SAP MOBILE: ATTACK & DEFENSE

Julian Rapisardi
jrapisardi@onapsis.com

Fernando Russ
fruss@onapsis.com
This presentation contains references to the products of SAP AG. SAP, R/3, xApps, xApp, SAP NetWeaver, Duet, PartnerEdge, ByDesign, SAP Business ByDesign, and other SAP products and services mentioned herein are trademarks or registered trademarks of SAP AG in Germany and in several other countries all over the world.

Business Objects and the Business Objects logo, BusinessObjects, Crystal Reports, Crystal Decisions, Web Intelligence, Xcelsius and other Business Objects products and services mentioned herein are trademarks or registered trademarks of Business Objects in the United States and/or other countries.

SAP AG is neither the author nor the publisher of this publication and is not responsible for its content, and SAP Group shall not be liable for errors or omissions with respect to the materials.
Onapsis Inc. Overview

Company mission is to secure business-critical applications.

Transforming how organizations protect the applications that manage their business-critical processes and information.

- **Founded:** 2009
- **Locations:** Buenos Aires, AR | Boston, MA | Munich, DE | Lyon, FR
- **Research:** 200+ SAP security advisories and presentations published
- **What does Onapsis do?**
  - Innovative business-critical applications security software
  - Trainings and presentations on business-critical infrastructure security
Who are we?

- Julian Rapisardi  
  **SAP Security Specialist @ Onapsis**
  - Background on SAP Security Assessments
  - Has been involved in several SAP GRC projects

- Fernando Russ  
  **Senior Researcher @ Onapsis**
  - Background on Penetration Testing and Vulnerabilities Research
  - Reported vulnerabilities in different SAP and Oracle Products

- Both Authors/Contributors on diverse posts and publications
- Speakers and Trainers at Information Security Conferences
Agenda

- Introduction
  - Context
  - History

- SAP Mobile
  - SMP (SAP Mobile Platform)
  - SAP Fiori

- Attack surface
- Architecture Overview
- Security challenges while building our application

- Conclusions
Introduction
Introduction

So...what is SAP?

**SAP** *(Systems, Applications and Products in Data Processing)* is a German company devoted to the development of business solutions.

- Founded in 1972
- 75,000 employees
- More than 291,000 customers in 190 countries
- *Working with Global Fortune-500 companies and large governmental organizations*
SAP systems store and process the most critical business information. If the SAP platform is breached, an intruder would be able to perform:

**ESPIONAGE**

Obtain customers/vendors/human resources data, financial planning information, balances, profits, sales information, manufacturing recipes, etc.

**SABOTAGE**

Paralyze the operation of the organization by shutting down the SAP system, disrupting interfaces with other systems and deleting critical information, etc.

**FRAUD**

Modify financial information, tamper sales and purchase orders, create new vendors, modify vendor bank account numbers, etc.
As part of the industry's push towards remotely accessible business functions, SAP has been evolving their business critical applications to this trend.

Going mobile brings some security challenges, such as:

- Choosing adequate authentication mechanisms
- Securing communications
- Defining proper data encryption requirements
**SAP Mobile Platforms** have travelled several miles in SAP history.

<table>
<thead>
<tr>
<th>2010</th>
<th>2011</th>
<th>2012</th>
<th>2013</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Sybase</strong></td>
<td><strong>OData</strong></td>
<td><strong>Syclo</strong></td>
<td><strong>SAP Mobile Platform Cloud Edition</strong></td>
<td><strong>SAP Mobile Platform 3.0 (SMP3)</strong></td>
</tr>
<tr>
<td><em>An SAP Company</em></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><em>SAP buys Sybase</em></td>
<td><em>Sybase Unwired Platform (SUP)</em></td>
<td><em>SAP buys Syclo</em></td>
<td><em>(SMP3) unifies SUP, Syclo Agentry and SAP's mobile technologies into one mobile platform.</em></td>
<td></td>
</tr>
<tr>
<td>Sybase is SAP's largest acquisition ever.</td>
<td>Supports integration with SAP NetWeaver Gateway via OData.</td>
<td>Syclo’s Agentry, another mobile product (supporting Online and Offline Capabilities). <em>Mobile Analytics Kit</em></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

© 2015 Onapsis, Inc. All Rights Reserved
SAP Mobile
SAP Mobile


64 apps
(just for Android)
SAP’s mobile enterprise solutions are various. Most used ones today are SAP Fiori and SAP Mobile Platform (SMP).

**SAP Fiori** is a collection of pre-built mobile applications, delivered via the SAP Store.

**SMP** is used to build and deploy mobile applications across a range of mobile devices. It is a middleware platform, which enables users to connect the existing enterprise systems or applications with the mobile devices.

Let’s get a deeper look at them..
SAP Fiori is a collection of apps for frequently used SAP functions (Finance, HR, Sales & Marketing, Procurement, Manufacturing, Supply Chain etc.) that work across devices – desktop, tablet, or smartphone.

SAP Fiori landscape includes:
- SAP backend systems
- SAP NetWeaver Gateway
- SAP UI5 (UI development toolkit for HTML5) for NetWeaver

No mobile platform is required
Sybase Unwired Platform and the Syclo Agentry development platform have been integrated, and the product rebranded to SAP Mobile Platform (SMP).

SMP landscape includes:

**SAP backend systems**
- SAP ERP (Enterprise Resource Planning)
- SAP CRM (Customer Relationship Management)
- SAP SCM (Supply Chain Management)
- SAP SRM (Supplier Relationship Management)

*NetWeaver Gateway* for providing interfaces to business logic

*SMP* to store and pass data between NetWeaver Gateway and mobile devices

*Afaria* assists managing and securing mobile devices, across platforms.
Attack surface
The App lets you browse the bookings of a series of airline carriers, based on the flight connection available in certain periods of time. (as enhancement is planned to show the receipt as a Fiori plug in).

- **Rotten by design™ :)**
- Implemented using...
  - Apache Cordova 4.3.0 + Kapsel (using SMP 3.0 SP08)
  - SAP Fiori Wave 1 SP02
  - SAP Netweaver Gateway (SAP EHP 2 for SAP NetWeaver 7.0)
  - SAP IDES (EHP6 FOR SAP ERP 6.0)
Architecture Overview
Our Architecture

IDEs
Plug-ins

Consumer
Consumer
Consumer

Network Standards

SAP NetWeaver Gateway

Tools
- OData with SAP Annotations
- Generators (SOA/300/RF)
- Custom Dev.
- REST
- Metadata Repository
- Service Adaptation
- Events
- Supportability
- Monitoring
- Security
- Security

Data Source Providers
- BAPI
- RFC
- Dynpro

SAP NetWeaver

Reverse Proxy (Optional)

DMZ

Client

Mobile Device

Native Mobile Application

Web View

Network Interface

Native APIs

Device OS

Backend systems

© 2015 Onapsis, Inc. All Rights Reserved
Apache Cordova is a platform for building native mobile applications using HTML, CSS and JavaScript.

- Open source technology

- Supports ~ 15 Platforms
  - Android
  - IOS
  - Windows Phone
  - ...

https://cordova.apache.org/
Kapsel Framework

A serie of Apache Cordova plugins that enhance it allowing interactions with SAP

- Javascript + Native Code

<table>
<thead>
<tr>
<th>Plugin</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>AppUpdate</td>
<td>Push</td>
</tr>
<tr>
<td><strong>Logon</strong></td>
<td><strong>Encrypted Storage</strong></td>
</tr>
<tr>
<td>AuthProxy</td>
<td>Settings</td>
</tr>
<tr>
<td>Logger</td>
<td><strong>ClientHub</strong></td>
</tr>
</tbody>
</table>
Security challenges while building our application
1. Login mechanisms
1. Login mechanisms

▪ Anonymous Authentication
  ▪ No user/password needed
  ▪ No role mapping (generic users)
  
  Use for public content

▪ HTTP Basic Authentication
  ▪ Defined at RFC7235
  ▪ User and password in plaintext (base64 encoded)
  
  Without using SSL / TLS this method is totally useless
1. Login mechanisms

- **Token-based Authentication**
  - Uses SAP Single Sign-On tokens
  - In general it is used as an opaque value (as an HTTP Header)

  Using SSL/TLS helps avoiding security issues

- **Certificate-based Authentication**
  - Uses X.509 certificates
  - Mutual authentication is assured

  Not frequently used, due to it’s complicated configuration
2. Securing data in transit

SAP NetWeaver Gateway

IDEs

Tools

Generators

Custom Dev.

REST

Metadata Repository

Events

Supportability

Monitoring

Security

Data Source Providers

BAPI

RFC

Dynpro

SAP Business Suite

Backend systems
2. Securing data in transit

- Use HTTPS as communication channel
- ..or a VPN network (or per app vpn)

- It MUST be used for every requested resource
- DON´T use Self Signed Certificates or suppress TLS error messages

- Using Mutual Authentication is highly recommended
2. Securing data in transit

Stay tuned with security updates related on securing communications.

Notable SSL / TLS vulnerabilities recently found:

- Heartbleed (CVE-2014-0160)
- SMACKTLS
  - FREAK (CVE-2015-0204)
  - SKIP-TLS (CVE-2015-0205, CVE-2014-6593, ...)
- LogJam (CVE-2015-4000)
  
  Also affects some VPN implementations
3. Securing data at rest
3. Securing data at rest

▪ Defining the proper data encryption requirements
  ▪ Avoid custom "obfuscation"/encryption techniques

▪ **DON´T EVER** use hardcoded cryptographic keys in the app
  ▪ Use the System Keyring if available
  ▪ Use SAP ClientHub or similar

▪ Kapsel provides a plugin: **EncryptedStorage**
  ▪ Sqlite / AES256
  ▪ API based on the W3C Web Storage proposal
  ▪ Or use SQLCipher...(https://www.zetetic.net/sqlcipher/)
## 4. Patch Management

<table>
<thead>
<tr>
<th>Component</th>
<th>SAP Note</th>
<th>Short Title</th>
<th>Release Date</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SAP Afaria</strong></td>
<td>2153690</td>
<td>Multiple vulnerabilities in SAP Afaria Server</td>
<td>12.05.2015</td>
</tr>
<tr>
<td></td>
<td>2155690</td>
<td>Missing authentication check in SAP Afaria</td>
<td>12.05.2015</td>
</tr>
<tr>
<td></td>
<td>2132584</td>
<td>Buffer overflow in SAP Afaria 7 XcListener</td>
<td>10.03.2015</td>
</tr>
<tr>
<td><strong>Apache Cordova</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2116121</td>
<td>Hybrid Web Container 2.3.4.7320 vulnerable to XAS attack</td>
<td>10.03.2015</td>
</tr>
<tr>
<td><strong>SAP Mobile Platform</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2125513</td>
<td>XXE vulnerability in SAP Mobile Platform</td>
<td>10.03.2015</td>
</tr>
<tr>
<td></td>
<td>2114316</td>
<td>Unauthorized use of application functions in SMP 3.0</td>
<td>10.02.2015</td>
</tr>
<tr>
<td></td>
<td>2125358</td>
<td>SAP Mobile Platform XXE vulnerability</td>
<td>10.02.2015</td>
</tr>
<tr>
<td><strong>Sybase Unwired Platform</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2094830</td>
<td>Potential information disclosure relating to mobile onboarding</td>
<td>14.04.2015</td>
</tr>
<tr>
<td><strong>Agentry</strong></td>
<td>2036547</td>
<td>Security mitigation instructions for Agentry 6.1.3</td>
<td>09.09.2014</td>
</tr>
<tr>
<td></td>
<td>2105793</td>
<td>Fixing Poodle SSLv3 vulnerability for Agentry</td>
<td>09.12.2014</td>
</tr>
<tr>
<td></td>
<td>2038190</td>
<td>Potential information disclosure relating to the Agentry 6.1.3 iOS Client</td>
<td>09.12.2014</td>
</tr>
</tbody>
</table>
### 4. Patch Management

<table>
<thead>
<tr>
<th>Component</th>
<th>SAP Note</th>
<th>Short Title</th>
<th>Release Date</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SAP Afaria</strong></td>
<td>2153690</td>
<td>Multiple vulnerabilities in SAP Afaria Server</td>
<td>12.05.2015</td>
</tr>
<tr>
<td></td>
<td>2155690</td>
<td>Missing authentication check in SAP Afaria</td>
<td>12.05.2015</td>
</tr>
<tr>
<td></td>
<td>2132584</td>
<td>Buffer overflow in SAP Afaria 7 XcListener</td>
<td>10.03.2015</td>
</tr>
<tr>
<td><strong>Apache Cordova</strong></td>
<td>2116121</td>
<td>Hybrid Web Container 2.3.4.7320 vulnerable to XAS attack</td>
<td>10.03.2015</td>
</tr>
<tr>
<td><strong>SAP Mobile Platform</strong></td>
<td>2125513</td>
<td>XXE vulnerability in SAP Mobile Platform</td>
<td>10.03.2015</td>
</tr>
<tr>
<td></td>
<td>2114316</td>
<td>Unauthorized use of application functions in SMP 3.0</td>
<td>10.02.2015</td>
</tr>
<tr>
<td></td>
<td>2125358</td>
<td>SAP Mobile Platform XXE vulnerability</td>
<td>10.02.2015</td>
</tr>
<tr>
<td><strong>Sybase Unwired</strong></td>
<td>2094830</td>
<td>Potential information disclosure relating to mobile onboarding</td>
<td>14.04.2015</td>
</tr>
<tr>
<td><strong>Platform</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Agentry</strong></td>
<td>2036547</td>
<td>Security mitigation instructions for Agentry 6.1.3</td>
<td>09.09.2014</td>
</tr>
<tr>
<td></td>
<td>2105793</td>
<td>Fixing Poodle SSLv3 vulnerability for Agentry</td>
<td>09.12.2014</td>
</tr>
<tr>
<td></td>
<td>2038190</td>
<td>Potential information disclosure relating to the Agentry 6.1.3 iOS Client</td>
<td>09.12.2014</td>
</tr>
</tbody>
</table>
### 4. Patch Management

<table>
<thead>
<tr>
<th>Component</th>
<th>SAP Note</th>
<th>Short Title</th>
<th>Release Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP Afaria</td>
<td>2153690</td>
<td>Multiple vulnerabilities in SAP Afaria Server</td>
<td>12.05.2015</td>
</tr>
<tr>
<td></td>
<td>2155690</td>
<td>Missing authentication check in SAP Afaria</td>
<td>12.05.2015</td>
</tr>
<tr>
<td>Apache Cordova</td>
<td>2116121</td>
<td>Hybrid Web Container 2.3.4.7320 vulnerable to XAS attack</td>
<td>10.03.2015</td>
</tr>
<tr>
<td>SAP Mobile Platform</td>
<td>2125513</td>
<td>XXE vulnerability in SAP Mobile Platform</td>
<td>10.03.2015</td>
</tr>
<tr>
<td></td>
<td>2114316</td>
<td>Unauthorized use of application functions in SMP 3.0</td>
<td>10.02.2015</td>
</tr>
<tr>
<td></td>
<td>2125358</td>
<td>SAP Mobile Platform XXE vulnerability</td>
<td>10.02.2015</td>
</tr>
<tr>
<td>Sybase Unwired Platform</td>
<td>2094830</td>
<td>Potential information disclosure relating to mobile onboarding (CVE-2015-3978)</td>
<td>14.04.2015</td>
</tr>
<tr>
<td>Agentry</td>
<td>2036547</td>
<td>Security mitigation instructions for Agentry 6.1.3</td>
<td>09.09.2014</td>
</tr>
<tr>
<td></td>
<td>2105793</td>
<td>Fixing Poodle SSLv3 vulnerability for Agentry</td>
<td>09.12.2014</td>
</tr>
<tr>
<td></td>
<td>2038190</td>
<td>Potential information disclosure relating to the Agentry 6.1.3 iOS Client</td>
<td>09.12.2014</td>
</tr>
</tbody>
</table>

- Since September 2010, security notes are released the 2nd Tuesday of every month (SAP Security Patch Day).
- The notes information is only accessible to SAP customers.
- Many security notes need to be applied manually.
- Only the implementation of some Security Notes can be automatically analyzed using the transaction RSECNOTE.
1. Login mechanisms

1. Securing data in transit

1. Securing data at rest

1. Patch Management
Conclusions
Conclusions

- Bring your own device (BYOD) is here to stay.
- Building mobile applications integrated with SAP is challenging itself.
  - SAP is a huge environment
  - Mobile devices are complex
  - Security is hard
- In our mobile devices our business critical data coexists with other usually suspect applications such as AngryBirds to Sudoku...
- Our business critical information is now being carried in many unsuspected places, such as pubs, nightclubs...
  - This is a user trend behaviour that will not change... at least for a while...
- In order to protect our business information, we need to protect ALL the systems and products within the landscape.
- Use the Secure Sockets Layer (SSL/TLS) protocol in the SAP NetWeaver Gateway host to secure communication in your landscape.
- Use Secure Network Communications (SNC) connections between the SAP NetWeaver Gateway host and the SAP systems.
- The security guidelines described in the SAP NetWeaver Security Guide also apply to SAP NetWeaver Gateway components (as they are based on the same topology).
Questions?

Julian Rapisardi
jrapisardi@onapsis.com

Fernando Russ
fruss@onapsis.com