onapsis
Securing Business Essentials

SAP® Backdoors

A ghost at the heart of your business

Mariano Nuñez Di Croce
mnunez@onapsis.com

September 16, 2010

Ekoparty Security Conference

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?

- Specialized company focused in the **security of ERP and Business-critical Applications** (**SAP®,** Siebel®, Oracle® E-Business Suite™, JD Edwards® …).
- Core business areas:
  - ERP Security software (**Onapsis X1™**, **Onapsis Bizploit**).
  - Security consultancy services.
  - Trainings on business-critical systems security.

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, …
- **Speaker/Trainer** at Black Hat, HITB, Sec-T, Hack.lu, DeepSec, Ekoparty..

Agenda

- Introduction
- A Ghost in the User Master
- Backdoors in SAP Business Modules
- Backdoors in the Authentication Procedure
- Onapsis Integrity Analyzer for SAP
- 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.

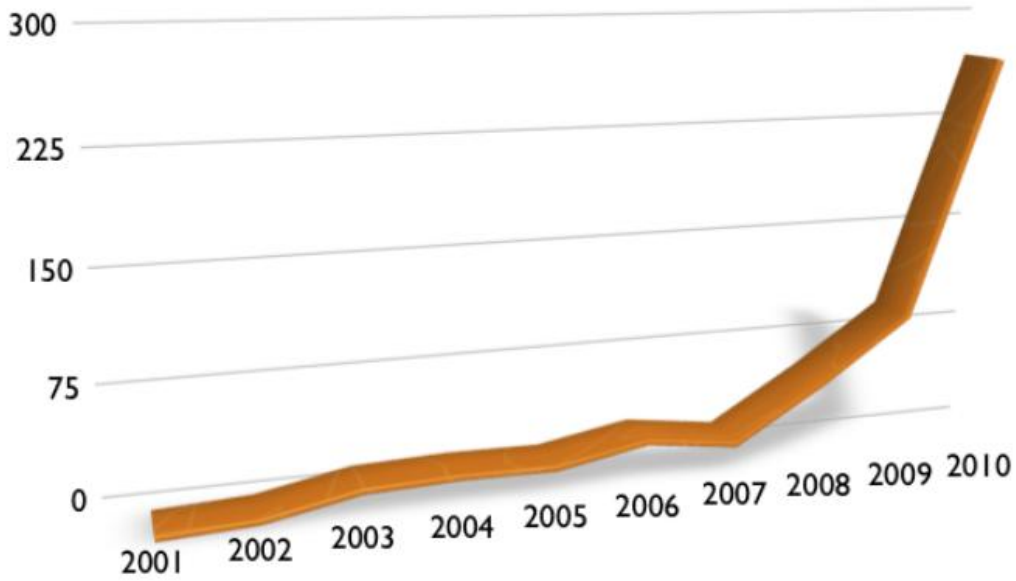
Why are SAP Backdoors special?

- Backdoors have been known since the origins of computer systems.
- However, there is very little (no) public information about how they can affect SAP platforms.
- **"Not Public" != "Not currently being exploited"**

- The biggest mis-conception in the term "SAP Security": **SAP Security is much more than Segregation of Duties!**
  - Most standards & regulations still don't get it.
  - Most Auditing companies still don't get it.
  - Some customers still don't get it.

Why are we talking about SAP security?

- SAP Vulnerabilities are in the rise.



- By default, **anyone** with network connectivity with an SAP Application Server can take **complete control** of the business information. No user, No password, No problems :P

SoD is not enough to prevent Backdoors!

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.

With that kind of privilege, a backdoor could have been installed.

Ok, but… which is the real risk?

CONFIDENTIALITY

AVAILABILITY

INTEGRITY

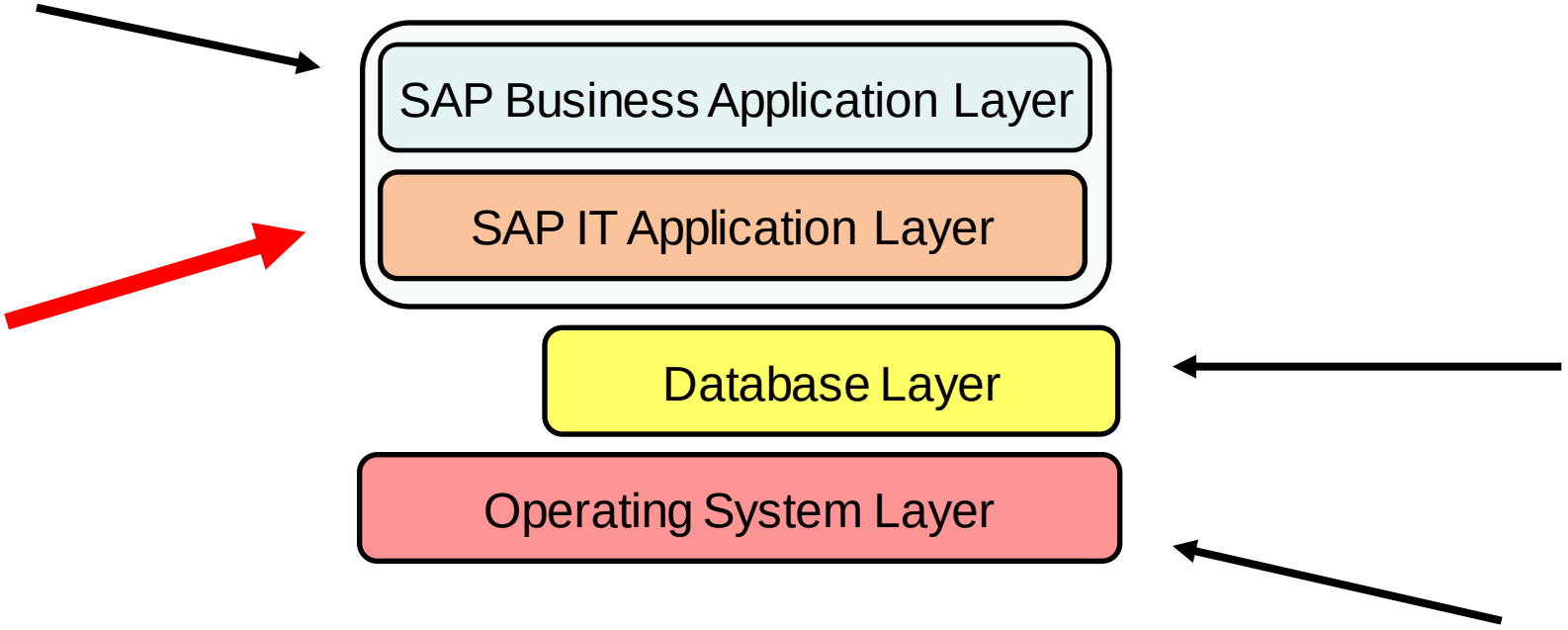
ESPIONAGE

SABOTAGE

FRAUD

The Initial Compromise

- In order to install a backdoor, the attacker **needs to compromise the system first**, and obtain high privileges.
- The Threat Model map includes the following components:



A Ghost in the User Master

Welcome to the SAP world…

- You connect to your company's Production SAP system through SAPGUI.
- **You have to specify access credentials**:
  - Client (logical "independent" unit in the SAP system)
  - Username
  - Password
- The system checks your saved password from the User Master.
- If your provided passwords matches the stored one… access granted.
- You start performing business processes and making the company earn billions.

Oops! Downwards compatibility…

- SAP has implemented different password hashing mechanisms to make systems stronger (from 8-characters MD5 to 40-characters SHA-1)

- The problem happens when a "weak" system wants to connect with a "strong" one… **integration fails -> business fails**.

- **Workaround: By default, the User Master shall contain the downwards-compatible hashes, as well as the strong one.**

- More than one password hash per user.

- This opens room for several attacks. Check Onapsis's "SAP Security In-Depth" Publication, issue #2 [2]

Oops! Downwards compatibility…

- **Which** password hash to use for comparison?
- Controlled through profile parameter **login/password_downwards_compatibility**

Value	Impact
0	Downwards-compatibility disabled. No weak hashes are generated.
1	Downwards-compatibility enabled. Weak hashes generated for integration with older releases. Weak hashes not evaluated.
2	If the logon attempt using the downwards-incompatible password fails, check if the downwards-compatible would work. Log and deny access.
3	The same as with 2, but **the logon is considered as successful**. This is registered in the system log.
4	The same as with 3, but **no system log entry is written**.

- Parameter can be modified dynamically! (No SAP restart required)

Live demo

Backdoors in SAP Business Modules

("Fraude", en criollo)

Welcome (back) to the SAP World…

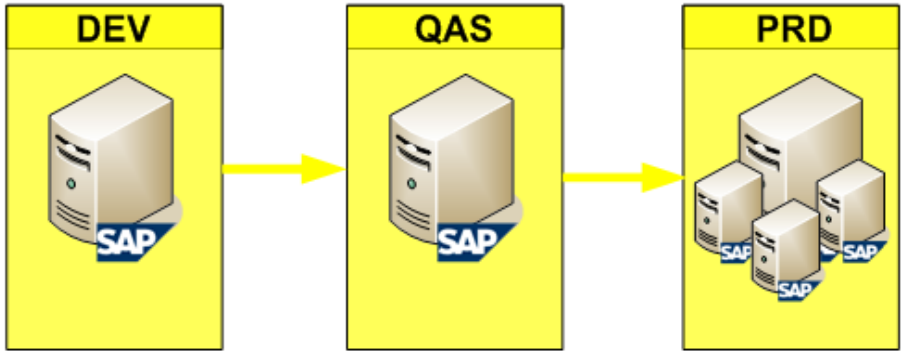
- Once logged-in, you interact with the system running Transactions.
- In fact, **you are running ABAP Programs/Reports**.
- ABAP Programs can be divided in:
  - **Standard** (Developed and Shipped by SAP A.G)
  - Custom (Developed in-house by the company. Starts with Z* or Y*)

- Standard programs can be modified, but strongly discouraged.
- **SSCR** steps in =>You must ask SAP A.G for a special key.

- ABAP Programs are stored in the **system's database**.
  - Table **REPOSRC** contains compressed source-code.
  - Table **REPOLOAD** contains ABAP load (~ bytecode).

The Change and Transport System

- Typical SAP system landscape:



- Developments and changes "can only be done in the DEV system".
- **The PRD system is configured to block any attempt to modify programs directly in the system.**

- Through this procedure, it is expected that *"the quality and availability of the SAP production systems is maximized".*

Unauthorized modification of ABAP Programs directly in the Production System is possible.

SAP's Heart: The Database

- Unauthorized modification at the SAP layer **may be possible**, **but not trivial.**
- What about the usually **mis-configured-left-by-default-LAN-accesible Database**??
  - SAP + Oracle Authentication Weakness.
  - Default *SAP Database user's* credentials.
  - Database exploits.
- The attacker can still get to the Database through the SAP system, due to the **intrinsic Trust relationships**!

- No CRC or signature check on the stored ABAP code.
- **Simple SQL queries will do the trick!**

Live demo

Backdoors in the Authentication Procedure

Protection for Critical ABAP Programs

- Certain **critical standard ABAP programs are protected** to prevent access to their source code from the SAP System, i.e. using transaction SE80.

- Started researching on **how this feature was implemented**:
  - REPOSRC.SQLX = 'X' ? No noticeable results.
  - **Special ABAP "Magic String": *@#@@[SAP]**

- If the source code contains the magic string, **the SAP Kernel rejects access to the source code**.

- However, there seems to be something else…

SAPMSYST – The SAP's Cop

- Probably **the most critical ABAP piece of code in an SAP system**.
- Handles the **User Authentication Procedure**.

- **This program is protected** through a specific, hard-coded **Kernel check**!

- The check is performed on the ABAP program's name…

- **Bypass is possible by pivoting the program in the Database.**

Live demo

Onapsis Integrity Analyzer for SAP

Onapsis Integrity Analyzer for SAP

- Purpose: **Detect modifications of ABAP code in an SAP system**.
- **Free** download from http://www.onapsis.com/ianalyzer (upcoming...)
- **Proof-of-concept**: Only working for SAP/Oracle 10g.
- Developed by Jordan Santarsieri and me @ the Onapsis Research Labs.

- Why you need it? **It's not feasible to detect backdoors from inside the SAP system itself:**
  - Backdoors can leave the Program's "Last modified date" untouched.
  - The analysis programs may have also been manipulated to hide the backdoor's presence!

Onapsis Integrity Analyzer for SAP

- Want to do it manually? Number of SAP programs are measured in hundred of thousands (and even more).
- *Onapsis Integrity Analyzer* connects with the **Database** and **performs "snapshots" of sensitive ABAP report tables.**
- Periodically, new snapshots are compared with older snapshots and modified programs are identified.
- Tracking of SAP Notes is also considered.

The detection of suspicious modifications should trigger a special investigation.

Conclusions

Some Thoughts on SAP Backdoors

- **The Backdoor threat** affects every information system; **it's not a specific SAP platform's risk**.
- Once an attacker obtained maximum privileges over an information system, it is **really** difficult to restrict his activities, and **SAP is not the exception.**
- **It's possible to modify ABAP programs directly in Production.**
- **SAP Backdoors can have devastating impacts over Business.**
- Attacks are possible through other vectors than DB access.
- These backdoors won't be installed for fun, **it's about MONEY.**

- **Onapsis's Integrity Analyzer for SAP** can help you to implement more in-depth reactive controls.

Some Thoughts on SAP Backdoors

- The best cost/effective protection: **Minimize probability of the initial compromise.**
  - Automated controls.
  - **Periodic technical security assessments of SAP platforms.**
    - Vulnerability Assessments.
    - Penetration Tests.
    - Security Audits.

Questions?

mnunez@onapsis.com

Work@Onapsis

jobs@onapsis.com

Security Researchers

Test Engineers

Python Developers

…

Thank you!

www.onapsis.com