SAPtips
www.SAPtips.com
SAPtips
February 2003 Volume I Issue 1

SAPtips

SAP® Security: A Framework for Successful Implementation

By Joey Hirao, Jotech LLC

Editor's note: In today's SAP environment, security is not about locking the door behind us. It's about developing and implementing an overall strategy that protects the system from misuse and provides the right level of access to the right users. SAP provides a high level of security functionality, but it's up to us to put it to work. To get us on the right track, Basis Editor Joey Hirao has developed a step-by-step guide to the proper implementation of SAP security. This article is a great outline for those who are mounting or revamping their SAP security strategy, but it will also be of interest to those readers who are already up and running and want to compare their own installation to Joey's "best security practices."

Purpose

Security is an integral part of all SAP implementations. However, the importance of security is often overshadowed by the business functionality and process improvement the SAP implementation intends to achieve. Security is most likely not the reason why an organization implements SAP, but a poorly designed and implemented security model will become the Achilles heel - to the overall success of software delivery. This document will describe a framework for a successful implementation of SAP security during the course of the SAP implementation.

Overview

Security in itself is not necessarily an independent action within an implementation. In reality, during the course of developing the business requirements and parameters for the SAP software, the actual role and function of security are formulated. Security becomes an effective and useable function only when the business requirements, existing security rules, and internal controls are merged to form a comprehensive SAP security strategy. Under this model, security definition becomes a definitive deliverable in conjunction with defining how SAP will function within the organization. The next section illustrates an SAP security implementation plan. It summarizes the deliverables as well as the detailed tasks required for implementation. This is a generic model that can be adapted to fit within the various SAP implementation methodologies developed by SAP and other implementation partners. The specific procedures covered in this document come from an SAP 4.6C system.

A poorly designed and implemented security model will become the Achilles heel to the overall success of software delivery

The outline below captures, in chronological order, the key milestones for a security implementation, separated into generic security tasks and specific tasks associated with roles creation.

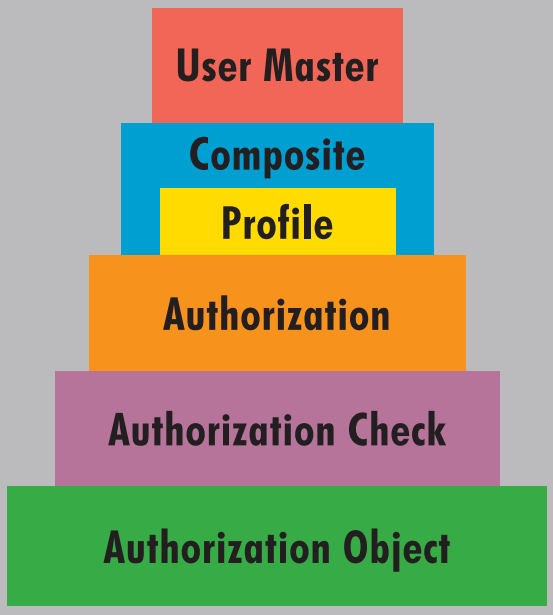
1. First Steps
   - Activate Profile Generator
   - Secure SAP system
   - Define security policy
     - Password rules
     - Session rules
     - Logging rules
     - User termination rules
     - User id naming convention
     - Role naming convention
     - Profile naming convention
     - Output device naming convention
   - Define rules for securing custom objects
   - Define standard for batch users
   - Identify process for modifying security roles and users
   - Define periodic audit requirements and tasks for security
   - Define periodic security jobs

2. User roles
   - Named user identification
   - Roles definition
   - Roles creation
   - Role testing
   - Role delivery

SAP Security continued on page 2

SAP Security continued from page 3

Security Detail



- A user in SAP is granted a profile (single profile or composite profile.
- A profile consists of authorizations. A composite profile consist(s) of profile(s). When security is created using Profile Generator, these objects are referred to as Activity groups or Roles.
- When an SAP process is executed, the underlying ABAP code may invoke an authorization check on an authorization object.
- If the proper authorization is assigned to the profile, the check is successful and the ABAP code continues. Otherwise the check fails.
- SAP security is based on positive checks and not on negative ones.

Figure 1. SAP Security Model

1. First Steps

1a. Activate Profile Generator
After the SAP system is installed, a task performed by the Basis administrators, the security team needs to activate the Profile Generator. The Profile Generator is a front-end tool security tool. Prior to SAP R/3 3.1G, all SAP security was performed without the aid of the Profile Generator. The concepts of SAP security are the same, with or without Profile Generator; Profile Generator simply serves as a user-friendly interface to facilitate security administration. Profile Generator has evolved since its debut and has many objects such as tables and structure specific to itself. Figure 1 provides an overview to the basics of SAP security.

Profile Generator is activated following these steps:

1. Set SAP instance parameter auth/no_check_in_some_cases = Y
   a. Instance parameters are often changed and controlled by the Basis administrator. Instance parameters are changed via transaction RZ10. Use caution when making any instance parameter changes. These parameters are one of the critical components to the SAP Basis subsystem.
2. Execute transaction SU25 and perform the following tasks:
   a. Copy the SAP check indicator and field values (Step 1 in SU25)
   b. Adjust the check indicators for transaction codes (optional) (Step 4 in SU25)
   c. Deactivate, if necessary, authorizations objects (optional) (Step 5 in SU25)

SAP Security continued on page 3

SAPtips

SAP Security continued on page 2

1. First Steps cont.

1b. Secure SAP system

SAP comes delivered with standard passwords for special super users. In order to secure the installation, these passwords need to be changed. Beware, standard passwords are readily documented, and it will be one of the first holes a hacker will try to exploit.

a. Change default passwords. Run standard report RSUSR003 to check the current status of the passwords.
b. Change passwords for database users
c. Implement password rules as described in section 1.c
d. Implement session rules as described in section 1.c

1c. Define security policy

Obtain the current security policy and identify if any existing rules can be applied to SAP. The following rules and conventions need to be addressed:

1. Password rules
2. Session rules
3. Logging rules
4. User termination rules
5. User id naming convention
6. Role naming convention
7. Profile naming convention
8. Output device naming convention

1. First Steps cont.

The implementation of these requirements is described below:

1. Password rules
   a. The following instance parameter control password rules
      i. login/min_password_lng = 8
         Sets the minimum password length
      ii. login/password_expiraton_time = 90
         Set the expiration time for passwords

2. Session rules
   a. The following instance parameter control session rules
      i. login/disable_multi_gui_login = 1
         Disable multiple dialog logons
      ii. rdisp/gui_clean_delay = 0
      iii. login/multi_login_users = JOEYH
         List of users who can have multiple sessions
      iv. login/fails_to_session_end = 3
         Number of invalid logon attempts until session is terminated
      v. login/fails_to_user_lock = 6
         Number of invalid logon attempts until user is locked. Lock is released at midnight
      vi. login/failed_user_auto_unlock = 0
         User is not unlocked if invalid attempts were made in previous days
      vii. rdisp/gui_auto_logout = 3600
         Time in seconds when session is terminated after inactivity

3. Logging rules
   a. The implementation of AIS allows for detailed security logging
   b. Otherwise the following security items are logged in SAP:
      i. Last logon/logoff
      ii. Password changes
      iii. User metadata changes (Example: Address, password, default settings)
      iv. Profile changes

4. User termination rules
   a. How to delete users from the system
      i. Establish procedure to purge users (Example: Lock user then delete after 30 days)
      ii. This policy also helps keep the installation in line with contractual obligations with SAP. SAP periodically requests user audits to ensure license compliance.

5. User id naming convention
   a. Identify user id naming convention. The maximum is 12 characters.
   b. Some example are below
      i. Last + First + Initial
         First Name = John, Last Name = Smith, Middle Initial = A, Username = SMITHJA)

6. Role naming convention
   a. Roles are identified by a name and a description. All roles should follow a similar standard.

7. Profile naming convention
   a. Profiles also have a name and a description. Roles generate profiles. When roles are first saved, SAP assigns it a generated name. In lieu of the generated name, security should utilize a naming convention. (Example: Role name = HQ:INV_MGR, Profile = HQ:INV_MGR)

8. Output device naming convention
   a. The Basis team, in conjunction with legacy application administration personnel, produce the names for output devices. Output devices are usually limited to printers and FAX devices. The importance of a naming convention comes into play when dealing with secure devices. Examples of secure devices include production check printers and pick printers. When there is a logical naming convention for output devices, it facilitates the securing process. For example, all un-secure printers lie in the alphabetical range of A* and all secure printers lie in the range of S*. This allows the security administrator to identify these printers easily when building the security roles.

SAP Security continued on page 4

SAPtips

SAP Security continued from page 3

1. First Steps cont.

1d. Define rules for securing custom objects
SAP comes delivered with thousands of standard objects such as reports and tables, however it usually does not meet the need for all customers. Ergo, custom objects are often created. Establishing a standard early during the implementation will help avoid unnecessary rework later.

Example: Define all custom tables in specific authorization groups. If not explicitly defined, the tables become part of a default authorization group. Changes to this require additional planning and effort.

1e. Define standard for batch users
SAP batch jobs are scheduled and executed by a specific named user within the system. A special named user should be created to execute periodic batch jobs. One reason for this technique: prevent jobs from failing after a user is purged from the system and standardize job queries.

Example: Create a standard Human Resource (HR) user HRBATCH. HRBATCH schedules and executes daily a job that sends timesheet data to an external interface. The batch administrator performs a search in SAP for jobs by username HRBATCH.

1f. Identify process for modifying security roles and users
This process becomes the process in which all security related changes are identified and implemented. A change control process ensures due process prior to implementing a change. The security change control process should answer the following questions.

1. Who can request a change to an existing profile/user id
2. Who is the approving person(s) for this change
3. Who is responsible for implementing the change
4. How is the change documented and archived

1g. Define periodic audit requirements and tasks for security
In organizations with internal audit departments (IAD), audit parameters such as frequency and extent will be defined by IAD. The IAD will develop an audit plan and perform substantive tests in order to validate and test internal checks and controls. During audits, the security team's job is to educate and assist IAD. Some organizations also contract external auditors to perform functions similar to IAD. During an implementation, the security team will work with IAD or external auditors to help develop an SAP security audit plan.

Aside from external reviews, the security team should perform periodic checks itself. The frequency depends on resource availability and magnitude of the implementation. The following list describes items to check:

1. Default SAP passwords
2. Never logged in users
3. Obsolete users
4. Critical authorization holders
5. Completeness, accuracy of user records
6. Monitor locked users and frequency of locked users

1h. Define periodic security jobs
The following list describes a couple security jobs that should run periodically:

1. Schedule PFCG_TIME_DEPENDENCY via transaction PFUD. Create a variant for this job. This job will compare profiles with the corresponding roles in the user master record.
2. Schedule program SAPPROFC_NEW. Create a variant for this job. This job performs a generation of required profiles.

2. User Roles

End-user roles and project team roles are different, but they go through a similar creation process. The following list describes the different phases for role creation and deployment. It also highlights the specific tasks for project team and end-user role creation and deployment.

2a. Named user identification:
Information obtained about a named user will be used to populate the different fields associated with that user in the SAP system. Most fields other than user name are optional. The important aspect of user information is consistency and completeness. Insist on this. Gather your requirements by identifying any and all required fields for your installation:

1. User name (system mandatory)
2. First name (optional)
3. Last name (optional)
4. Location (optional)
5. Telephone number (optional)
6. Default output device (optional)
7. Default number format (optional)
8. Default date format (optional)
9. SAP parameters (optional)

SAP Security continued on page 5

SAP Security continued from page 4

2. User Roles cont.

End-user roles and project team roles are different, but they go through a similar creation process. The following list describes the different phases for role creation and deployment. It also highlights the specific tasks for project team and end-user role creation and deployment.

2b. Roles definition

This aspect of security is probably one of the most important. In this step, the look and feel of security is defined. This task should be given particular attention. Not only will roles definition affect what types of access users have, but it will also define what the actual roles will look like. The roles can take the shape of derived, composite, and/or single roles. A single role is straightforward, since it contains no dependency with other roles. It is a role within itself. Composite roles are more complex - these are roles within roles. Composite roles are difficult to maintain and understand, since they can contain many dependencies on other roles. Use composite roles with caution. Derived roles (children) are roles based off one template role (parent). The children inherit all the qualities of the parent, except the organization- specific data. Derived roles are useful when different organizational roles all share the same security requirements.

a. Project team roles are customarily defined by the security administrator and with project management. The following questions will help decide on the actual project team security requirements:
   i. Separate user by functional module?
   ii. Separate developer and functional users?
   iii. Who can possess SAP_ALL?
   iv. Deny access to Basis transaction to users?
   v. Deny security access to members other than security?
   vi. What are the different roles in the client deployment strategy?
   vii. Who has access to OSS?
   viii. What access is granted in OSS?
b. End-user roles requirements are based on a business blueprint. This blueprint defines the business processes to be implemented with SAP. In addition to business processes, security requirements are also explicitly defined. Based on these requirements, the security team works with business process owners to get more specific data necessary to create the security roles.

2c. Roles creation

Role creation is a mechanical process within SAP. The security team creates roles based on the detailed requirements defined in Section 2, Role definition, and assigns it to user names. The success of this phase depends on the completeness and accuracy of data captured during role definition.

2d. Role testing

A fully integrated test is necessary prior to delivering the profile to the end user. Testing will reveal any overlooked details. Specific scenarios are necessary to test the roles. This allows for different test iterations to be comparable and consistent. The success of security is hinged on completing multiple iterations of testing prior to delivery. A technique utilized during many implementations is to perform security testing using actual end-user roles.

2e. Role delivery

Prior to delivery, the users need to be informed of their user names and initial passwords. This is often accomplished via an email or paper memo. In addition to the login information, the users need to be informed on the problem identification and resolution process.

Conclusions

This security implementation outline is intended to aid security team leads, as well as SAP project managers, during an SAP implementation. We've highlighted the important milestones and tasks that need to be included in the implementation project plan. Since all implementations are different, use this as a model to develop and plan your own security implementation. The concepts of planning and standards proliferate throughout this document. Standards and planning are important in any technical implementation; it is especially so with SAP. Since everything in SAP is so intertwined, undoing or redoing something after the fact can prove to be impossible or terribly painful. A little thought up front will save you loads of grief. As a wise man once told me, "Prior planning prevents piss-poor performance." Planning and consistent execution are the ingredients of a successful security implementation.

Joey Hirao, *Jotech LLC.* Joey is a Basis consultant with expertise in SAP Basis, UNIX, NT, and database technologies. He designs, implements and maintains SAP systems for customers worldwide. Joey has been working with SAP technology for the past six years. He is the founder of Jotech LLC, and the author of SAP R/3 Administration for Dummies. Joey is SAP Basis certified, Solaris Administrator certified, and a MCSE. Joey can be reached at **Joey.Hirao@SAPtips.com.**

SAP Security continued on page 6

SAPtips

SAP Security continued from page 5