The SAProuter

An Internet Window to your SAP Platform (and beyond)

Mariano Nuñez Di Croce
mnunez@onapsis.com

July 2, 2010

HITBSecConf, Amsterdam

Disclaimer

Onapsis offers no specific guarantee regarding the accuracy or completeness of the information presented, but the professional staff of Onapsis makes every reasonable effort to present the most reliable information available to it and to meet or exceed any applicable industry standards.

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?

- Specialized company focused in the **security of ERP and Business-critical Applications** (SAP®, Siebel®, Oracle® E-Business Suite™, JD Edwards® …).
- Core business areas:
  - Development of specialized security software solutions.
  - Security consultancy services.
  - Trainings on business-critical systems security.
- Founding member of BIZEC – The Business Security Community.

Who am I?

- **Director of Research and Development at Onapsis.**
- Degree in Computer System Engineering.
- Originally devoted to **Penetration Testing** and **Vulnerability Research**.
- Discovered **vulnerabilities** in Microsoft, Oracle, SAP, IBM, …
- Lead developer of **Bizploit**, the open-source ERP Penetration Testing framework.
- **Speaker/Trainer** at Black Hat, HITB, Sec-T, Hack.lu, DeepSec, Ekoparty..

Agenda

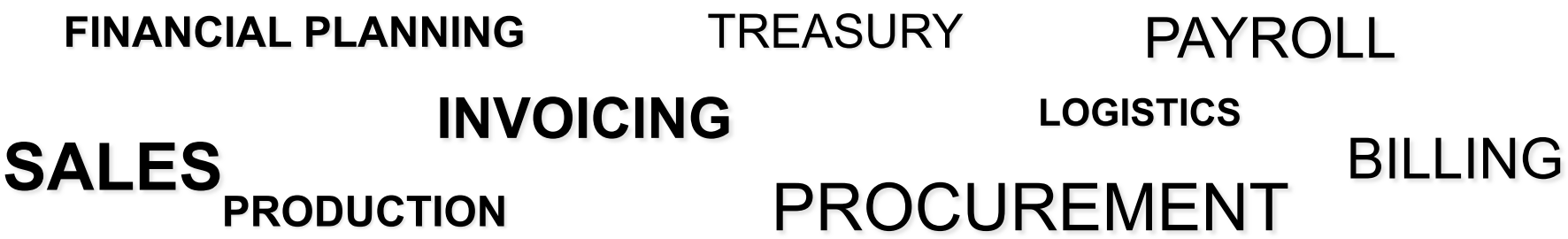
- Introduction
- The SAProuter
- SAProuter Security Assessment
  - Retrieving useful information
  - Discovering internal systems and services
  - Proxying Bizploit through misconfigured SAProuters
  - SAProuter “Agents”
- Securing the SAProuter
- Conclusions

Introduction

What is SAP?

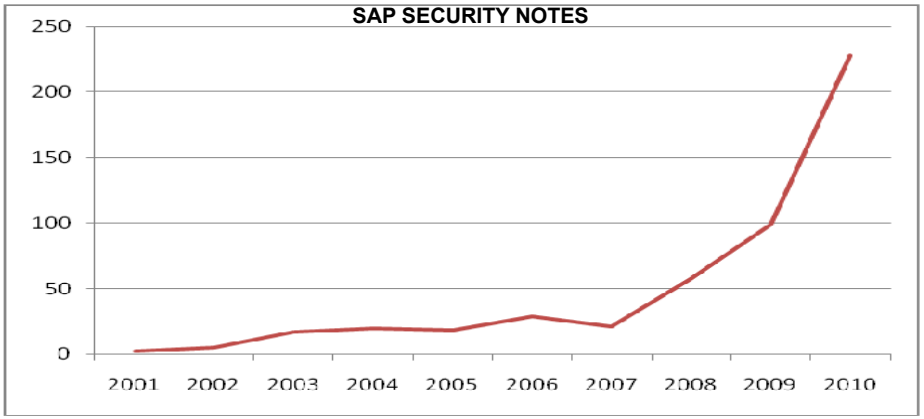
- **Largest** provider of **business management solutions** in the world.
  - More than 140.000 implementations around the globe.
  - More than 90.000 customers in 120 countries.

- Used by **Fortune-500 world-wide companies**, **governmental organizations** and **defense facilities** to **run their every-day business processes.**
  - Such as Revenue / Production / Expenditure business cycles.



Why are we talking about SAP security?

- SAP Vulnerabilities are in the rise.



- The biggest mis-conception: “SAP Security” is “security of roles & profiles”. The facts: **Segregation of Duties is not enough!**
  - Most standards & regulations still don’t get it.
  - Most Auditing companies still don’t get it.
  - Some customers still don’t get it.

SoD is not enough to “be secure”!

From the trenches:

During an assessment, a “SoD compliant” SAP system (which had cost $$$$^n to implement), could be remotely compromised in a matter of seconds through the exploitation of a vulnerability in a technological component.

Ok, but… which is the real risk?

CONFIDENTIALITY

AVAILABILITY

INTEGRITY

ESPIONAGE

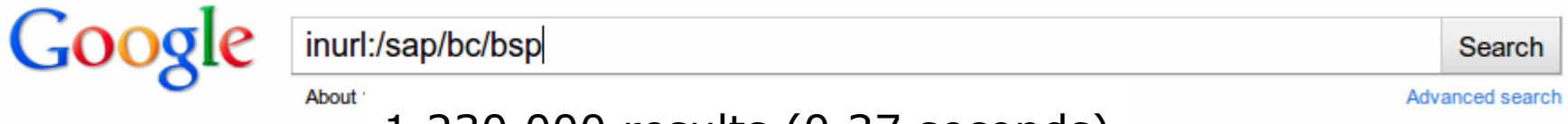
SABOTAGE

FRAUD

“SAP systems are not in the Internet”

34,200 results (0.44 seconds)

103,000 results (0.39 seconds)



1,230,000 results (0.37 seconds)

New talk coming soon…! ;-)

The SAProuter

SAProuter

SAProuter is an SAP program working as a reverse proxy, which **analyzes connections between SAP systems and between SAP systems and external networks.**

It is designed to analyze and **restrict SAP network traffic** which was **allowed to pass through the *firewall*.**

SAProuter does not replace the *firewall,*

it complements it

Typical Scenarios

You need to provide **remote access** to your SAP platform.

Why?

- Access from remote developers/consultants/administrators.
- Access from Business Partners.
- Access from SAP A.G.

You can avoid the first two, but **remote access from SAP is mandatory**:

SAP technicians **connect through your SAProuter to your SAP systems** for monitoring and troubleshooting support.

This means you likely have a SAProuter running right now!

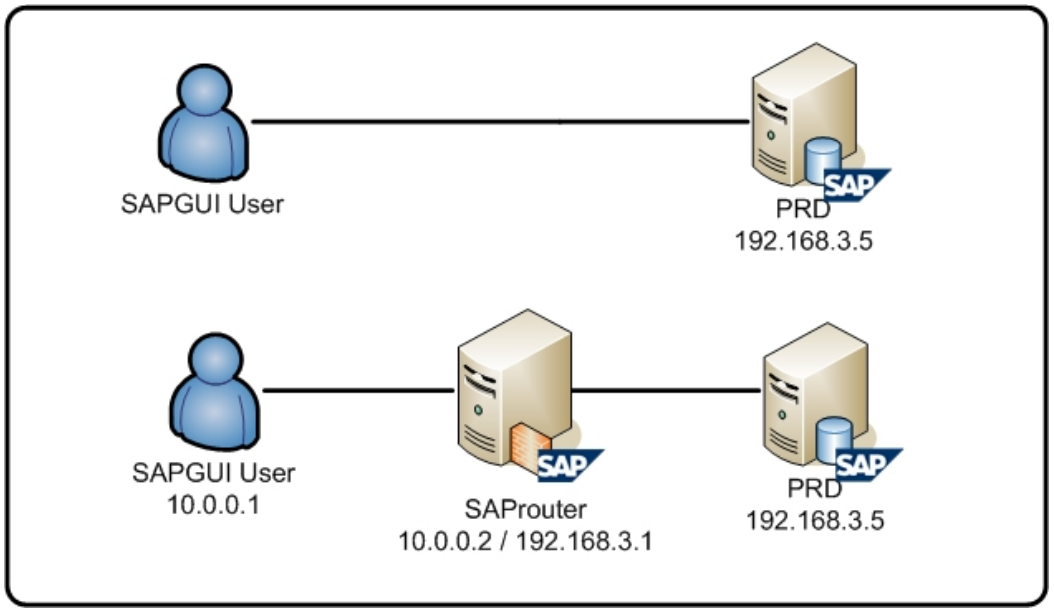
Why is the SAProuter useful?

The SAProuter can be used for:

- Filter requests based on IP addresses and/or protocol.
- Log connections to SAP systems.
- Enforce security, requiring the use of a secret password for the communication.
- Require communications using Secure Network Communications (SNC).

SAProuter *Route Strings*

Once SAProuter is in place, clients have to specify a *route string* to connect to target servers.



/H/10.0.0.2/S/3299/H/192.168.3.5/S/3200

Syntax: (/H/host/S/service/W/pass)*

- /H/ specifies the *hostname.*
- /S/ indicates the *service* or *port. (optional)*
- /W/ or /P/ are used for the connection password. (*optional)*

Restricting Access: The Route Permission Table

The Access Control List is specified in a special textfile called *the Route Permission Table.*

Entry format:

P/S/D <source-host> <dest-host> <dest-serv> <password>

- P - Permit this connection.
- S - Only allow connections using the SAP Protocol.
- D - Deny this connection.

Rule Evaluation:

- First-match criteria.
- If there is no match, deny the connection.

Route Permission Table Example

```
D       host1           host2           serviceX
P       192.168.1.*     host2           *               pwd123
S       10.1.*.*        10.1.2.*        *
D       *               *               *
```

Route Permission Table *Real-World* Example

```
...
P       192.168.3.1     sapserver01     3200    *
P       192.168.3.56    sapserver01     3200    *
P       192.168.3.14    sapserver01     3200    *
# 2009-31-12 by John S: I got tired of maintaining this file.
P       *               *               *       *
```

SAProuter Security Assessment

Onapsis Bizploit

- The first **ERP Penetration Testing Framework**.
- Developed by the Onapsis Research Labs.
- Open-source and free.
- Modules for **Discovery, Vulnerability Assessment** and **Exploitation.**
- Mainly comprising SAP modules at this moment.
- Modules for other popular ERPs coming soon!

- Using Bizploit, you can assess the security of remote SAProuters.

Retrieving Useful Information

- The SAProuter provides useful information through ***info-requests.***

```
C:\Documents and Settings\Administrator>saprouter -l

Thu Oct 25 13:11:23 2007
SAP Network Interface Router, Version 38.9

peer SAProuter with NI version 38 ...
send info-request to running SAProuter ...

SAP Network Interface Router running on port 3299 (PID = 3164)
Started on: Thu Oct 25 12:22:56 2007


ID  CLIENT                          ¦ PARTNER                                service
------------------------------------+-----------------------------------------
1   127.0.0.1                       ¦ (no partner)

Total no. of clients: 1
Working directory    : c:\SAP\NSP\sys\exe\run
Routtab              : c:\windows\system32\saprouttab
```

- For this to work, **connections to the SAProuter port must be permitted** (P * * * * will also work).
- Useful to **discover internal SAP servers and IP address scheme.**
- What about **attacking the SAP users**? *(Check Alexander Polyakov's great work on this area).*

Live demo

Discovering Internal Systems and Services

- The SAProuter is connected to the internal network.
- The systems it will be able to connect to, mainly depends on:
  - The entries of its Route Permission Table.
  - The deployed network filtering and segmentation on the internal side.

Using **Onapsis Bizploit's *saprouterSpy* module** it is possible to **perform a portscanning** of the Organization's internal systems, located "behind" the SAProuter.

Live demo

Proxying Bizploit Modules through SAProuters

- Some **Bizploit modules can be used through a vulnerable SAProuter**.
- Using discovery module ***saprouterSpy*** again, but setting *createTargets* to *True*.
- New targets will be created, which can be used just as regular Bizploit targets!

Live demo

Native Protocols

- What's the difference between "P" and "S"? According to the SAP Library:
  - **P**(ermit) causes SAProuter to set up the connection.
  - **S**(ecure) only allows connections **with the SAP Protocol**; connections with other protocols (such as TCP) are not allowed.

- Some "**strange**" Route Permission Tables in the Internet:

```
# SNC-connection from SAP to local R/3-System for pcANYWHERE, if it is needed
KP "p:CN=sapserv2, OU=SAProuter, O=SAP, C=DE" 196.123.150.233 5631
# SNC-connection from SAP to local R/3-System for NetMeeting, if it is needed
KP "p:CN=sapserv2, OU=SAProuter, O=SAP, C=DE" 196.123.150.233 1503
# SNC-connection from SAP to local R/3-System for saptelnet, if it is needed
KP "p:CN=sapserv2, OU=SAProuter, O=SAP, C=DE" 196.123.150.233 23
```

Native Protocols == OS/DB Access

- Designed to **allow SAP to access your OS and Databases**.
- **Access to non-SAP services is possible!**
- Increased out-of-the-box security: In modern versions of SAProuter, a "*" in the service field will not allow native access.
- **If vulnerable, it is possible to connect to ANY service on ANY system on the Organization's internal network (that the SAProuter can access).**

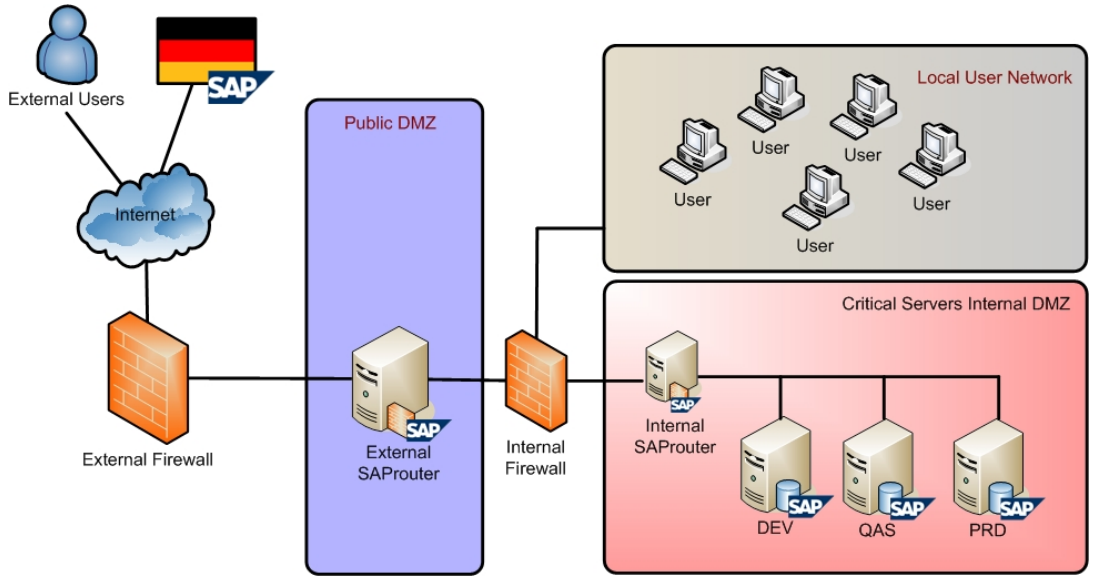
- Upcoming **Onapsis Bizploit** modules:
  - ***saprouterNative*** – Detect if native connections are possible.
  - ***saprouterAgent*** – "Deployment" of SAProuter agents.

Live demo

Securing the SAProuter

Security at the Network Level

- Configure a **VPN between your SAProuter and SAP servers**! The SAProuter port should not be visible to the Internet and the system should be placed in public DMZs.
- If no VPN:
  - The border Firewall should only allow access to the SAProuter port.
  - SNC should be enabled to encrypt the traffic.
- SAProuters should be used to restrict internal access as well.



Securing the Route Permission Table

- Simple approach: **Only allow what is strictly necessary (whitelist).**
- **Avoid using many wildcards (*).**
- Access to SAProuter host and port is only used for administration. This kind of access should be restricted to authorized entities.
- If SNC is in use, KT entries should be fully defined.
- If only allowing SAP connections, **don't use P, use S.**
- Always add a "D * * * *" as the bottom line.

Additional Protections

- **Protection against Denial of Service attacks**
  - By default, only 800 concurrent connections are supported. Once limit is reached, new connections will be rejected.
  - Solution:
    - Use the "*–Y 0"* option. A new SAProuter will be spawned on-demand.
    - Use the "*-C"* option, specifying a higher number of clients if required.

- **Avoid Error Information Disclosure**
  - Use the "*-Z"* option. Non-descriptive errors will be returned.

- Keep SAProuter **binaries updated** with latest SAP security patches.

Auditing & Intrusion Detection

- It's critical to start SAProuter with the "-G" flag, to **enable logging**.
- This will allow you to **detect malicious activity and intrusion attempts**.

Regular connection (accepted)

```
Mon May 31 14:30:45 2010 CONNECT FROM C1/- host 192.168.0.1/43556
Mon May 31 14:30:45 2010 CONNECT TO S1/2 host 192.168.0.105/3200 (192.168.0.105)
Mon May 31 14:30:58 2010 DISCONNECT S1/2 host 192.168.0.105/3200 (192.168.0.105)
```

Regular connection (rejected)

```
Mon May 31 14:32:25 2010 CONNECT FROM C1/- host 192.168.0.1/44654
Mon May 31 14:32:25 2010 PERM DENIED C1/- host 192.168.0.1 (192.168.0.1) to 192.168.0.105/3201
Mon May 31 14:32:25 2010 DISCONNECT C1/- host 192.168.0.1/44654 (192.168.0.1)
```

Auditing & Intrusion Detection (cont)

Info-request (accepted)

```
Mon May 31 14:33:13 2010 CONNECT FROM C1/- host 192.168.0.1/4218
Mon May 31 14:33:13 2010 SEND INFO TO C1/-
Mon May 31 14:33:13 2010 DISCONNECT C1/- host 192.168.0.1/4218 (192.168.0.1)
```

Info-request (rejected)

```
Mon May 31 14:34:54 2010 CONNECT FROM C1/- host 192.168.0.1/4218
Mon May 31 14:34:54 2010 PERM DENIED C1/- info request
Mon May 31 14:34:54 2010 DISCONNECT C1/- host 192.168.0.1/4218 (192.168.0.1)
```

Native connection

```
Mon May 31 14:51:38 2010 CONNECT FROM C2/- host 192.168.0.1/54650
Mon May 31 14:51:38 2010 CONNECT TO S2/1 host 192.168.0.105/22 (192.168.0.1), ***NATIVE ROUTING
***
```

Auditing & Intrusion Detection (cont)

Detecting Port-scanning Attacks

```
Wed Jun 30 22:28:16 2010 CONNECT FROM C1/- host 10.0.0.1/56734
Wed Jun 30 22:28:16 2010 PERM DENIED  C1/- host 10.0.0.1 (10.0.0.1) to 192.168.3.2/3200
Wed Jun 30 22:28:16 2010 DISCONNECT   C1/- host 10.0.0.1/56734 (10.0.0.1)
Wed Jun 30 22:28:16 2010 CONNECT FROM C1/- host 10.0.0.1/56735
Wed Jun 30 22:28:16 2010 PERM DENIED  C1/- host 10.0.0.1 (10.0.0.1) to 192.168.3.2/3201
Wed Jun 30 22:28:16 2010 DISCONNECT   C1/- host 10.0.0.1/56735 (10.0.0.1)
Wed Jun 30 22:28:16 2010 CONNECT FROM C1/- host 10.0.0.1/56736
Wed Jun 30 22:28:16 2010 PERM DENIED  C1/- host 10.0.0.1 (10.0.0.1) to 192.168.3.2/3202
Wed Jun 30 22:28:16 2010 DISCONNECT   C1/- host 10.0.0.1/56736 (10.0.0.1)
Wed Jun 30 22:28:16 2010 CONNECT FROM C1/- host 10.0.0.1/56737
Wed Jun 30 22:28:16 2010 PERM DENIED  C1/- host 10.0.0.1 (10.0.0.1) to 192.168.3.2/3203
Wed Jun 30 22:28:17 2010 DISCONNECT   C1/- host 10.0.0.1/56737 (10.0.0.1)
...
```

Conclusions

Conclusions

- The **secure deployment of the SAProuter** is a **critical** issue to the **overall security** of the SAP implementation.
- If not configured securely, **an attacker may be able to access SAP systems remotely**, just as if he was sitting in the company's LAN.
- Furthermore, a vulnerable SAProuter may allow remote unauthorized parties to **access any application in the internal network**, such as SSH servers, databases, Web intranets, other business solutions, etc.
- **Onapsis Bizploit** can help you to perform basic security reviews of your SAProuters.
- It's strongly advisable to **perform comprehensive security assessments of your SAProuter and SAP implementation.**

Questions?

mnunez@onapsis.com

Thank you!

www.onapsis.com