



Vulnerabilities of SAP systems

History & Trends

Based on personal experience :
90% of existing SAP systems today are vulnerable to attacks.

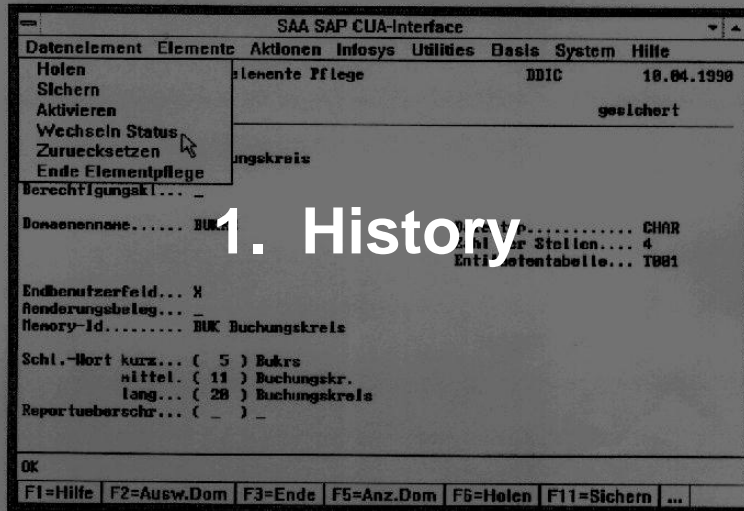
In order to avoid the exploitation of these vulnerabilities you **must** take additional measures to harden your SAP systems against attacks.

Topics of this presentation :

- **History** of the SAP application
- **Publications** about methods of attack
- **Trends** in type and frequency of attack
- **Risks**, data breach law and costs
- **Vulnerabilities** that need to be addressed

but first ...

... a practical example of an exploit ...



History

1972 : SAP was founded by 5 former IBM employees. Its first version ERP software was an accounting system called RF (later known as R/1) based on the mainframe platform that came out in 1973.



History : SAP R1

1972 : SAP was founded by 5 former IBM employees. Its first version ERP software was an accounting system called RF (later known as R/1) based on the mainframe platform that came out in **1973**.



1979 : SAP came out with R/2 that used real time data processing on a mainframe and integrated all the functions of an enterprise such as : accounting, material management, sales and delivery and human resources.

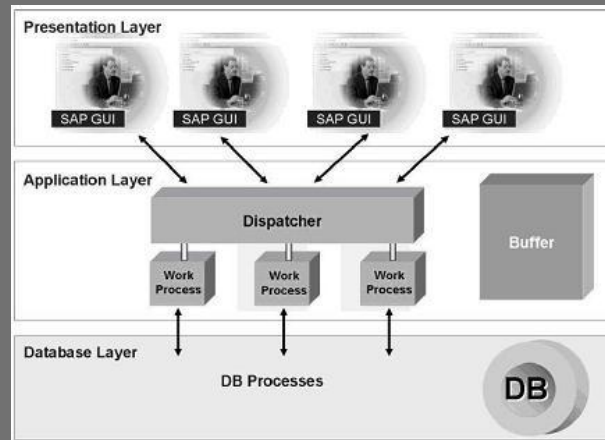
History : SAP R1 & R2

1992 : The R/3 solution was launched. The R/3 software was based on client / server architecture and ran on several different hardware platforms.



History : SAP R3

R/3 system architecture



History : example of a SAP R3 system

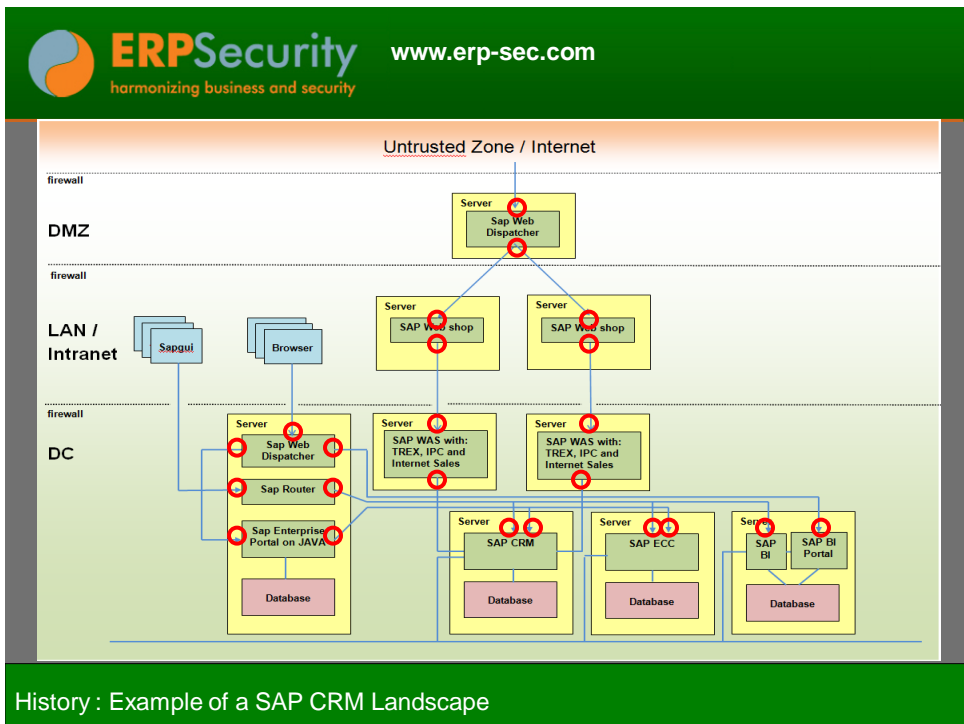
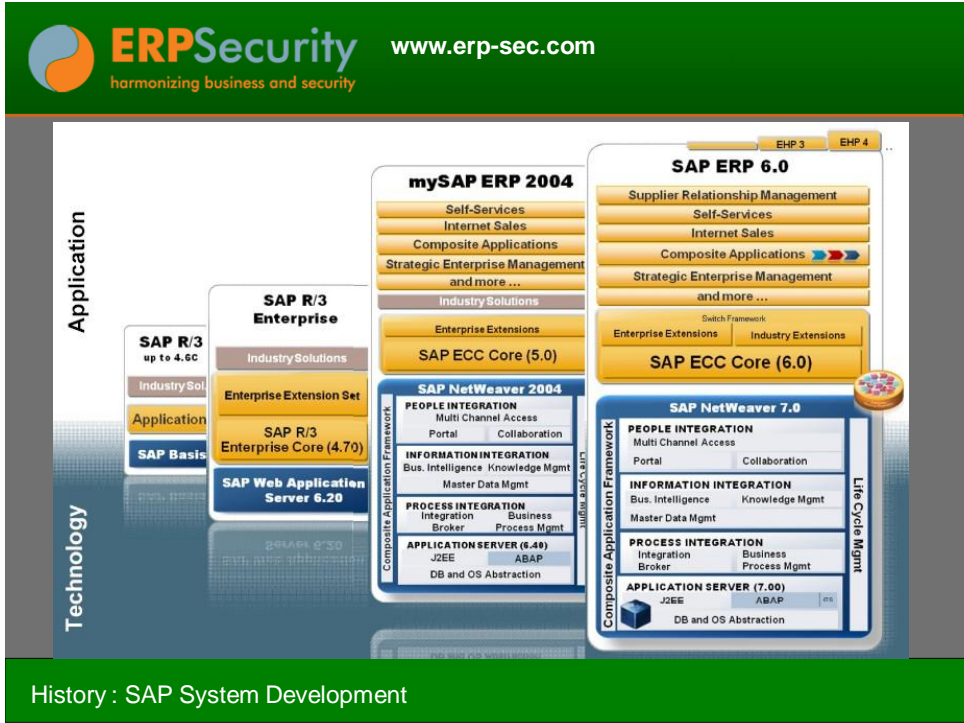
2003: SAP Web Application Server 610 & 620
2004: SAP Netweaver 2004
2005: SAP Netweaver 2004s



Today, all SAP ABAP systems are based on the SAP Netweaver component.

An important feature of SAP Netweaver is the ability to use the Internet as a communication channel.

History : SAP WAS & Netweaver



Google Search

Results 1 - 10 of about 30,900 for inurl:/scripts/wgate. (0.24 seconds)

Google

Results 1 - 10 of about 126,000 for inurl:/irj/portal. (0.26 seconds)

Google

Results 1 - 10 of about 487,000 for inurl:/sap/bc/bsp. (0.28 seconds)

Google

Results 1 - 10 of about 686 for inurl:sap/bc/gui/sap/its/webgui. (0.26 seconds)

..but high visibility has its price ...

History : SAP's internet presence



SAP systems have become visible targets
 Increased security hardening effort required
 Classical SOD type security is not enough



2. Publications

Publications

2002

SAP Virus "SAPvir" (See OSS Note 512595)

There was a lot of media attention for this virus program written in ABAP, but the risk of infection and spread could be mitigated efficiently by conventional SAP security procedures.

Publications: 2002



ERPSecurity
harmonizing business and security

www.erp-sec.com

2002

SAP Virus "SAPvir" (See OSS Note 512595) There was a lot of media attention for this virus program written in ABAP, but the risk of infection and spread could be mitigated efficiently by conventional SAP security procedures.

"Wir hacken eine SAP Datenbank"

(author Jochen Hein) An early description of hacking techniques applied to SAP and Oracle.

Publications: 2002



ERPSecurity
harmonizing business and security

www.erp-sec.com

Demo of exploit using different tools and techniques

Publications : Demo

2003
Paper "SAP Password Sicherheit "
(author: Frank Dittrich)

Publications: 2003

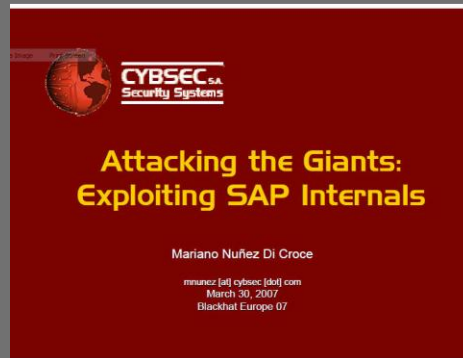
2003
Paper "SAP Password Sicherheit "
(author: Frank Dittrich)

2005
Paper review "SAP Password Sicherheit "
(author: Frank Dittrich)

Publications: 2003 -2005

2007

**Paper "Attacking the giants: Exploiting SAP internals"
(author: Mariano Nuñez Di Croce)**



Publications: 2007

2008

**John the Ripper patch for SAP passwords.
A SAP password cracker patch for the popular
password hacking tool "John the Ripper" is
officially released on the John the Ripper website
by someone called "sap friend".**

Publications: 2008



ERPSecurity
harmonizing business and security

www.erp-sec.com

2008

John the Ripper patch for SAP passwords.

A SAP password cracker patch for the popular password hacking tool "John the Ripper" is officially released on the John the Ripper website by someone called "sap friend".

2009

Paper "Sniffing SAPGui passwords"

(authors Andreas Baus & Rene Ledosquet)

This paper describes a method of obtaining the clear text passwords from the SAPGui protocol.

Publications: 2008 - 2009



ERPSecurity
harmonizing business and security

www.erp-sec.com

2009

Paper "The risks of downward compatibility"

(author: Mariano Nuñez Di Croce)

Publications: 2009

2009

Paper "The risks of downward compatibility"
(author: Mariano Nuñez Di Croce)

Paper "SAP Security: attacking SAP clients"
(author: Alexander Polyakov)

Publications: 2009

2009

Paper "The risks of downward compatibility"
(author: Mariano Nuñez Di Croce)

Paper "SAP Security: attacking SAP clients"
(author: Alexander Polyakov)

**Method of decompression of SAP's DIAG protocol
& sniffing clear text passwords**
(author: Dennis Yurichev)

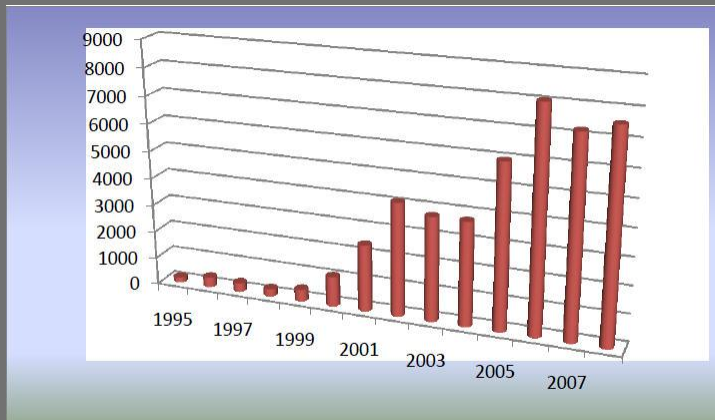
Publications: 2009

Demo of exploit using network sniffing technique

Publications : Demo



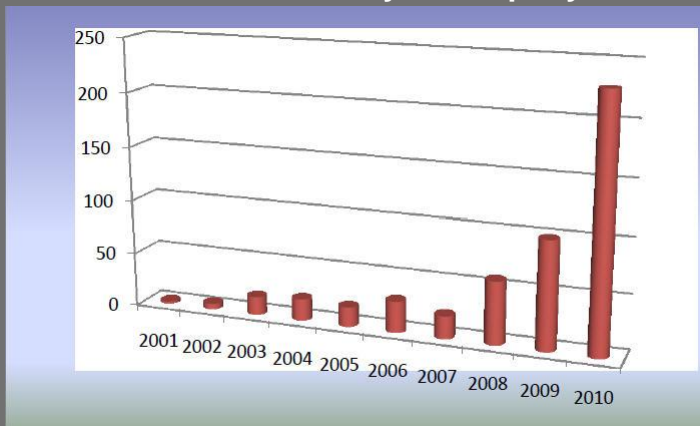
Number of CERT Cataloged Vulnerabilities



(source <http://www.cert.org/stats/>)

Trends : CERT Statistics

Number of SAP Security Notes per year



(note that value for 2010 is linearly extrapolated from 01.06.2010)

Trends : <http://service.sap.com> , Help & Support, SAP Security Notes

SAP "hardening" is rapidly becoming a new business

Trends

SAP "hardening" is rapidly becoming a new business

More wide spread availability of user friendly hacking tools

Trends

SAP "hardening" is rapidly becoming a new business

More wide spread availability of user friendly hacking tools

Users might become hackers (Insider threat)

Trends

SAP "hardening" is rapidly becoming a new business

More wide spread availability of user friendly hacking tools

Users might become hackers (Insider threat)

Global competition raises the value of business data

Trends

SAP "hardening" is rapidly becoming a new business

More wide spread availability of user friendly hacking tools

Users might become hackers (Insider threat)

Global competition raises the value of business data

Outsourcing, off shoring and 3rd party access

Trends

SAP "hardening" is rapidly becoming a new business

More wide spread availability of user friendly hacking tools

Users might become hackers (Insider threat)

Global competition raises the value of business data

Outsourcing, off shoring and 3rd party access

Hardening SAP systems requires specialist knowledge

Trends

Demo of exploit targeted at business data

4. Risks

- Data Theft
- Data Manipulation
- System Sabotage

Risks



ERP Security
harmonizing business and security

www.erp-sec.com

Examples of Data Theft

Vendors : contact persons, purchasing data
Customers : contact persons, discounts,
Sales data : sales per area per period per sales unit
HR data : personnel, contact details, wages
Materials : manufacturer, warehouse storage locations
Fi/Co : GL Account data, balance sheet, profit & loss
Plants : recipes in manufacturing

Etc. etc

Risks : Data Theft



ERP Security
harmonizing business and security

www.erp-sec.com

Examples of Data Manipulation

Accounts payable : creating a new supplier plus related purchase orders and invoices

Sales and Delivery : Changes of addresses in deliveries

HR : Creating “ghost” employees and fake timesheets

Risks : Data Manipulation

Examples of System Sabotage

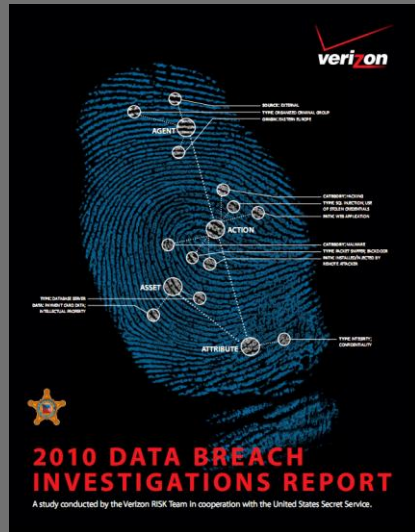
- drop a SAP database
- delete a SAP system
- stop a SAP system
- execute a denial of service attack etc. etc.

Risks : System Sabotage



2009 Annual Study: Global Cost of a Data Breach

Understanding Financial Impact, Customer Turnover, and Preventive Solutions



Risks : Data Breach Report

Top findings from Ponemon and Verizon reports :

Average organisational costs are **\$3.4 million**

Average cost per compromised record is **\$142**

48% were caused by insiders (+26%)

48% involved privilege misuse (+26%)

28% employed social tactics (+16%)

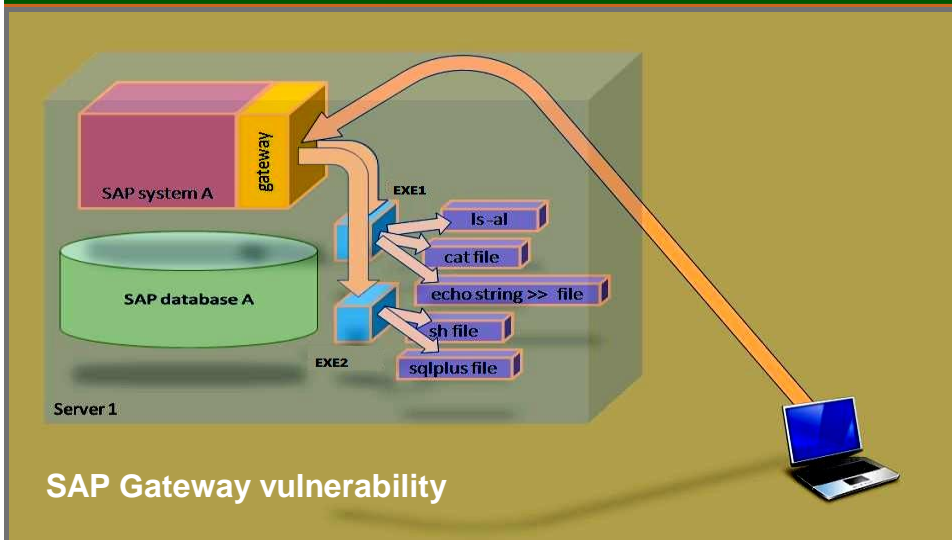
2010 Annual Study: Global Cost of a Data Breach
 Understanding Financial Impact, Customer Turnover,
 and Preventive Solutions

Risks : Data Breach Report

5. Vulnerabilities

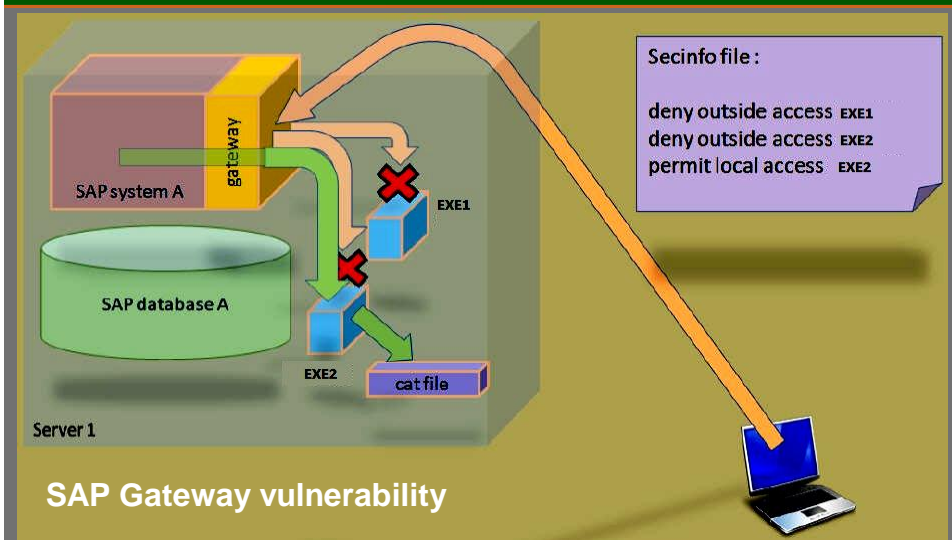
- SAP Gateway
- Downwards PWD compatibility
- Unencrypted SAPGUI

Vulnerabilities




SAP Gateway vulnerability

Vulnerabilities : SAP Gateway




SAP Gateway vulnerability


Vulnerabilities : SAP Gateway

 **ERP Security** www.erp-sec.com
harmonizing business and security


Downwards PWD Compatibility




Vulnerabilities : Downwards PWD compatibility

 **ERP Security** www.erp-sec.com
harmonizing business and security

Downwards PWD Compatibility

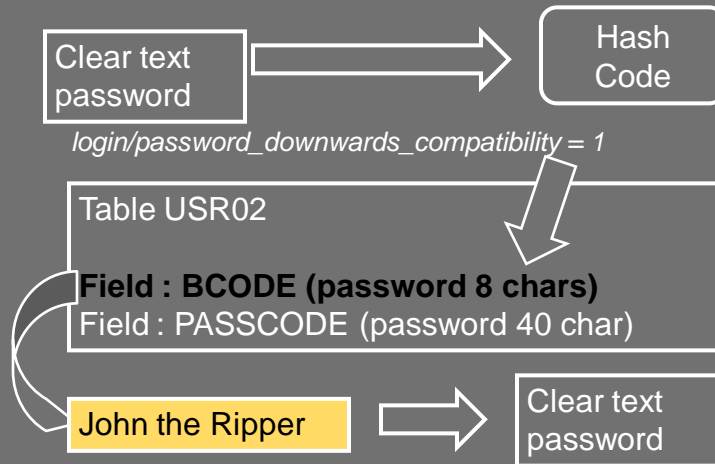


login/password_downwards_compatibility = 1



Vulnerabilities : Downwards PWD compatibility

Downwards PWD Compatibility

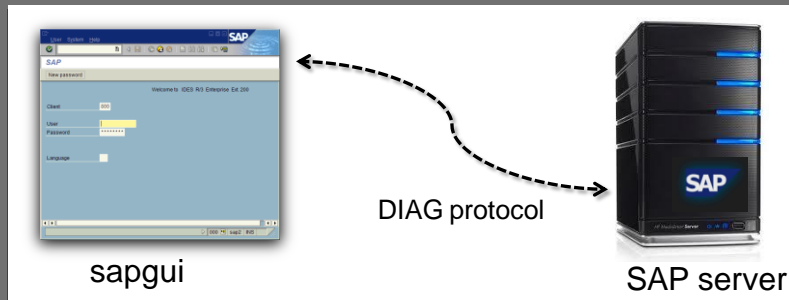


Vulnerabilities : Downwards PWD compatibility

- Disable old passwords if you can and set :
login/password_downwards_compatibility = 0
If you cannot : allow special characters in passwords.
- Restrict direct database access
- Use authorisation object S_TABU_DIS on tables :
USR02, USH02 & USRPWDHISTORY
- Use different passwords for users SAP* and DDIC in
different systems and clients
- Use the USR40 table in order to avoid easy passwords

Vulnerabilities : Downwards PWD compatibility

SAPGUI vulnerabilities



Vulnerabilities : SAPGUI

Encrypt your SAPGUI traffic !

Switch to the SAPWebgui with HTTPS (small companies)

Or: use **SNC** in combination with any 3rd party product that implements the GSS-API V2, you receive application-level and end-to-end security. All communication that takes place between two SNC-protected components is then secured.

*This also prevents attacks on the SAPIpd port as described by Alexander Polyakov.

More information about these topics ?

Download our PDF report :

“Vulnerabilities of SAP systems: history and trends”

From our website : www.erp-sec.com

QUESTIONS