Invest in security to secure investments

SAP Security Landscape.
How to protect (Hack) your (Their) big business.

Alexander Polyakov. CTO ERPScan
About ERPScan

• The only 360-degree SAP Security solution - ERPScan Security Monitoring Suite for SAP
• Leader by the number of acknowledgements from SAP (150+)
• 60+ presentations key security conferences worldwide
• 25 Awards and nominations
• Research team - 20 experts with experience in different areas of security
• Headquarters in Palo Alto (US) and Amsterdam (EU)
Large Enterprise sectors:

- Oil and Gas
- Manufacturing
- Logistics
- Finance
- Nuclear Power
- Retail
- Telecommunication
- etc.
• Business applications’ role in a typical work environment
• The need to harness them to optimize business-processes
• Scope for enormous reduction in resource overheads and other direct monetary impact.
• Potential problems that one can’t overlook
• The need to reflect on security aspects, is it overstated!
• Why is it a REAL and Existent Risk?
What can be the implications?

- **Espionage**
  - Theft of Financial Information
  - Corporate Secret and information theft
  - Supplier and Customer list theft
  - HR data theft

- **Sabotage**
  - Denial of service
  - Tampering of financial records and accounting data
  - Access to technology network (SCADA) by trust relations

- **Fraud**
  - False transactions
  - Modification of master data
• The most popular business application
• More than 250000 customers worldwide
• 83% Forbes 500 companies run SAP
• Main system – ERP
• Main platforms
  • SAP NetWeaver ABAP
  • SAP NetWeaver J2EE
  • SAP BusinessObjects
  • SAP HANA
  • SAP Mobile Platform (SUP)
Risk 1: Credit card data theft

- **Risk:** credit card data theft
- **Affects:** Companies storing and processing PCI data: Banks, Processing, Merchants, Payment Gateways, Retail.
- **Type:** Espionage
- **Module:** SD (Sales and Distribution) – part of ERP
- **Attacker can get access to tables that store credit card data.** There are multiple tables in SAP where this data is stored. Tables such as VCKUN, VCNUM, CCARDEC and also about 50 other tables. Credit card data theft is a direct monetary and reputation loss.
Risk 1: Credit card data theft

- There are multiple ways how an attacker can access the CC Data
- Even if its encrypted one can:
  - use FM to decrypt it - CCARD_DENVELOPE
  - Use Report to get decrypted
  - Or use another report to find some info RV20A003
- DEMO
- Solution: Configuration checks, Patch Management, Access Control, Code scanning
- Defense
  - Decryption of credit card data in SD - notes 766703
  - Decryption of credit card data for the whole ERP - note 1032588
  - Credit Card data in report RV20A003 - note 836079
Risk 1: Credit card data theft (DEMO)
Risk 2: Competitive intelligence

- **Risk: Compromise of bidding information**
- **Affects:** Companies using SRM for bidding
- **Type:** Espionage
- **Module:** SRM

**Competitors intelligence (Espionage)**

Access to the SAP SRM systems is available through the Internet and could provide unfair competitors sufficient loophole required to glance privileged pricing information and allow them to propose competitive pricing, thus helping in winning a tender by unfair means.
Risk 2: Competitive intelligence

• SAP Cfolders application for document exchange is a part of SRM and has some vulnerabilities and unsecure configuration problems, which could help in availing access to official pricing information.

• This means that the competitor’s documents could be completely removed from the systems, or the information might be manipulated to win a tender.

• This attack was successfully simulated during penetration tests.

• Some program vulnerabilities that aid an attacker:
  – [Link](http://erpscanc.com/advisories/dsecrg-09-014-sap-cfolders-multiple-stored-xss-vulnerabilities/)
  – [Link](http://erpscanc.com/advisories/dsecrg-09-021-sap-cfolders-multiple-linked-xss-vulnerabilities/)

• Defense: SAP Notes 1284360, 1292875
Risk 3: Intentionally causing manufacturing defects

- **Risk:** Intentionally causing manufacturing defects (Sabotage)
- **Affects:** Manufacturing sector such as Aviation, Aerospace, Automotive, Transportation, Consumer Products, Electronics, Semiconductor, Industrial Machinery and Equipment
- **Type:** Sabotage
- **Module:** SAP PLM
- **Access to SAP PLM systems could allow unauthorized changes in product creation schematics, as usually SAP PLM is integrated into CAD. This means that only one small change could result in production of a defective batch of products, causing serious financial and reputational losses and sometimes harm to life and limb.**
• FDA recalled the whole production batch of 1200 tracheostomical devices because of three deaths which were caused by technical problems

• IKEA had to recall the entire batch of 10000 beds with steel rods, claiming it to be a designer’s mistake [8], that had caused physical trauma to kids.

• Toyota was forced to recall 3 large batches of passenger cars of up to 500000 each because of wide ranging construction problems with airbags, throttle and other parts of the car having impaired functionality.[9]

• US statistics from FDA [10] reveal such recalls occurring frequently. A similar situation can also be observed with consumer products

The financial losses, caused by different traumas is about one trillion dollars per year.

* those examples are not caused by misusing SAP!
• Risk: Salary data: unauthorized data manipulation
• Affects: Every company
• Type: Fraud
• Module: HCM
• Access to the SAP HR system also allows insiders to manipulate the wage figures. Since the direct change can be easily detected, the risk lies in the manipulation potential of number of additional working hours to be processed, which in turn affects the amount payable as wages. In such a case, the fraud is extremely difficult to detect.
Risk 4: Salary data unauthorized access

- User can find out a colleague’s salary details (PA30 transaction) - > Demotivation
- Also, attacker may do this by direct table PA0008, PA0014, PA0015 access
- DEMO (PA30)
Risk 4: Salary data unauthorized access

• User can modify own salary
  – Transaction PA30 is responsible for salary access
  – Attacker can change number of hours by using this transaction

• DEMO
Risk 5: Industrial Sabotage

- **Risk**: Industrial sabotage and Disaster
- **Affects**: Every company with ICS/Technology network. Oil and Gas, Utilities, Manufacturing
- **Type**: Sabotage/Fraud
- **Module**: SAP EAM / SAP XMII
- **SAP EAM system** can have technical connections to facility managements systems thus, by breaking into EAM system it may be possible to hack facility management/SCADA/Smart Home/Smart Grid systems as well. So, if hacker can get access to SAP EAM he can more easily get access to facility management and industrial systems and he can actually change some critical parameters like heat or pressure which can lead to disaster and potential loss of life.
• Usually technology systems are not secure and based on obsolete operation systems and the only security for them is a firewall, which totally isolates them from corporate network except for those systems with which there should be connection for data transfer such as SAP EAM.

• How they attack:
  – RFC Connections
  – Shared Database or other resource
  – Same passwords for OS/DB/Application
  – Same domain
  – Simply exploit ICS vulnerabilities
Risk 6: Misappropriation of material resources

- **Risk**: misappropriation of material resources
- **Affects**: Every company with Warehouse, Or natural resources mining
- **Type**: Insider Fraud
- **Module**: MM(Material Management) – part of ECC
- **Attacker** can manipulate data about quantity of material resources in stock or delivery, pilfer from warehouses at times in collusion with the very employees entrusted with the stock taking responsibilities.
Risk 6: Misappropriation of material resources

- Exploit by direct table access
- Not so hard if you can google for it
Risk 7: Tampering banking information

- **Risk:** Tampering banking information
- **Affects:** Every company
- **Type:** Insider Fraud
- **Module:** ERP
- **Attacker can manipulate data about bank Account number of any company in database and pilfer money to a chosen account number.**
• 3000+ Vulnerabilities in all SAP Products
• 2368 Vulnerabilities were found in SAP NetWeaver ABAP based systems
• 1050 Vulnerabilities were found in basic components which are the same for every system
• About 350 Vulnerabilities were found in ECC modules.

How they can do this?
Is A Tsunami Of SAP Attacks Coming?

Ericka Chickowski

New banking Trojan modification points to greater trend of attackers targeting ERP and business critical applications

Last week at RSA Europe, a leading researcher in the security of business critical applications warned that a new wave of SAP attacks could crash down on enterprises after the discovery of an old banking Trojan had been modified to look for SAP GUI installation on infected endpoints.

The modified application was Trojan:bank, which was found to be trollering for SAP installations by researchers at Dr. WEB recently, says Alexander Polyakov, co-founder and CTO of ERPScan, who brought up the modified malware in a broader talk at RSA about the dangers of SAP ERP vulnerabilities. Polyakov told Dark Reading that one of the likely ways attackers could use such targeted malicious functionality could be for the purpose of gathering information.

New malware variant suggests cybercriminals targeting SAP users

Lucian Constantin, IDG News Service

A new variant of a Trojan program that targets online banking accounts also contains code to search if infected computers have SAP client applications installed, suggesting that attackers might target SAP systems in the future.

The malware was discovered a few weeks ago by Russian antivirus company Doctor Web, which shared it with researchers from ERPScan, a developer of security monitoring products for SAP systems.
• Main platform
• Base platform for: ERP, SRC, CRM, PLM
• Purpose: Automate business processes
• If compromised:
  • Halting of operations and other business processes
  • Fraud
  • Industrial espionage
SAP NetWeaver ABAP - Statistics

Figure 5.1-1 SAP Security Notes sorted by type in SAP NetWeaver ABAP engine

Cross-site scripting: 20.36%
Directory traversal: 15.53%
Hardcoded credentials: 3.98%
Configuration issues: 9.10%
Cross-site request forgery: 7.45%
SQL-injection: 9.31%
Code injection: 4.44%
Information disclosure: 3.55%
Denial of service: 1.18%
Other: 4.19%

Figure 5.1-2 SAP Security Notes sorted by years in SAP NetWeaver ABAP engine

- 2009: 9%
- 2010: 31%
- 2011: 25%
- 2012: 20%
- 2013: 11%
- 2014: 5%

Cross-site scripting

Figure 5.1-3 SAP Security Notes in SAP NetWeaver ABAP engine compared to all security notes by year

- 2009: 72.4%
- 2010: 88.4%
- 2011: 79.9%
- 2012: 72.9%
- 2013: 71.2%
- 2014: 69.6%

2363 vulnerabilities

erpscan.com

ERPScan – Invest In Security To Secure Investments
SAP NetWeaver ABAP - Services

- NetWeaver Application Server ABAP
  - SAP Gateway
  - SAP Message server
  - SAP Message server HTTP
  - SAP Dispatcher
  - SAP ICM
  - SAP IGS
  - SAP Enqueue server
  - SAP MMC
  - SAP HostControl
• 2002 "Wir hacken eine SAP Datenbank
• 2003 “SAP Password Sicherheit”
• 2007 "Attacking the giants: Exploiting SAP internals"
• 2009 “Attacking SAP users with SAPSploit”
• 2011 “SQL Injection with ABAP”
• 2011 “SAP (in)security: Scrubbing SAP clean with SOAP
• 2012 “The SAP Platform's Brain: Attacks to SAP Solution Manager
• 2012 “Top 10 most interesting SAP vulnerabilities and attacks”
• 2013 “Transporting evil code into the Business: Attacks on SAP TMS”
• 2013 “If I Want A Perfect Cyberweapon I’Il Target ERP
• 2014 “Analysis Of 3000 Vulnerabilities In SAP
• 2014 “Practical SAP Pentesting”
• +50 more.....
Multiple DOS vulnerabilities

- [ERPSCAN-14-011] SAP NetWeaver Dispatcher Buffer Overflow – RCE, DoS (sapnote 2018221)
- [ERPSCAN-14-012] SAP NetWeaver Dispatcher Multiple Vulnerabilities – RCE, DoS (sapnote 2025931)
- [ERPSCAN-14-014] SAP Network Interface Router – RCE, DoS (sapnote 2037492)
- [ERPSCAN-14-016] SAP Netweaver HTTPd - Partial HTTP POST requests DoS (sapnote 1966655)
- [ERPSCAN-14-017] SAP Netweaver HTTP - Slowloris HTTP POST requests DoS (sapnote 1986725)
- [ERPSCAN-14-019] SAP Netweaver J2EE Engine - Slowloris HTTP POST requests DoS (sapnote 1986725)
- [ERPSCAN-14-020] SAP Netweaver Management Console (gSAOP) - Partial HTTP requests DoS (Sapnote 1986725)
Remote backdoor update
   – Remotely (Via SAP Router)
   – Almost without any trace

SAP Router is used to obtain updates from SAP before sending them to SAP Solution Manager

Attacker can exploit SAP Router’s Heap overflow issue

After that, he can change updates on the fly

There is no way to identify this attack

Defense: SAP Security note 1820666
• Vulnerability Management
• Configuration Monitoring
• Source Code Security
• SOD

The SAP NetWeaver ABAP Platform Vulnerability Assessment Guide
• Additional platform
• Base platform for IT stuff. Like:
  – SAP Portal, SAP XI, SAP Solution Manager, SAP NWDS
  – Purpose: Integration of different systems
• If compromised:
  • Stopping of all connected business processes
  • Fraud
  • Industrial espionage
SAP NetWeaver J2EE - Statistics

**Figure 5.2-3 SAP Security Notes in NetWeaver J2EE engine compared to all security notes by year**

**Figure 5.2-1 SAP Security Notes sorted by type in NetWeaver J2EE engine**

- Cross-site scripting: 28.85%
- Information disclosure: 16.16%
- Configuration issues: 13.45%
- Missing Authorization: 9.55%
- Cross-site request forgery: 7.80%
- Other: 9.36%
- XML external entity: 1.56%
- SQL-injection: 2.53%
- Denial of service: 2.73%
- Verb tampering: 4.09%
- Directory traversal: 5.45%

513 vulnerabilities
• General services
  – SAP Visual Admin (P4)
  – SAP NetWeaver HTTP (webserver)

• Additional services
  – SAP Portal (Part of HTTP)
  – SAP SDM
  – SAP SDM Admin
  – SAP LogViewer
  – SAP LogViewer Standalone
  – SAP J2EE Telnet
• 2011. Architecture And Program Vulnerabilities In SAP’s J2EE Engine

• 2011. SAP: Session (Fixation) Attacks and Protections

• 2012. SSRF Vs Business Critical Applications: XXE Tunneling In SAP

• 2012. Breaking SAP Portal

• 2014. “Injecting Evil Code In Your SAP J2EE Systems”
• **SAP BusinessObjects** (a.k.a. BO, BOBJ) is an enterprise software company, specializing in business intelligence (BI). acquired in 2007 by SAP SE

• Additional platform for business analytics

• If compromised:
  • Fraud
  • Industrial espionage
• Business Intelligence
  – BI Platform
    • New - SAP BusinessObjects Business Intelligence Platform 4.1
    • Old - SAP BusinessObjects Enterprise XI 3.x
  – Dashboards
    • New - SAP BusinessObjects Dashboards 4.1
    • Old - Xcelsius 2008
• GRC
  – SAP Process control 10.x
  – SAP Access control 10.x
• Enterprise Information Management
  – SAP Data Services 4.2
  – SAP BusinessObjects Data Services 4.0
SAP BusinessObjects - Statistics

Vulnerabilities

Figure 5.4-2 SAP Security Notes sorted by years in SAP BusinessObjects

Figure 5.4-1 SAP Security Notes sorted by types in SAP BusinessObjects

Figure 5.4-3 SAP Security Notes in SAP BusinessObjects compared to all security notes by year

76 vulnerabilities
SAP BusinessObjects - Services

- General services
  - Apache Tomcat
  - Web application Container
  - CMS (Central management Server)
  - SIA (Server Intelligence Agent)
  - Version Management
  - Database
- Additional services
  - JobServer
  - fileserver
  - EventServer
  - crystalras.
  - ConnectionServer

http://gerardnico.com/wiki/dat/bobj/bobj_architecture
• 2011 Multiple advisories in SAP BusinessObjects
  – [DSECRG-11-011] SAP Crystal Reports 2008 — Multiple XSS

• 2010 ”Hacking SAP BusinessObjects”

• 2014 “SAP BusinessObjects Attacks”
• [ERPSCAN-13-001] SAP Xcelsius – Insecure Crossdomain Policy

• CSNC-2013-016 SAP BusinessObjects Explorer Port-Scanning

• CSNC-2013-017 SAP BusinessObjects Explorer Cross-Site-Flashing

• CSNC-2013-018 SAP BusinessObjects Explorer XXE
• New platform SAP HANA (High-Performance Analytic Appliance)
  – In-memory relational database management system
• Will be default database for all systems
• If compromised:
  • Fraud
  • Industrial espionage
  • Sabotage
SAP HANA - Statistics

14 vulnerabilities
SAP HANA - Overview
• A lot of new SAP technologies which can be used for attacks
  – XSJS
  – Web IDE
  – Call c/c++ function directly from browser (XSCFUNC)
• XSJS
  – This is HANA’S version of Server Side Javascript
  – UI rendering completely in the client
  – Server side procedural logic in Javascript
  – All artifacts stored in the SAP HANA repository
• Client side javascript code injection
  – service.xsjs (note 1993349 )
• Server side javascript code injection
• Code injection
  – net.xsjs (note 2015446)
• SQL injections
  – [ERPSCAN-14-013] SAP HANA metadata.xsjs - SQL injection (note 2067972)
• R – language
• Can be used to extend SQLScript functionality
• It is possible to
  – Read OS files
  – Write OS files
  – Execute OS code
  – Open remote connections
• CREATE R SCRIPT privilege should be assigned

Example of procedure creation:

```
CREATE PROCEDURE p_name(param)
LANGUAGE RLANG AS
BEGIN <R CODE HERE>
END.
```

“HANA supports the usage of R, but R is not part of the HANA shipment. HANA just delivers an adapter. A customer has to install an R server on a separate server (it is not supported to install an R server on the HANA machine) and secure this server appropriately. That means the most customers are not affected by R issues.” – says SAP PSRT
• [ERPSCAN-14-010] SAP HANA Application Lifecycle Manager – CSRF Token Bypass
• Hardcoded keys
• User details (including passwords) stored in *hdbuserstore*
• Located in the */usr/sap/hdbclient/SSFS_HDB.DAT*
  – User data (login, encrypted pass)
  – Encrypted Root key
  – Encrypted Other keys
- File: SSFS_HDB.DAT
- Signature: RSecSSFsData
- Algorithm: 3DES
- Default key: The same as in the ABAP Security Storage
• SAP HANA – in memory database
• But it drops some data into FS
  – Backup
  – Savepoint

“The SAP HANA database holds the bulk of its data in memory for maximum performance, but it still uses persistent disk storage to provide a fallback in case of failure. Data is automatically saved from memory to disk at regular savepoints. The data belonging to a savepoint represents a consistent state of the data on disk and remains so until the next savepoint operation has completed. After a power failure, the database can be restarted like any disk-based database and returns to its last consistent state”

– SAP HANA Security Guide
• “Data volume encryption ensures that anyone who can access the data volumes on disk using operating system commands cannot see the actual data. If data volumes are encrypted, all pages that reside in the data area on disk are encrypted using the AES-256-CBC algorithm.”

• “After data volume encryption has been enabled, an initial page key is automatically generated. Page keys are never readable in plain text, but are encrypted themselves using a dedicated persistence encryption root key.”
“SAP HANA uses SAP NetWeaver SSFS to protect the root encryption keys that are used to protect all encryption keys used in the SAP HANA system from unauthorized access.”

- **SSFS_HDB.DAT**
  - HDB_SERVER/PERSISTENCE/ROOTKEY
  - HDB_SERVER/DPAPI

- The persistence encryption feature does not encrypt the following data:
  - Database redo log files
  - Database backups
  - Database traces
• Vulnerability management
• Change the encryption key after installation
• Restrict access to the key file
• Restrict access to the DAT file
• SAP HANA Security Guide
• Secure storage in the file system:
  – [http://help.sap.com/saphelp_nw70ehp2/helpdata/en/a0/82dd0abbde4696b98a8be133b27f3b/content.htm](http://help.sap.com/saphelp_nw70ehp2/helpdata/en/a0/82dd0abbde4696b98a8be133b27f3b/content.htm)
• SAP HANA Security Overview
• SAP Mobile Platform
  – From 3.0
  – Formerly Sybase Unwired platform (before 2.3)

• Mobile Applications (318+ applications)
**SAP Mobile Platform - Architecture**

**Backend Systems**
- SAP ERP 6.0 Ehp4
- SAP ERP 7.0 APO
- SAP BusinessObjects

**Middleware**
- SAP Mobile Platform

**Device**
- iPad
- Smartphone
• Information disclosure
• Man in the middle
• Hardcoded data
• Buffer overflow
• Code injection
• RCE

Sybase Mobilink, SQL Anywhere
CVE-2008-0912
SAP Mobile Platform – Mobile applications

- Hardcoded Credentials (patching)
- Lack of permissions (patching)
- Stored certificates (patching)
- SQL Injections
  - [ERPSCAN-13-024] SAP EMR Unwired – Multiple SQL Injections (note 1864518)
• EAS-SEC: Recourse which combines
  – Guidelines for assessing enterprise application security
  – Guidelines for assessing custom code
  – Surveys about enterprise application security
• 1. Lack of patch management
• 2. Default passwords
• 3. Unnecessary enabled functionality
• 4. Remotely enabled administrative services
• 5. Insecure configuration
• 6. Unencrypted communications
• 7. Internal access control and SoD
• 8. Insecure trust relations
• 9. Monitoring of security events

• Critical networks are complex
• System is as secure as its most insecure component
• Holistic approach
• Check eas-sec.org
• Check erpscan.com