13 Real ways to destroy business by breaking company’s SAP Applications and a guide to avoid them

Alexander Polyakov (CTO 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)
• Most of my work has focused on SAP Security
• Things that will be discussed can be applied to every system
• Since I enjoy a closer familiarity with SAP, most examples will be SAP relevant.
• Then again all ideas, attacks, risks can be applied to every system
• This talk is not really a faultfinding exercise with SAP, as can be easily misperceived.
• This talk is about the ‘need to know’ things, ones you can’t afford to ignore after implementation of any business application processing critical data
• So, let’s go!
Big companies

- Oil and Gas
- Manufacturing
- Logistics
- Finance
- Nuclear Power
- Retail
- Telecommunication
- etc.
Business applications can make your life easier

The need to harness them to optimize business-processes

Scope for enormous reductions in resource overheads and other direct monetary benefits.

Potential problems that one can’t disregard

The need to consider security, can it be overstated!

Why is it REAL and Existent Risk?
What can happen

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

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

- **Fraud**
  - False transactions
  - Modification of master data
Risk 1: Stealing credit card data

- **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: Stealing credit card data

- There are multiple ways how an attacker can access the CC Data
- Even if it’s encrypted you 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: Stealing credit card data

Which payment cards will be invalid in a specific period of time?

Card invalid during: 05.10.2000 to 01.01.2030
Payment card type:
Cardholder:
Card valid from:
Payment card category:
Payment card block:

<table>
<thead>
<tr>
<th>Type</th>
<th>Card number</th>
<th>Exp. date</th>
<th>Name of cardholder</th>
<th>Valid from</th>
<th>Cat</th>
<th>Block</th>
<th>Issuing bank</th>
</tr>
</thead>
<tbody>
<tr>
<td>VISA</td>
<td>4100000000000001</td>
<td>31.05.2005</td>
<td>Andrew Sands</td>
<td>02.07.2003</td>
<td>01</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VISA</td>
<td>4200000000000000</td>
<td>31.12.2007</td>
<td>Tech Inc.</td>
<td>19.11.2004</td>
<td>01</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Risk 2: Competitive intelligence

- **Risk:** Compromising competitor’s 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 give unfair competitors an opportunity to access 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 allow attacker to do that:
- Defense: SAP Notes 1284360, 1292875
Risk 3: Creating defects in products intentionally (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 cause unauthorized changes in product creation schematics, because 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 even casualties.
Risk 3: Creating defects in products intentionally

- 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 obligated to recall 3 large batches of passenger cars totaling up to 500000 each time because of wide ranging construction problems, with airbags, throttle and other parts of the car not working properly.[9]
- USA statistics from FDA [10] tells us about such recalls occurring frequently. The same 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 4: Salary data unauthorized modifications

- **Risk:** Salary data: unauthorized modifications
- **Affects:** Every company
- **Type:** Fraud
- **Module:** HCM
- Access to the SAP HR system also allows insiders to manipulate the wage amounts. 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 affects the amount payable as wages. In such a case, the fraud is extremely difficult to detect.
Risk 4: Salary data unauthorized modifications

- 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 modifications

- 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: Delayed Salary payout (Sabotage)

- **Risk:** *Delayed Salary payout (Sabotage)*
- **Affects:** Every company
- **Type:** Sabotage
- **Module:** HCM
- Denial of service on the HR system, for e.g. on a payday could lead to holding up of salary payouts resulting in employee disgruntlement, thereby negatively impacting productivity. The implementation of this attack with a certain periodicity in case of a difficult economic situation for the company or the geopolitical situation could even potentially lead to work strikes.
2% (~60) of vulnerabilities in SAP can be exploited for DOS attacks

- Most of services are vulnerable:
  - SAP Gateway
  - SAP Message Server
  - SAP Router
  - SAP Dispatcher
  - SAP MMC
  - SAP Portal

- Sometimes you do not need a vulnerability
- You can execute some heavy functionality
Risk 6: Falsification of business-critical data

- **Risk**: Falsification of business-critical data to allocate more than needed or simply unneeded expenditure.
- **Affects**: Every company with asset management
- **Type**: Sabotage/Fraud
- **Module**: EAS
- If an attacker can get access to these systems he can modify data about some equipment conditions in different ways. For example, he may change data passing from CMB (Condition Based Maintenance) in such way that there is a need to replace different elements of facilities. Such an act will thus force the company to spend money and time on new equipment when it is not needed.
• For better optimization of Business Processes EAM systems sometimes are integrated with CBM where the state of the equipment is observed and monitored continually on a real-time basis.

• Deviations from a standard range or tolerance will cause some form of alarm and identification of the need for a maintenance intervention.

• So, if an attacker can get access to those systems he can modify data about some equipment health in different ways.

• Attack on EAM, Attack on CBM, Attack between systems.
Risk 7: 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 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:** Unauthorized tampering with Financial Reports
• **Affects:** Every company with Business Objects BI
• **Type:** Sabotage
• **Module:** SAP BI

  – *Financial reports: unauthorized data modification* - divert the attention of management causing problems with the auditors and leading to drying up of investment return on projects.

  – *Tangible and intangible resources unauthorized data modification* - improper estimates from the incorrect data on the spending of resources and workload of employees. This could lead to the misuse of funds and cause direct and indirect losses.

  – *Sales reports unauthorized data modification* - wrong conclusions about pricing strategy and policies
Risk 8: Modification of reports

- SAP BI system is based on SAP Business Objects platform
- Around 80 vulnerabilities were found in this platform
- The number of vulnerabilities is growing
Risk 9: Remote Illegal updates upload

- **Risk**: Illegal updated upload
- **Affects**: Every company
- **Type**: Sabotage/Fraud
- **Module**: Solution Manager

SAP Solution Manager is a platform which allows SAP Basis team to remotely control, monitor, and update other SAP Solutions. Thus, by obtaining access to Solution Manager it is possible to upload any backdoor code on each SAP System in disguised as a legal update.
What's more dangerous is that attack can be exploited
  – 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 a fly

There is no way to identify this attack

Defense: SAP Security note 1820666
Risk 10: Portal Denial of service

- **Risk: Customer** Portal denial of service
- **Affects:** Every company with public portal on SAP
- **Type:** Sabotage
- **Module:** SAP Enterprise portal
- **Denial of service vulnerabilities in SAP EP which can be exposed to internet can lead to downtime with portal operations. If it is a customer portal, company may have huge monetary and reputation losses. Such attack was performed against Nvidia company.**
Risk 10: Portal Denial of service

- SAP Portal has about 600 Vulnerabilities (In Platform and Applications)
- Some of them can be exploited without any authentication
- Most critical issues such as Verb Tampering can also be used to obtain full control on a system
  - Create users
  - Assign roles
  - Execute OS commands
Risk 11: Attack from Internet

- **Risk: Access to company’s internal resources**
- Affecting: Every company with public portal on SAP
- Type: Espionage
- Module: SAP Enterprise portal
- Different vulnerabilities in SAP EP which can be exposed to internet can lead to unauthorized access not only to SAP Portal itself but also to internal resources of company.
• SAP Portal usually can be accessed via Internet
• More than 1000 SAP Portals exist in Internet
• Using vulnerabilities in portal attacker can
  – Use Single-Sign-On and login into any internal system
  – Attack internal systems using SSRF vulnerability
  – Search for passwords stored in Portal KM
- **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 12: misappropriation of material resources

- Exploit by direct table access
- Not so hard if you can google for it

---

**Access Table Relationship MM**

The field of Materials Management (MM = Material Management) is very extensive and includes such B. inventory management and purchasing.
- The table EKKO is the head of the table orders (linked above field EBELN with the position table EKPO EKPO) and across the fields EBELN and EBELP with the classification.
- The table LFA1 is the head table of suppliers (linked via the field LIFNR 2 with the purchase order header table EKKO).
- In the address table ADRC many addresses are stored for suppliers (associated with the order header table EKKO over the ADRNR field).
- The purchase requisition table / Purchase Requisition EBAN may precede an order (associated with the order item table EXPO over the fields BANFN and BNFPO).
- In MM-range order history table EKBE is comparable to the table VBPA in the SD area (linked to the purchase order item table EXPO over the fields EBELN and EBELP. In (transaction order history) refer the GJAHR, BELNR and BUZEL fields in different tables MSEG (material document), RSEG (incoming invoice) or BSEG (Accounting Doc).
- The purchase invoice has the head table RBKP and the position table RSEG (linked via the fields EBELN and EBELP with the order item table EXPO).
- The head table for the Buchhaltung is BKPF (linked via the AWKEY fields (reference key) to input the Invoice header table RBKP (fields BELNR and GJAHR).
- The head table for the Material Master is the MARA (linked via the MATNR field with the order item table).
• Risk: Changing bank account data
• Affects: Every company
• Type: Insider Fraud
• Module: ERP
• Attacker can manipulate data about bank Account number of any company in database and transfer 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.
Public examples
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

Nvidia downs customer service portal over SAP bug

Published on 9th January 2014 by Gareth Halfacree

Nvidia has been forced to disable access to its customer service portal following the discovery that it was vulnerable to a three year old vulnerability in its back-end software.

The NVCare website, used for customer support and warranty claims, has been deactivated by Nvidia following the public disclosure of a vulnerability in its back-end platform on the Full Disclosure mailing list earlier this week. According to the poster, identified only by the alias ‘Finger’, the bug was first reported to Nvidia on the 21st of November but with no response prior to the public release of the details.

Embarrassingly for the company, the flaw highlighted in the report was not a new one, the vulnerability in

WEB & COMMUNICATION SOFTWARE

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.
- Price of vulnerability is low
- Patching is nightmare
- Creation of exploit is easy
- Interconnection is high
- Availability via internet

**Ease of development**

**NetWeaver ABAP versions by popularity**

- 7.0 EHP 0 (Nov 2005) - 36%
- 7.0 EHP 2 (Apr 2010) - 11%
- 7.0 EHP 1 (Oct 2008) - 19%
- 7.3 (Jun 2011) - 6%
- 6.2 (Dec 2003) - 5%
- 6.4 (Mar 2004) - 5%

**Exposed services 2011**

- SAP HostControl
- SAP Dispatcher
- SAP MMC
- SAP Message Server httpd
- SAP Message Server
- SAP Router

**Exposed services 2013**

- SAP HostControl
- SAP Dispatcher
- SAP MMC
- SAP Message Server httpd
- SAP Message Server
- SAP Router
• 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