 48 0a 42 a8 84 4b  be 32 bb 1b 86 53 fc db  |..H.B..K.2...S..|
000000a0  e8 6e 3a 9e 84 35 ac 48  a7 12 39 95 64 5c c6 32  |.n:..5.H..9.d\.2|
000000b0  a9 49 72 8d 68 08 a1 77  b8 14 4c ee ef ae 47 38  |.Ir.h..w..L...G8|
000000c0  f8 34 9d 8d 3e e0 57 58  77 8d 97 56 38 1b bd c7  |.4..>.WXw..V8...|
000000d0  1f ab da 95 a6 e2 df c7  b3 77 d8 19 87 f7 1f f1  |.........w......|
000000e0  24 c4 46 dd 0d a2 5a 86  5e d7 03 6c e0 72 b9 0c  |$.F...Z.^..l.r..|
```

00 00 06 d6 7c 9d 0c 23 00 40 00 00 12 1f 9d 02

Data File

- Similar compression algorithms are used on other SAP components.
- Once decompressed, the protocol is purely text, separated by blocks.

The contents can be retrieved and modified (need re-calculation of the CRC32 checksums).

```
00 00 00 2a 20 2a 52 33 74 72 61 6e 73 20 76 65 ......R3trans.ve
72 73 69 6f 6e 3a 20 33 31 2e 31 30 2e 31 32 20 rsion..31.10.12.
2d 20 32 30 3a 31 32 3a 30 36 00 00 00 68 20 2a ..20.12.06...h..
53 6f 75 72 63 65 20 53 79 73 74 65 6d 20 3d 20 Source.System...
41 4d 44 2f 49 6e 74 65 6c 20 78 38 36 5f 36 34 AMD.Intel.x86.64
20 77 69 74 68 20 4c 69 6e 75 78 20 6f 6e 20 44 .with.Linux.on.D
42 4d 53 20 3d 20 41 44 41 42 41 53 20 44 20 2d BMS...ADABAS.D..
2d 2d 20 44 42 4e 41 4d 45 20 3d 20 27 27 20 2d ...DBNAME.......
2d 2d 20 53 59 53 54 45 4d 20 3d 20 27 45 52 36 ...SYSTEM....ER6
27 2e 00 00 00 41 20 2a 6c 61 6e 67 75 61 67 65 .....A..language
73 3a 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d 4e s.ABCDEFGHIJKLMN
4f 50 51 52 53 54 55 56 57 58 59 5a 30 31 32 33 OPQRSTUVWXYZ0123
34 35 36 37 38 39 61 62 63 64 69 28 29 2c 2e 2f 456789abcdi.....
3a 3b 26 00 00 00 7a 20 2a 69 73 6f 2d 6c 61 6e ......z..iso.lan
67 75 61 67 65 73 3a 49 53 4f 2d 41 52 48 45 43 guages.ISO.ARHEC
53 44 45 45 4e 46 52 45 4c 48 55 49 54 4a 41 44 SDEENFRELHUITJAD
41 50 4c 5a 46 4e 4c 4e 4f 50 54 53 4b 52 55 45 APLZFNLNOPTSKRUE
.....
```

Dissecting Transport Requests

- **The transport requests can be parsed and opened using compression algorithms.**

- If unauthorized access to the data files is achieved, then all the information hosted on those files can be **accessed and modified**.

- Furthermore, evil transports can be specifically generated and later transported into the target systems containing:
  - New users.
  - Backdoor functionality
  - Any piece of information on any table.

Live Demonstration

Dissecting Transport Requests

- **The transport requests can be parsed and opened using compression algorithms.**

- If
info

- F
transported into the target systems containing:
  - New users.
  - Backdoor functionality
  - Any piece of information on any table.

Protection / Countermeasure

- Analyze all transport requests before being imported into PRD systems.
- Secure ALL the TMS infrastructure including Users, RFC communications and CTD location.
- *Check the "References" slide for more information!*

Transport Management System

System ER6 System ER6
Transp. Domain DOMAIN_ER6 Transport domain ER6

TP tool

You are logged onto the domain controller

TMS TP tool

The main OS tool used by the TMS is called “TP”. This binary can be used by command line and can be called remotely through the gateway (External “STARTED” Server).

If the SAP Gateway ACL’s are not secured (it is secure by default only in the latest Netweaver versions) → **Any transport could be uploaded and imported remotely into production without restrictions**.

Check Bjoern Brencher’s presentation: “SAP runs SAP: RFC Gateway Hacking and Defense” covering attacks and mitigation of SAP gateway **(References - #2)**

Live Demonstration

TMS TP tool

The main tool related to the TMS is the “TP”. This binary was developed to be used by command line and it can also be called remotely through the gat

If th
late
→A
production without restrictions.

(Test can be triggered using SE37 and RFC FM TRINT_TP_INTERFACE)

Check Bjoern Brencher’s presentation: “SAP runs SAP: RFC Gateway Hacking and Defense” covering attacks and mitigation of SAP gateway

Protection / Countermeasure

- Secure the SAP Gateway, only allowing authorized systems to start external servers, specifically the TP server.
- Implement SAP Security Note 1371799 to restrict execution of TP through the SAP Gateway.
- *Check the “References” slide for more information!*

TMS & Forensics

Tracing TMS activity

- If **table change logging** is enabled, all changes to tables performed through the transport system (recclient) can be saved. All changes are saved into table DBTABLOG.
- All transport requests information is saved in specific **TR tables** that are populated during the import of each TR.
- During the execution of the transport (including commands tp and R3Trans, among others), all **logs** are generated and stored in a specific location.
- If the **Gateway Log** is enabled, this log can show information regarding RFC connections and remote execution of the tp command.

ABAP – Table Change Logging: Summary

Description	Value
Enabled by default	No
Physical location of the log file(s)	Table DBTABLOG
Limit of the log file	No limit
Action performed after reaching log limit	N/A
Centralized logging capabilities	Not possible
How to access log(s) contents	Transaction SCU3

ABAP – Imported TR Tables: Summary

Description	Value
Enabled by default	Yes
Physical location of the log file(s)	Tables E070, E071, E071K…
Limit of the log file	No limit
Action performed after reaching log limit	N/A
Centralized logging capabilities	Not possible
How to access log(s) contents	Transaction SE01

ABAP – Transport Logs: Summary

Description	Value
Enabled by default	Yes
Physical location of the log file(s)	/usr/sap/trans/log
Limit of the log file	No limit
Action performed after reaching log limit	N/A
Centralized logging capabilities	Not possible
How to access log(s) contents	Access the files at the OS level or using transaction SE01

Gateway Logs: Summary

Description	Value
Enabled by default	No
Physical location of the log file(s)	/usr/sap/**<SID>**/**<INSTANCE>**/work/<file_name> **<file_name>** is defined by key **LOGFILE**
Limit of the log file	Specified by **MAXSIZEKB** (kb)
Action performed after reaching log limit	Defined by **FILEWRAP** and **SWITCHTF**
Centralized logging capabilities	No
How to access log(s) contents	Transaction SMGW

Conclusions

Conclusions

- If the SAP Transport Management System is not protected, an attacker can create/modify malicious transports bypassing the Change Control/Management mechanisms.

- These transports could have dramatic impact if deployed to Production (espionage, sabotage, fraud).

- Use non-standard credentials for the TMSADM user and do not assign extra authorizations.

- Place the Common Transport Directory in a secure location and properly configured.

- Secure all the systems as **ANY** other Productive System

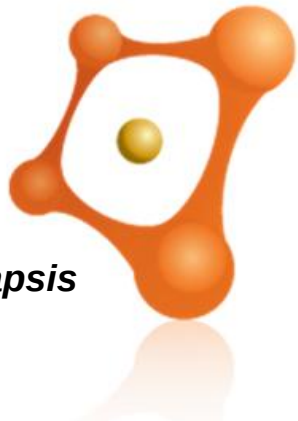
- Update the systems!!!. Use the latest versions of all SAP solutions and components. Apply all relevant SAP Security Notes.

References

1. CTS Security Guide
   http://help.sap.com/saphelp_nw70ehp3/helpdata/en/ec/b3b638faa32d19e10000009b38f8cf/content.htm
2. SAP runs SAP: RFC Gateway Hacking and Defense by Bjoern Brencher
   http://www.sapvirtualevents.com/teched/sessiondetails.aspx?sId=3399
3. 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
4. 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
5. Security Settings in the SAP Gateway
   http://help.sap.com/saphelp_nw73ehp1/helpdata/en/48/b2096e7895307be10000000a42189b/frameset.htm
6. Securing RFC Connections http://scn.sap.com/docs/DOC-17089
7. Onapsis X1 http://www.onapsis.com/x1

Questions?

jppereze@onapsis.com



Follow us! ***@onapsis***

Thank you!