Hiding the breadcrumbs:
Anti-forensics on SAP systems

Juan Perez-Etchegoyen
jppereze@onapsis.com

Will Vandevanter
wvandevanter@onapsis.com

March 2014
Troopers Security Conference
Disclaimer

This publication is copyright 2014 Onapsis, Inc. – All rights reserved.

This publication 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.
Who is Onapsis, Inc.?

- Company focused in **protecting ERP systems from cyber-attacks.**
  - SAP®, Siebel®, Oracle® E-Business Suite™, PeopleSoft®, JD Edwards® …
- Trusted by Global Fortune-100 and large governmental organizations.
- What does Onapsis do?
  - Innovative ERP security software (Onapsis X1, Onapsis Bizploit, Onapsis IA).
  - ERP security consulting services.
  - Trainings on business-critical infrastructure security.

Who are we?

- Juan Perez-Etcheogoyen, CTO at Onapsis.
- Will Vandevanter, Security Researcher at Onapsis.
Agenda

- Introduction
- Anti-Forensic techniques
- Conclusions

What should we expect out of this talk:

- Not a full anti-forensics guide.
- Shows several techniques taking advantage of current problems affecting logging mechanisms on SAP products.
- Follow-up of Troopers 2013 “SAP Forensics” talk.
- Hot an hour talk.
Introduction
What is SAP?

- **Largest** provider of **business management solutions** in the world.
  - Hundreds of thousands of implementations and customers located all over the world.

- Used by **Global Fortune-1000 companies**, **governmental organizations** and **defense agencies** to **run their every-day business processes**.
  - Such as Revenue / Production / Expenditure business cycles.

**FUNCTIONS**:
- Financial Planning
- Treasury
- Payroll
- Logistics
- Sales
- Invoicing
- Production
- Procurement
- Billing
Over 95% of the SAP systems we evaluated were exposed to espionage, sabotage and fraud attacks due to vulnerabilities in the SAP Application Layer.

Unlike SoD gaps, attackers do not need access credentials to exploit this kind of vulnerabilities...
SAP Forensics & The Anatomy of an Attack

- Several SAP components are shipped with out-of-the-box capabilities to register user and technical activities.

- While in the previous talk we analyzed the most important ones, in this talk we will focus on specific attacks that might completely bypass some logging/auditing mechanisms.

Anonymous attacker gains access / valid user 
elevates privileges

Attacker performs fraudulent business process /access info

High profile attacker hides 
trails of any activity
Forensics

- According to Wikipedia “Digital forensics (sometimes known as digital forensic science) is a branch of forensic science encompassing the recovery and investigation of material found in digital devices, often in relation to computer crime”.

- Through Forensics, we are looking for an answer to these questions:
  - Has my SAP platform been hacked?
  - Is it being attacked right now?
The Security Audit Log

The security audit log can record the following security-related information:

- Dialog Logon attempts (successful and unsuccessful).
- RFC Logon attempts (successful and unsuccessful).
- Remote Function Calls.
- Transactions start attempts (successful and unsuccessful).
- Report start attempts (successful and unsuccessful).
- Changes to user master records.
- Changes to the auditing configuration.
SAL - Event Processing and Record Structure

- The audit log uses filters.
- Every time an event occurs, it is checked against defined filters.
- If it matches, a log record is written to the audit file.
- The log record has the following structure:
  - **Event identifier.**
  - SAP User ID and client.
  - **Terminal Name.**
  - Report Name.
  - Time and date.
  - Process ID.
  - Session Number.
  - Other information.
  - **Token:** 2685-8765-2432-1790-3141
Abusing of Security Audit Log
Attack #1 – Delete SAL messages

- Security Audit Log Events are shown through TX SM20
- The template messages are stored in table TSL1D
- User with only TCODE authorizations to SE92 can delete messages!
- This results in SAL events not being shown anymore (even though these are triggered).
- SAP Released Security Note 1926485 to fix this issue.

Any low-privileged user could delete SAL messages resulting in those messages not being unavailable for all users

Impact: Complete anonymity on any attack.
### Attack #1 – Delete SAL messages

The table below illustrates the Data Browser: Table TSL1D Select Entries. The specific entries highlighted are:

**USER** | **SUBID** | **CLASSID** | **SUBCLASSID** | **SEVERITY** | **MONBEW** | **MONKAT** | **TXT**
--- | --- | --- | --- | --- | --- | --- | ---
AU | 0 | X | 1 | 2 | GR | SH | Audit - Test, Text: &A
AU | 1 | X | 2 | 5 | YE | SH | Logon Successful (Type=&A)
AU | 2 | X | 2 | 9 | RE | SH | Logon Failed (Reason = BB, Type = &A)
AU | 3 | X | 4 | 2 | GR | SH | Transaction &A Started
AU | 4 | X | 4 | 9 | RE | SH | Start of transaction &A failed (Reason=BB)
AU | 5 | X | 16 | 2 | GR | SH | RFC/CPIC Logon Successful (Type = &A)
AU | 6 | X | 16 | 9 | RE | SH | RFC/CPIC Logon Failed, Reason = &B, Type = &A
AU | 7 | X | 32 | 9 | RE | SH | User &A Created
AU | 8 | X | 32 | 9 | RE | SH | User &A Created
AU | A | X | 32 | 9 | RE | SH | User &A Created
AU | B | X | 32 | 9 | RE | SH | User &A Created
AU | C | X | 32 | 9 | RE | SH | User &A Created
AU | D | X | 32 | 9 | RE | SH | User &A Created
AU | E | X | 32 | 9 | RE | SH | User &A Created
AU | F | X | 32 | 9 | RE | SH | User &A Created
AU | G | X | 32 | 9 | RE | SH | User &A Created
AU | H | X | 32 | 9 | RE | SH | User &A Created
AU | I | X | 64 | 9 | RE | SH | Audit: Slot &A Inactive
AU | J | X | 64 | 9 | RE | SH | Audit: Active Status Set to &B
AU | K | X | 128 | 9 | RE | SH | Successful RFC Call &C (Function Group = &A)
AU | L | X | 128 | 9 | RE | SH | Failed RFC Call &C (Function Group = &A)
AU | M | X | 2 | 9 | RA | SH | User &B Locked in Client &A After Erroreneous Password Checks
AU | N | X | 2 | 9 | RE | SH | User &B in Client &A Unlocked After Being Locked Due to Invalid Password Entered
AU | O | X | 2 | 9 | RE | SH | User &B in Client &A Unlocked After Being Locked Due to Inval. Password Entered
AU | P | X | 2 | 5 | YE | SH | Transaction &A Unlocked
AU | Q | X | 4 | 5 | YE | SH | Transaction &A Locked
AU | R | X | 32 | 5 | YE | SH | &A &B Created
AU | S | X | 32 | 5 | YE | SH | &A &B Deleted
AU | T | X | 32 | 5 | YE | SH | &A &B Changed
AU | U | X | 32 | 9 | RE | SH | &A &B Activated
AU | V | X | 1 | 9 | RE | TP | Digital Signature Error (Reason = &A, ID = &B)
Attack #1 – Delete SAL messages

Protection / Countermeasure

- Implement SAP Security Note 1926485 (December 2013)
- Restrict S_DEVELOP authorization as those users could still delete messages.
Attack #2 – Hide source of attack

- Security Audit Log Events have a unique field for the source.
- By default the SAP App. Server makes a best effort to add the terminal name, but if not possible, then adds the IP address.
- Terminal name is data provided by the client!
- An IP address could be provided instead.
- Profile parameter rsau/ip_only is the only restriction for this attack (default value disabled)

The source for any (un)authenticated connection in the Security Audit Log cannot be trusted.

Impact: Complete anonymity on the source of the attack.
Attack #2 – Hide source of attack
Protection / Countermeasure

- Enable profile parameter `rsau/ip_only`
- Follow recommendations detailed in SAP Note 1497445
Attack #3 – Reaching the limit

- Limits are defined for the security audit log. By default no more than 100M of logs can be saved per day.
- Default behavior if the maximum size is reached is to stop logging!
- Some events can be triggered remotely and unauthenticated.
- If attacker knows what is being logged could potentially turn it off.

An unauthenticated user could disable the SAL if not properly sized by triggering events.

Impact: Complete anonymity on any attack.
Anti-Forensics on SAP systems

Attack #3 – Reaching the limit
Protection / Countermeasure

- Perform a proper sizing of the Security Audit Log requirements to reduce the risk of reaching size limits.
- Send the alerts to an external source, potentially through CCMS.
Attack #4 – SAP BO Temporary audit

NOTE: The Auditor and Auditee can also co-exist on the same CMS server.
Attack #4 – SAP BO Temporary audit

- BO architecture is distributed and by design there is a gap between when an event occurs and when it is written to the ADS.
- This provides an attacker the opportunity to modify the event and hide actions.
- No Integrity Check on the Temporary Files.

Any user with filesystem access could delete temporary logs before reaching the ADS.

Impact: Complete anonymity on any attack.
Attack #4 – SAP BO Temporary audit

- BO architecture is distributed and by design there is a gap between when an event occurs and when it is written to the ADS.
- This provides an attacker the opportunity to modify the event and hide actions.

**Protection / Countermeasure**

- Protect Temporary Files at the OS level
- Correlate Events to detect anomalies

Any user with filesystem access could delete temporary logs before reaching the ADS.

Impact: Complete anonymity on any attack.
Locations
# SAP Log and traces - Location

<table>
<thead>
<tr>
<th>Logging mechanism</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Audit Log</td>
<td><code>/usr/sap/&lt;SID&gt;/&lt;INSTANCE&gt;/log/audit_date</code></td>
</tr>
<tr>
<td>Developer traces</td>
<td>Directory: <code>/usr/sap/&lt;SID&gt;/&lt;INSTANCE&gt;/work/dev_*</code></td>
</tr>
<tr>
<td>System Log</td>
<td><code>/usr/sap/&lt;SID&gt;/&lt;INSTANCE&gt;/log/SLOG&lt;SYSNR&gt;</code></td>
</tr>
<tr>
<td>SQL Audit</td>
<td><code>/usr/sap/&lt;SID&gt;/&lt;INSTANCE&gt;/log/SQL_+++++++.AUD</code></td>
</tr>
<tr>
<td>System Trace</td>
<td><code>/usr/sap/&lt;SID&gt;/&lt;INSTANCE&gt;/log/TRACE</code></td>
</tr>
<tr>
<td>Gateway Log</td>
<td><code>/usr/sap/&lt;SID&gt;/&lt;INSTANCE&gt;/work/&lt;file_name&gt;</code></td>
</tr>
<tr>
<td></td>
<td><code>&lt;file_name&gt;</code> is defined by key LOGFILE</td>
</tr>
<tr>
<td>Web Dispatcher Log</td>
<td>Specified by parameter <code>icm/HTTP/logging_XX</code></td>
</tr>
<tr>
<td>WD Security Log</td>
<td><code>/usr/sap/&lt;SID&gt;/&lt;INSTANCE&gt;/work/dev_icm_sec</code></td>
</tr>
<tr>
<td>Table Change Logging</td>
<td>Table DBTABLOG</td>
</tr>
<tr>
<td>User &amp; Auth.</td>
<td>Tables USH02, USH04, USH10, USH12...</td>
</tr>
<tr>
<td>ABAP Change Doc.</td>
<td>Tables CDHDR, CDPOS</td>
</tr>
</tbody>
</table>
General recommendations

• Enable logging and tracing mechanisms according to business requirements
• Enable technical logs too.
• Send the logs to a centralized facility
• Periodically review all logs
• Implement SAP Security Notes on all SAP systems to mitigate the risk of new vulnerabilities, specially the ones affecting the audit and logging mechanisms.
• Secure the profile parameters and the configuration of the SAP systems.
• Perform a proper sizing of the logging and tracing mechanisms to avoid reaching the defined limits.
Conclusions

● It is important to understand the limitations and features of each logging and tracing mechanism to ensure we are logging the necessary information.

● If an attacker gets SAP_ALL or equivalent privileges and the logs were not sent to an external system, then no auditing or logging feature is reliable.

● If it is already difficult to know whether an SAP platform has been compromised, not PROPERLY recording user and technical activities makes it impossible.
References

● SAP Note 539404 - FAQ: Answers to questions about the Sec. Audit Log
● SAP Note 1497445 - SAL| Logging the IP instead of the terminal name
● SAP Security Note 1926485 - Missing authorization check in application
"Edit System Log and Security Audit Log Messages"

● http://scn.sap.com/thread/3298688
● Troopers 2013 – “Detecting white-collar cybercrime: SAP Forensics”
● http://www.onapsis.com

● Special Thanks to the Onapsis Team:
  ● Sergio Abraham
  ● Nahuel Sanchez
  ● Alex Horan
Questions?

jppereze@onapsis.com
wvandevanter@onapsis.com
Thank you!

www.onapsis.com

Follow us! @onapsis