SAP, Credit Cards and the Bird that Talks Too Much

Visit us at stand A10 for interactive Q&A and live SAP hacks

Ertunga Arsal
Agenda

‣ Business Processes
‣ SAP Systems
‣ Exploit Demo
‣ “SAP Credit Cards and Birds”
‣ External Payment Solutions on SAP
‣ How to Stay Secure
‣ About Us
Want to know how this happened?
Part I - The Business Processes

The Background
SAP: The Dominating System

- SAP ERP is pretty much the dominating system which translates the business processes to the digital world
- Covers almost all aspects of business
- Allows extensive customizations
- SAP is the core of major businesses
Attacking the Core

- SAP systems are complex systems
- Numerous components
- Rarely hardened
- ...or properly patched
- It does not stop there...
  - SAP applications contain 3rd party ABAP add-ons
How can it be attacked?

Example: BASIS Components

- [ESNC-2013-003] Remote OS Command Execution in SAP BASIS Communication Services
  - Allows OS command execution, with the rights of the SAP application server
  - We reported this in 2011, it got patched in 2013 [SAP Note 1674132]
  - SAP’s CVVS v2 base score for this vulnerability is **6.0 (Medium Risk)**

- We were able to bypass the patch’s protection
  - Second patch came a couple of months later [SAP Note 1826162]
  - This time CVSS v2 score is: **7.5 (High Risk)**

- Same vulnerability higher CVSS score
How can it be attacked?

3rd Party Components

- [ESNC-2013-004] Remote ABAP Code Injection in OpenText/IXOS ECM for SAP NetWeaver
  - Widely used 3rd party component for archiving and document management.
  - Vulnerability allows injecting ABAP code to the SAP system.
Exploit Demo

Becoming an admin user on the SAP system
What is a Business Process?

› Collection of related activities that produce a specific service or product for customers
› Begins with a customer’s need and ends with a customer’s need fulfillment.
› Commonly done using SAP systems

Famous Example: The pin factory by Adam Smith
The attacker could directly go to vendor payment history for determining the target bank accounts of vendors.
Determining Victim Bank Accounts

- Attacker can filter out uninteresting accounts and focus on ones where the victim company will transfer more than 10,000 EUR.
Attacker can pick the largest sum which will be paid
Attacker can also check when the transfer will be done
Now only one step is left for the result
  – Replacing the bank account of the Vendor with the attacker’s bank account
Changing the Bank Accounts

- Attacker runs the transaction FK02 and searches victim vendor
- Attacker replaces the account number of the vendor with evil one
- When the payment time comes, sum is transferred to the attacker’s account
For the second part of the presentation, we assume that the attacker has sufficient authorizations for executing any action mentioned later.

- By exploiting vulnerabilities
- Collusion
- Existing rights

So, system is compromised. But where else can the attacker go from there?

Before that, let’s talk about credit cards and the birds...
Part II - SAP Credit Cards and Birds

Credit Card Processing on SAP
Credit Card Processing on SAP

- Sales and Distribution (SD) and many SAP modules utilize payment card processing
  - Customer orders
  - Retail point of sale (POS)
  - Financial accounting
  - Internet commerce
  - HR - travel expenses
- The cardholder data passes through SAP system and it is stored on the system on many occasions
  - Data tables
  - Change documents
  - Transaction logs
  - DB logs
- Only few external solutions use tokenizing and external portals, outside SAP
Credit Card Data

DB Tables

- During our research, we found more than 50 SAP database tables which contain e.g. credit card numbers
- The used tables differ based on which modules and functionalities are used/activated on the customer
- Some common SAP tables are:

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FPLTC</td>
<td>Payment cards: Transaction data - SD</td>
</tr>
<tr>
<td>BSEGC</td>
<td>Document - Data on Payment Card Payments</td>
</tr>
<tr>
<td>VCKUN</td>
<td>Assign customer-credit card</td>
</tr>
<tr>
<td>VCNUM</td>
<td>Credit card master</td>
</tr>
<tr>
<td>Pa0105 (Subtype 0011)</td>
<td>HR Master Record: Infotype 0011 (Ext.Bank Transfers)</td>
</tr>
<tr>
<td>PCA_SECURITY_RAW</td>
<td>Card Master: Encryption</td>
</tr>
<tr>
<td>CCSEC_ENC, CCSEC_ENCV</td>
<td>Encrypted Payment Card Data</td>
</tr>
<tr>
<td>CCARDEC</td>
<td>Encrypted Payment Card Data</td>
</tr>
<tr>
<td>/PMPAY/PENCRP</td>
<td>Paymetric – Encrypted Paymetric Card Data (for offline usage, now obsolete)</td>
</tr>
</tbody>
</table>
Accessing Cleartext Cardholder Information

Recipe

- Type SE16 at the command bar of SAPGUI after you logon, hit Enter.
  - Type the table which you want to display and press Enter.
  - E.g. FPLTC
- Enter your criteria (empty == all)
- Copy paste the data as desired to your favorite PasteBin
Accessing Cleartext Cardholder Information
Using Remote Function Calls

- RFC (Remote Function Call) protocol can be utilized to script the access and to run the functions remotely.
- SOAP-RFC over HTTP allows Internet based access to RFC functionality.
- RFC_READ_TABLE function allows generic access to contents of the tables.
- Sapsucker could be used for it?

Sapsucker

Bird

The sapsuckers are four species of North American woodpeckers in the genus Sphyrapicus. Wikipedia

Scientific name: Sphyrapicus
Rank: Genus
Higher classification: Picinæ
Lower classifications: Red-breasted Sapsucker, Williamson’s Sapsucker, Yellow-bellied Sapsucker, Red-naped Sapsucker

Free Tool? - Sapsucker

- Named after the famous bird
- Allows easy access to SAP tables via RFC and HTTP(s) protocols
- Allows reusing XSSed SAP logon cookies for RFC connections
- SNC (Secure network communications) supported
- SAP router supported
- Easily extract and filter sensitive data
Due to PCI-DSS requirements, cardholder data must be encrypted.

– Tables e.g. PCA_SECURITY_RAW, CCSEC_ENC, CCSEC_ENCV, CCARDEC, /PMPAY/PENCNP contain encrypted data (if encryption is enabled)

Program RS_REPAIR_SOURCE spawns a code editor

– An attacker could use it to type malicious ABAP code, even on production systems
Are we the only ones?

- The data can be decrypted via function modules **CCARD_DEVELOPE** or **CCSECA_CCNUM_DECRIPTION**
  - the RFC /PMPAY/P_ENCRYP_RFC or **XIPAY_E4_CRYPTO** for Paymetric
- People are already doing this!
  - and they are sharing their experiences
External Payment Solutions on SAP
External Vendors for Payment Solutions

- It is common to see external solutions for securing CC data
  - Paymetric XiPay-XiSecure (cool tokenizing stuff) and others such as GMAPay, PaylinX, DelegoSecure, Princeton CardConnect to name a few...

- Secure (assuming) payment solution + insecure SAP system equals to?

- Most common solutions use “registered RFC servers” for SAP connectivity
External Payment Card Interface Connectivity - with registered RFC Servers

1. Payment Card Interface Server registers itself on SAP Gateway and accepts connections.

2. External programs can send requests to PCI Server over the gateway via RFC protocol.

A. SAP system can send requests to PCI Server over the gateway via RFC protocol.

B. Reginfo ACL defines who can register a server or connect to a registered server.

SAP, Credit Cards and the Bird that Talks Too Much

Ertunga Arsal - BlackHat Asia 2014
External Payment Card Interface Connectivity

Standard Concept - Common Security Issues

- Customer does not configure ACL
- ACL can be bypassed (missing SAP kernel patch)
- Customer uses SAP’s tool to generate the access control list
  - SAP’s reginfo ACL generator creates access lists with $\text{ACCESS=*}$
  - SAP does not acknowledge this as a security issue
- Predictable TP names of payment processors
  - enabling unauthenticated attacks
External Payment Card Interface Connectivity

With registered RFC Servers - Attacks

1. Payment Card Interface Server registers itself on SAP Gateway and accepts connections.

2. SAP system sends requests to PCI Server over the gateway.

SAP System

Gateway Service

PCI Server

CC_AUTHORIZATION

CC_SETTLEMENT

Reginfo ACL defines who can register a server or connect to a registered server.

Evil external programs can send requests to PCI Server over the gateway via RFC protocol to extract CC information.

MITM: An attacker can pretend to be PCI server by registering with the same TP ID to sniff CC information or to trick the SAP system that payment is complete.

Merchant/Bank

Mitm: An attacker can
pretend to be PCI server
by registering with the same TP ID to sniff CC information or to trick the SAP system that payment is complete.
Further Security Issues

- Modern solutions that use e.g. SAP PI (process integration) are often misconfigured with fatal flaws
- Debugging or system tracing is not switched off.
- SNC (transport encryption) is rarely used between PCI and SAP system
- Redirecting e.g. SAP web shop users to an external provider (before payment) to avoid being in the PCI-DSS scope is the new trend
  - *Tokenizing* on its own is not sufficient. The SAP system must also be hardened.
- PCI-DSS auditors generally have little or no knowledge about SAP security.
External Payment Card Interface Connectivity

Standard Concept - Resulting in

- Man-in-the-middle attack for CC_SETTLEMENT and CC_AUTHORIZATION functions
- Credit card data theft
- Fake transaction authorization
  - SAP system can be fooled that transaction is complete and it can deliver the goods
- Foreseeable consequences
  - brand damage, legal consequences etc.
- And some unforeseeable consequences...
or Something More Entertaining
I’ve heard at many conferences that SAP should be more social networking enabled, so let’s do it!

Tampering the payment card interface functions is possible
- e.g. SD_CCARD_AUTH_CALL_RFC could allow capturing credit card numbers real-time
  - Including validation status, card validation code cvv2 (called cvc2 for mastercard, same thing)

Introducing TweetBttM
- THE FIRST SAP CREDIT CARD TO TWITTER INTERFACE
- Allows SAP system to tweet after a credit card transaction
- Requires patching SAP’s code, voids warranty!
  - That should be the least of your worries
- Fallback to DNS tunneling when Twitter is unreachable
TweetBtttM* Challenges

- Twitter changed its API this year so HTTP is not allowed anymore
  - Good side: PCI-DSS compliant backdoor
  - Requires importing Twitter’s cert via transaction STRUST
    - Workaround by invoking SAPGENPSE
  - Delays: 1-3 seconds per tweet

- DNS tunnel fallback when outbound connection is blocked
  - Function module RFC_HOST_TO_IP is (mis)used as a poor man’s DNS tunnel on ABAP

- Public source code?
  - Still in discussions with the legal guys. Follow me on twitter to stay informed :)

*BtttM = Bird that talks too much
Part III - How to Stay Secure

from unforeseeable consequences
No.1: Address The Complete Picture

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Passwords</td>
<td>Users with Critical Rights</td>
<td>Vulns in SAP’s Code</td>
<td>Missing for Gateway and Message Server ACLs</td>
<td>Direct Access to Tables</td>
<td>Os Vulns</td>
</tr>
<tr>
<td>Weak Passwords</td>
<td>Mandant Jumping</td>
<td>Vulns in 3rd Party Addons</td>
<td>Vulnerable SAP Services</td>
<td>Listener/Connection Security</td>
<td>SID Jumping</td>
</tr>
</tbody>
</table>
No.2: Implement a Holistic Process to Stay Secure

- **Prevention**
  - Vulnerability Discovery
  - Automatic Issue Fixing

- **Detection**
  - Real-time security monitoring
  - SAP event correlation

- **Response**
  - Automatic Threat Mitigation
  - Automatic Firewall Rule Creation
No.3: Automate It

- Automated SAP security scans
- Automated SAP PCI-DSS compliance checks
- Automated ABAP code corrections
- Automated SAP real-time monitoring
- Automated SAP event correlation
- Automated continuous integration into Security Incident Event Management - SIEM
- Automated SAP vulnerability/issue fixing (remediation)
- Automated SAP intrusion detection, prevention and alerting
ESNC GmbH

- ESNC assesses and fixes security vulnerabilities in SAP systems
  - ESNC Security Suite: Pentesting, real-time SAP security monitoring and automatic vulnerability mitigation
- Headquarters in Munich
- Customer base: Governmental institutions, banking, utilities, automative, oil and other critical industries
- Presenter: Ertunga Arsal
  - Security researcher with long history and focus on SAP
  - Audited hundreds of corporate and government enterprise SAP systems to date
  - Credited by SAP for 75 security patches in 2013 (over 100 vulnerabilities in total)
  - Lecturer “Systems and Network Security” at Sabanci University for postgraduates
  - Speaker at CCC annual congress, Defcon Hashdays, Deepsec, Sec-T etc...
  - Founder of ESNC
The Menu of SAP Security

- A01 - SAP Audit & Assessment
- A02 - SAP PCI DSS 3.0 Compliance
- A03 - SAP Remediation and Risk Management
- A04 - Security Policy Enforcement on SAP systems
- A05 - SAP Penetration Testing
- C01 - ABAP Code Security Assessment & Correction
- R01 - SAP Real-Time Monitoring & IDP
- R02 - SAP SIEM Integration
And many thanks to

– Eric Bushman <ebushman@paymetric.com> from Paymetric for the good input

– and my team
Q&A

Want more? Visit us at stand A10 to see cool SAP hacks

Ertunga Arsal
Email: ertunga@esnc.de

Brad Wilkinson
Email: brad@esnc.de