# Is It Time to Revisit Your SAP Security Infrastructure?

José A. Hernández

*José A. Hernández is Assistant Managing Director at realTech, an SAP partner and technical IT consulting firm specializing in R/3, mySAP.com, e-commerce, and the development of Enterprise Resource Management software. José is also the author of "The SAP R/3 Handbook" and the "SAP R/3 Implementation Guide."*

*(complete bio appears on page 54)*

All of us who are involved in the setup and support of an SAP system recognize that leveraging security technology and exercising sound security measures and policies is an absolute must. The information stored in the systems we support ranks among a company's most important assets. Moreover, addressing security during and after an SAP implementation not only protects valuable business information, it ensures continuous and stable systems operations — activities that are vital to protecting a hard-earned brand name and dependable reputation. With that said, all too often I find that SAP implementation projects don't take security beyond the application level, where security and authorization are often regarded as one and the same.

At the application level, the authorization concept (user masters, profiles, etc.) is undeniably key to securing access to proprietary transactions and data. You'll get no argument from me that a sound authorization strategy is of paramount importance to overall SAP security. But a sound security strategy can't start and stop there. To ensure adequate protection against unauthorized access by internal and external users, security measures must be factored into all layers of the SAP infrastructure:

- Presentation
- Transport system
- Operating system
- Remote communications
- Internet
- Application
- Database
- Network
- Document transfer

If you have any doubts as to whether or not revisiting your SAP infrastructure security is worth your while, take this short test and see how well your SAP systems security now fares:

✔ Launch your SAP GUI, enter “066” as client, “EARLYWATCH” as username, and “SUPPORT” as password. Were you able to log in? If you could *not* log in, give yourself a passing grade for this first test question. Your inability to log in means that either you have successfully changed one of the known passwords (SUPPORT) of a standard SAP username (EARLYWATCH), or you have locked this username. If you *were* able to log in, give yourself a failing grade for this question. Logging in under these conditions means that one of the basic security measures at the presentation and application level was not performed, and therefore any person with access to this SAP system can log in using this known username, which, while not a full-privileged one, has enough authorizations to perform certain functions that could be considered risky.

✔ Walk over to a colleague’s workspace and try to run the SAP GUI from that person’s PC. Could you do it? If you could *not* run the SAP GUI, you pass this test question. Your inability to run the SAP GUI means that your colleague had basic security measures — something as simple as having a password-protected PC or screen saver — implemented at the presentation level. If, on the other hand, you or anyone can freely access the applications installed on any PC, it means that someone could use this gateway for unwanted actions, or even fake the origin of a security attack.

✔ Do you use SAP shortcuts to quickly access the most frequently used transactions or reports? When you create a shortcut, does it allow you to store the password? If it does not, run the **REGEDIT** (Registry Editor) program, search for the key “HKEY_CLASSES_ROOT\ Sapgui.Shortcut.File\ Security”, and set **EnablePassword** to a value of “1”. Exit the Registry Editor and try again to create a shortcut. Now can you create a shortcut with the password stored in the definition? If you initially were not able to create a shortcut with a stored password, or you were unable to edit the registry at your Windows workstation, give yourself a passing grade. However, if you were able to store the password in the shortcut or edit the registry, then your workstation may not be correctly protected, and you may have a security problem at the presentation level.

✔ If you are an R/3 user that has either SAP_ALL or S_A.SYSTEM privileges, run report **RSUSR009** using standard transaction SE38 or SA38. This report can help security or system managers discover users with so-called “critical authorizations”. You may be surprised to learn just how many people have access rights to critical authorizations. If you find too many individuals who have been granted these privileges, or discover some surprising or suspect listings as the result of this report, it means security measures at the application level have not been completely implemented.

✔ Log in at the operating system level as user “<sid>adm”. If your database is Oracle, run **svrmgrl** (on UNIX systems) or **svrmgr30** (on Windows NT). At the prompt enter “connect internal”. Alternatively, try to connect as user “SAPR3” with password “SAP” (“connect SAPR3/SAP”). Were you able to connect? Who else can do this? In other words: Do many people know the privileged username and password at the operating system or database level? If this is the case, you may have a serious security problem because standard usernames and passwords of Oracle and other database engines are well known, and accessing the database at this level leaves your system highly exposed to the threat of deleting objects, extracting confidential information, or leaving a database in an inconsistent state.

✔ From an SAP session, run program **RSUSR006** (the ABAP report that shows unsuccessful logon attempts). Do you notice any login attempts that were denied? Many entries on this report are the result of users making typing mistakes, which is normal and expected. However, if you discover unexpected users with incorrect logon attempts, your systems might have been intentionally attacked. This report is included within the basic set of monitoring and security auditing tools. If you don't use this and/or similar reports regularly, give yourself a failing grade here.

✔ Copy one of your regular R/3 users (like a financial clerk or a warehouse operator) to a test user. Log in as this test user. Can you run transactions STMS, SA38, PFCG, and SU01? If you can run these or similar transactions as a regular user, you have a security breach at the application level, since regular users should not normally be allowed to perform operations that are meant to be performed by Basis administrators and/or User administrators. If your regular users *cannot* execute these types of transactions, give yourself a passing grade — otherwise you have a serious security problem at the application level.

✔ Can regular users add or edit system entries when using SAPLOGON? If edit functionality is disabled, can users edit the SAPLOGON.INI file and change the key "NoEditFunctionality" to "0"? If this is possible and you work in a company with many SAP systems, give yourself a failing grade, because it means that users can freely add new groups or servers to their SAPLOGON, which might enable them to connect to unauthorized systems. If, on the other hand, you use SAPLOGONPad or have protected Edit Functionality, give yourself a passing grade.

✔ Log in to an R/3 system with a user ID that has a very simple "display only" profile (e.g., the profile S_A.SHOW). Then run transaction SE16 and enter "USR02" as the table name. Can you display this table? Can you download it (**System → List → Save → Local file***)*? If a user with a "display only" profile *can* display and download the table contents, give yourself a failing grade. USR02 is the table that contains master user logon data, and although not easy, it is possible for a technical expert with access to an SAP system to use this table for discovering (cracking) passwords. This means there is a security problem at the application and the presentation level.

✔ Did you ever look at transactions SM19, SM20 (Security Audit Log), or SECR (Audit Info System)? Maybe you don't even have them enabled. If you don't know about these and other similar transactions (like SUIM), give yourself a failing grade. These are core control and auditing transactions that can help you verify the status of your security. Security logging and auditing operates at every layer of a security infrastructure, and therefore is a basic mechanism to measure your infrastructure elements' compliance with a security policy.

Did you get any failing marks, or did you pass all the tasks with flying colors? Even if you got a perfect score, don't walk away just yet! I made this test very, very simple. Things like remote administration and debugging of ITS servers, password crackers, and network sniffers have not been factored into this list, not to mention network services and firewall configurations. Given their client/server architecture, SAP systems include many components that exchange information with both SAP and non-SAP components alike. Each of the elements needed for the communication and exchange of information constitutes a layer of the SAP security infrastructure.[1] Only with a comprehensive security plan that encompasses all tiers of the SAP infrastructure can you ensure that you set in place a security policy that protects the most valuable assets of your company from intentional or unintentional, and external or internal attacks.

In this article, I will introduce you to this multi-level notion of security and what you need to be mindful of when reviewing your overarching security measures, as well as the security measures you have in

[1] For a comprehensive listing of infrastructure security elements, refer to SAP's "R/3 Security Guide: Volume III" Security Checklists. This reference can be found at **http://service.sap.com/security** (you need a username and password to access this).

place (or lack thereof) to address each specific level.

Writing about security always requires a bit of soul searching. While SAP systems offer the innate security needed to create a secure system, customers do not always enact the appropriate measures. I had to ask myself, “Should I reveal the security holes that I’ve seen develop as a result of inadequate customer follow-through? Or should I avoid those discussions?” After careful consideration, I have decided that the more knowledge I can pass on to you, the better. Warning you ahead of time about certain risks will put you in a better position to protect your systems, data, and ultimately your business. Still, one must not be reckless! I’ve tempered certain remarks so that less advanced technical users cannot take advantage of procedures that could either intentionally or unintentionally damage your data or put your systems at risk. So, for instance, I have intentionally excluded an example of ABAP code to crack SAP passwords, although a password-cracker might be a good tool for ensuring that the efficacy of your password policy.

## The Multilayer SAP Security Infrastructure at a Glance

Take a moment to get acquainted with the various layers of the SAP security infrastructure shown in **Figure 1**. These layers must inter-operate to form a cohesive security strategy. That can’t happen unless you understand what each layer is supposed to do. So that’s what we’ll explore in the sections that follow.

### *Presentation-Level Security*

Presentation-level security addresses all forms of frontends used for accessing SAP systems. This has traditionally been the SAP GUI, but other options are

*Figure 1* *The SAP Security Infrastructure at a Glance*

| Layer | Components | Readily Available SAP Security Measures | Performed by… |
|---|---|---|---|
| Presentation | • GUI<br>• Frontend<br>• PC<br>• Web GUI<br>• Shortcuts<br>• mySAP.com Workplace<br>• Session Manager<br>• SAP Automation<br>• SAP MAPI Client<br>• Other developed user interfaces | • Access controls<br>• User authentication<br>• Profile parameters<br>• SNC<br>• Smart cards<br>• Single Sign-On<br>• Client certificates<br>• LDAP integration<br>• User Exits<br>• Security Audit Log<br>• CCMS Security Monitor<br>• Audit Info System (AIS) | • Basis administrator<br>• User administrator<br>• Security department<br>• IT department |
| Application | • Application modules<br>• Work processes<br>• Enqueue server<br>• Local developments | • Authorization system<br>• Profile Generator<br>• Predefined roles<br>• Access controls<br>• AUTHORITY-CHECK<br>• Security Audit Log<br>• CCMS Security Monitor<br>• Audit Info System (AIS)<br>• Object locks | • Authorization administrator<br>• User administrator<br>• Application administrator<br>• SAP developers (ABAP, BAPI, others) |

*(continued on next page)*

*Figure 1 (continued)*

| Layer | Components | Readily Available SAP Security Measures | Performed by… |
|---|---|---|---|
| Database | • Relational database<br>• Remote database connections<br>• Critical tables<br>• SAPDBA | • Access controls<br>• DB user authentication<br>• SAPDBA expert mode<br>• Backup<br>• Administration<br>• Database Audit | • Basis administrator<br>• DBAs<br>• OS administrator |
| Operating System | • UNIX, Linux<br>• Windows NT<br>• OS/400, OS/390<br>• External SAP commands | • Access controls<br>• User authentication<br>• Authorization system<br>• OS Monitors<br>• OS Logging and Auditing | • OS administrator<br>• Basis administrator |
| Network | • Network services<br>• Topology<br>• SAPNet<br>• Public access (Modem, RAS, others) | • Access controls<br>• SAProuter<br>• Routers<br>• Firewalls<br>• SNC<br>• Log Book | • Network administrator<br>• Basis administrator |
| Transport System | • System landscape<br>• Object transport | • Client concept<br>• TMS<br>• Workbench/Customizing Organizers<br>• SSCR<br>• Access controls | • Basis administrator<br>• Customizing users<br>• SAP developers |
| Remote Communications | • CPIC<br>• RFC<br>• ALE<br>• BAPIs<br>• Trusted systems<br>• OLE<br>• Remote printing | • SAProuter<br>• SNC<br>• Access controls<br>• Authorization system<br>• Gateway Monitor | • Network administrator<br>• Basis administrator<br>• SAP developers |
| Document Transfer | • Electronic mail<br>• Media exchange<br>• Document management<br>• Application modules | • Public-key infrastructure[2]<br>• SSF<br>• Smart cards<br>• Digital signatures<br>• Digital envelopes<br>• SAP Security Library<br>• Trust centers | • Security department<br>• Legal department<br>• Basis administrator |
| Internet | • Web browsers<br>• Web servers<br>• ITS<br>• mySAP.com Workplace | • Access controls<br>• SNC<br>• Firewalls<br>• HTTPS<br>• SAProuter<br>• Client certificates (X.509)<br>• Single Sign-On<br>• Trust centers | • Web administrator<br>• Network administrator<br>• Basis administrator |

[2] With the evolution of backend business applications (classical SAP R/3) to a comprehensive e-business world (mySAP.com), where the Internet is at the forefront of any company business strategy, integration of Internet and complex system landscapes make security one of the most important elements for companies to consider. This is one of the reasons that mySAP.com security is incorporating a seamless integration with client certificates based on PKI (public-key infrastructure), and even providing its own trust center.

now becoming mainstream as well, such as the Web GUI, the shortcuts, the mySAP.com Workplace, the Session Manager, and other frontends or logon programs that can be programmed with SAP Automation and other utilities. The primary security service at the presentation level is user authentication.[3] When security fails at this level, it is typically because:

- The security policy is weak, not well communicated or enforced, or nonexistent.
- The profile parameters that enforce basic security measures are not set.
- You have not changed the passwords of standard users.
- Basic protection measures at the workstation are not taken.
- You have not implemented advanced security methods such as SNC, Single Sign-On, client certificates that allow encryption, or smart login devices.
- Security auditing and monitoring is scarce.

As a result, you see unauthorized users logging in with privileged user accounts, many unsuccessful logon attempts, or users using other people's accounts. Let me offer you a recent real-world scenario. I was asked to perform a security analysis for a customer. The customer gave me access to a PC. I asked him for a username and password to enter the SAP systems (they had many systems). He left for a few minutes to ask someone else for a username, and by the time he returned I had successfully logged in to every SAP system using the standard, well-known privileged username and password. At this point, I asked him, "What SAP instance do you want me to stop?"

**✔ *Tip***

*It is mainly the job of the Basis administrators and User administrators, together with the IT department and the security manager, to define a clear authentication policy, to set in place all the standard SAP security measures, and if needed, to add any advanced measures to protect the system at the presentation level.*

### *Application-Level Security*

Security at this level addresses the application logic that is run by the ABAP programs. Here, the main security service is the user authorization concept, which grants or denies access to business objects and transactions based upon a user's authorization profile. When security fails at this level, it is typically because:

- The authorization system has been poorly implemented.
- Critical authorizations have not been defined.
- Local development did not include appropriate authority checks.
- Administration of authorizations and profiles are not properly distributed and protected.
- The user and authorization information system is rarely used.

As a result, you see unintentional transaction executions by unauthorized users, performance problems, display or modification of confidential information by unauthorized users, or even deletion of

[3] Don't confuse the terms "authorization" and "authentication." *Authorization* is the process that determines what *access privileges* (i.e., permissions to perform particular operations) users are allowed. Authorizations are enforced by means of *access controls*, which are responsible for granting or restricting user access. In an SAP system, for instance, an R/3 authorization object is in charge of providing or denying access to particular entities or transactions within the system. *Authentication* is the process that verifies that users, programs, or services are actually who or what they say they are. Authentication is the cornerstone of any security infrastructure or technology. For example, entering the SAP user ID and password is an authentication technique. There are many other and more complex authentication techniques, such as authenticating to an external system, using smart cards with a PIN, reading a user's fingerprints, and so on.

important data. For example, on several occasions I have seen users who were not supposed to have sufficient authorizations unintentionally delete or change parts of the number range table (NRIV). Due to the legal implications of such alterations, these unintentional user actions required us to make a point-in-time recovery of the entire system.

***✔ Tip***

*It is the Application administrators' job to define which users have access to what data and transactions. These definitions must later be technically implemented by the User and Authorization administrators. It is also very important that every developer follows a programming methodology that includes security checks.*

### *Database-Level Security*

The R/3 database is the container for business information, as well as metadata, data models, and the Object Repository. It must be protected against unauthorized accesses. At this level, security services must grant access protection to R/3 data. When security fails at this level, it is typically because:

- Standard passwords have not been changed.
- Access to the operating system is not properly protected.
- Remote access to the database is not secure.
- Auditing has not been activated on critical tables.
- The authorization system at the SAP level is poorly implemented.

As a result, you see modifications at the database level that compromise systems integrity and consistency, uncontrolled access to confidential information below the application level, or systems unavailability. For instance, in one of my customer installations, an operator (who did not speak English very well) started a tablespace reorganization instead of adding a new datafile to a tablespace, causing the system to come to a complete halt for a few hours.

***✔ Tip***

*It is the job of the Database administrators, together with the OS system managers and the Basis administrators, to take appropriate security measures at this level. Some of these measures include changing the passwords of privileged database users, protecting SAPDBA with expert mode, restricting external remote access to read-only mode, auditing critical tables, and correctly setting the S_TABU_DIS authorization object.*

### *Operating System-Level Security*

Security services must guarantee access protection to R/3 files and directories, as well as the operating system commands and programs. At this level, security services are provided by the operating system features themselves. When security fails at this level, it is typically because:

- Permissions on files and directories are not properly set.
- The password and user policy at the OS level is static and widely known.
- Logging and monitoring is scarce.

As a result, you see deletion of important system and application files, software malfunctions, or unavailability. I have, on rare occassions, seen a system operator accidentally delete critical system files, like the database files, which were left fully unprotected. We then had to conduct a complete restore and recovery in order to get the system up and running again.

✔ *Tip*

*It is the job of the Operating System manager to implement security measures at the operating system level and to monitor the main log files that the audit system accesses. These measures include:*

- *Implementing a security password policy at the user level*
- *Avoiding the creation of unnecessary users or services*
- *Monitoring SETUID programs*
- *Setting ACLs (access control lists) in critical files and directories*
- *Protecting external commands from being executed from SAP*

### *Network-Level Security*

Networks are the de facto backbones of computing. There is no business or collaborative application that can work without one. SAP systems, based on a client/server architecture, are no exception. Starting with Release 3.1G, SAP R/3 systems include the SNC (Secure Network Connections) interface, which can, and in most cases should, be complemented with third-party security products to further protect network communications. When security fails at the network level, it is typically because:

- There are too many unprotected network services.
- The network topology is poorly designed.
- There is little or no network monitoring.
- Routers, filters, or firewalls are not correctly configured.
- The SAProuter configuration is not properly set.
- There is no automatic intrusion detection system.
- Communications are not traveling in encrypted form.

As a result, you see users (or programs) trying to log on to unauthorized systems, users logging on to the wrong servers, unbalanced system loads, or even sniffing. One example of security violations in the network environment is when end users log on directly to a database server that has an administrative instance. Another situation I have seen many times is when the **rlogin** service is completely unprotected and users have logged on through the network and stopped the wrong servers.

✔ *Tip*

*It is the Network administrators' responsibility to design and implement a security network topology that takes into consideration an automatic monitoring and intrusion detection system.*

### *Transport System-Level Security*

SAP has provided the CTS (Change and Transport System) as an environment for coordinated customizing and team development, and to protect the modification of objects and settings across an SAP landscape. Unfortunately, CTS is a facet of the SAP enterprise that is often under-secured.

When security fails at this level, it is typically because:

- System landscape settings are not properly configured.
- Repairs are freely allowed.
- There are no filters that control which objects are being transported.
- Authorizations are not completely implemented.
- Transport monitoring is not a periodic task.

As a result, you see software failures, transport of copied programs without security checks, or problems when upgrading your system. These problems are so common, I am sure you have seen them yourself in your own company.

> ✔ *Tip*
>
> *It is the task of the Basis administrator, together with customizers and developers, to properly set the system to basic security standards and to define a security policy that ensures that there is some type of filtering and monitoring within the Change and Transport System.*

### *Remote Communications-Level Security*

The natural openness of the R/3 system and the endless possibilities for communicating with and exchanging data between R/3 and other systems requires stringent security analysis from the point of view of external or remote communications, mainly in the areas of the RFC and CPIC protocols, which are used in other interfacing techniques such as ALE or BAPIs.

When security fails at this level, it is typically because:

- The authorization system is poorly implemented for remote communications.
- RFC communications include the passwords in their definitions.
- There is scarce monitoring at the gateways.
- OS and network security is weak.
- No encryption software has been used.

As a result, you see unexpected connections or program executions from other systems, software failures, or access to confidential information.

> ✔ *Tip*
>
> *It is the job of Basis administrators, together with Network administrators and developers, to implement standard security measures to avoid security holes at the remote communications level. Some standard measures include:*
>
> - *Avoiding the creation of more RFC destinations than are necessary*
> - *Including AUTHORITY-CHECK within the programs that can be remotely called*
> - *Protecting table RFCDES*
> - *Using standard interface techniques*
> - *Periodic monitoring of the gateway server*
> - *Ensuring that the **secinfo** file exits*

### *Document Transfer-Level Security*

SAP security services must guarantee the integrity, confidentiality, and authenticity of any type of business documents, such as electronic files, mail messages, and others. At this level, SAP provides Secure Store and Forward (SSF) mechanisms, which include digital signatures and digital envelopes based on public-key technology, and these mechanisms can be deployed using external security services, like digital certificates and digital envelopes.

When security fails at this level, it is typically because:

- Certificates and encryption are not used or implemented.
- Private keys are not properly protected.
- There is scarce tracing and monitoring.

As a result, you see documents intercepted by unauthorized persons or access to confidential information.

### ✔ Tip

*It is the job of the Basis administrators and expert security consultants, with the help of the legal department, to define and implement secure mechanisms like encryption methods for protecting the secure transfer of documents.*

### Internet-Level Security

The “Internet level” addresses the interactions that take place between an SAP system and browsers, Web servers, ITS, mySAP.com Workplace, firewalls, and so on.

When security fails at this level, it is typically because:

- Secure protocols are not properly set.
- Encryption and certificates are not used.
- Remote debugging of ITS is not disabled.
- Service files are not protected.
- Firewalls and authentication might not be properly configured.
- Security measures at Web servers are weak.
- Monitoring is scarce.

As a result, you see many types of attacks on Web servers that might render systems unavailable or compromise critical information.

### Multilevel Logging and Auditing

Last, but not least, a security infrastructure must include robust *logging and auditing* capabilities, the mechanisms you need to monitor and enforce your security policies. Logging and monitoring provides the feedback loop you need to gauge the efficiency of your security measures and helps you detect weaknesses, vulnerabilities, and trouble spots. There are logging and auditing facilities in the SAP security infrastructure at every level. These facilities are implemented mainly in the Security Audit Log, the Audit Info System (AIS), the security alerts within CCMS, and the User and Authorization Info System (SUIM). These tools are complemented by other logging facilities like those available at the operating system level, database auditing statements, network and Internet monitoring and management, etc.

The difficulty of monitoring the whole SAP security infrastructure is that there is no one tool that can do this for you automatically, although the evolution of the CCMS and the AIS tools indicate that there is a good chance it might happen in the future.

A comprehensive checklist for auditing security can be found in Volume III of the SAP Security Guide, which can be found at the SAP Service Marketplace (**http://service.sap.com/security**).

With so many security considerations to address, where do you begin? I like to start by identifying the entities that need to be protected and to what lengths a customer is willing to go in order to do so.

### ✔ Tip

*It is the job of the Basis administrator, Network administrator, and Web administrator to set in place a system design for implementing security measures that secure SAP systems that are tightly connected to the Internet.*

*As I’m sure you’re aware, there are thousands of Internet security incidents and break-ins reported — some of them make the CNN headlines. There are dozens of books and hundreds of Web sites covering Internet security, hacking, and protection software. For some examples, visit* ***www.securitynews.org****.*

*Figure 2* *Classifying the Degrees of Security*

| Classification | Description |
|---|---|
| Maximum | This level delivers maximum protection against system failure and downtime and the highest level of protection of confidential information, and delivers compliance with the strictest requirements for privacy, accuracy, and authenticity of information in critical business areas. |
| High | This level ensures general availability of information systems (i.e., with only short periods of downtime), and delivers a high degree of protection of confidential information, specifically in the critical business areas. Accuracy of data is not guaranteed, as it is at the maximum level of security. Here, the goal is that errors be detectable and corrected. |
| Moderate | At this level of security, short periods of unavailability of information systems can be tolerated. This level guarantees the confidentiality of information for internal use. Some types of non-critical errors could be tolerated; however, errors that could significantly impact system usage should be detectable and corrected. |
| Low | With a low degree of security, moderate periods of unavailability of information systems are tolerated, though long periods should be avoided — if information systems fail due to security problems and cause some alteration of operations, consequences are not considered critical. At this level, there is no requirement for information confidentiality. Errors are tolerated as long as they do not make it impossible to perform usual job functions. |

## *Establishing Degrees of Security: How Much Do You Have? How Much Do You Need?*

Security comes with a price tag. Depending on the human and technical factors that come into play, you will have to give up dollars and cents, manpower, application flexibility, system performance, or some combination thereof to achieve the desired level of security. Stronger security measures come at a higher "price." So, in practical terms, it is just not feasible to guarantee 100 percent security protection across the board. Resources are always limited, so expend them wisely. Ask yourself, "For each level of my SAP infrastructure, what tangible assets (e.g., critical information such as customer lists, employee data, contracts, hardware, and software) and intangible assets (hours of operation, cost of non-revenue, non-production, etc.) need to be protected?"

**Figure 2** offers some classification guidelines for determining degrees of security in your SAP infrastructure. Make a risk assessment where for each element within each security level, you rank, or classify, those assets together with:

- Standard, available security measures
- Additional security mechanisms
- Probability for vulnerability *before* you have revisited your security policy
- Time and cost of recovering the damage
- Tools or facilities for monitoring
- Tools or facilities for auditing

With the result of this risk assessment and your business requirements, you can objectively define those elements of the security infrastructure that need to be more urgently reviewed and implemented within your company.[4]

[4] Use available resources such as the SAP Security Guide (available at **http://service.sap.com/security**) for a comprehensive assessment of every security aspect of your SAP infrastructure.

How does your system security stack up so far? Is the appropriate degree of security being applied at each level of your SAP infrastructure? Having identified what is and what might still need to be secured, and to what degree, you must next identify a means for effecting the desired level of security. Numerous security resources come standard with an SAP R/3 system. These will be enumerated in the next section. As you review these standard offerings, ask yourself if these security measures are being optimally utilized in your environment. If they are not, it may, indeed, be time to revisit your SAP security infrastructure.

## Standard R/3 Security

SAP R/3 includes the standard security features listed below:

- User authentication
- User authorization
- Secure Network Communications (SNC)
- Secure Store and Forward (SSF)
- Digital signatures
- Single Sign-On (SSO) solutions
- Smart-card authentication
- Encrypted communications
- Logging and auditing

I've said it before, and I'm saying it again. You have got to secure *all* the layers of a multilayer SAP infrastructure. So exercising and improving SAP's standard security offerings is absolutely essential to the security of your system. Unfortunately, most customers don't do this. I suppose this is based on a misguided perception that the security that is operating at the network, operating system, and database levels is sufficient. Or perhaps they don't have an adequate command of how these security measures operate and can be improved upon.

## Operating and Improving Upon SAP's Standard Security Measures

Let's now take a closer look at the solutions SAP offers as part of its standard security measures, and some tips on how to improve upon them.[5]

### User Authentication

SAP's standard user authentication offering verifies a user's identity through the use of logon passwords.[6] (Unsuccessful logon attempts will cause the session to terminate and activate user locks.) As standard security measures, SAP provides several login profile parameters and an initial set of password rules, which you can expand on according to your needs. Standard security measures already provide a moderate-to-high degree of protection.

The Application administrator defines which users have access to what data and transactions, and the User and Authorization administrators perform the technical implementation of these definitions. It is also very important that every developer follows a programming methodology that includes security checks. User authentication applies mainly at the presentation level, but a breach will affect other layers as well.

The limitations of SAP's standard authentication have to do with the legal export rules of different

[5] In addition, a variety of third-party offerings can (and should) be applied as well. SAP supports the use of additional interfaces, add-ons, and external security products via smart-card authentication, SNC with encryption and SSO, and SSF. (Coverage of these solutions is beyond the scope of this article.)

[6] Users can also be authenticated at logon through the use of smart cards.

countries when including encryption software and algorithms — SAP overcame this by including SNC in the kernel.

✔ ***Tip***

*Additional security measures to raise your system to the highest protection level include:*

- *Using external security products that support encryption. Any such products, however, must be SNC-compliant (see the discussion below on SNC).*
- *Using techniques such as client certificates or logon tickets for Web user authentication security. However, these methods can only work if other security layers such as the network and Internet layers are also properly protected over secure protocols, such as SSL.*

Essential references for SAP user authentication can be found at SAP's online help, the SAP Security Guide, and the SNC user's guide (available at **http://service.sap.com/security**).

### *User Authorization*

SAP's standard user authorization offering secures user access to business data and transactions, ensuring that only pre-authorized users gain access to data and processes. User authorizations are defined by Authorization administrators in coordination with key business users in authorization profiles that are stored in the SAP user master records. An initial set of authorization profiles is predefined by SAP; you can modify/add to these profiles, and you can use the Profile Generator to automatically create new profiles based on user activity information.

Authorization applies to the application level mainly, but remote communications, operating system commands, and the Change and Transport System must also be taken into account.

The SAP authorization system is very comprehensive, but hard to fully implement to achieve the strictest, highest-degree security standards. It is hard to implement and maintain because it has a great deal of organizational requirements, where users, key users, managers, and technical consultants must be involved. Auditing and monitoring critical system authorizations is of paramount importance. The SAP online documentation as well as the SAP security guide provide the foundation for understanding and establishing a methodology for implementing the authorization concept.

✔ ***Tip***

*You can increase the security level of SAP's user authorization system by including well-defined development standards, along with a quality control that filters programs that do not implement the necessary security and authorization checks.*

### *Secure Network Communications (SNC)*

SAP's standard Secure Network Communications offering provides protection for the communication links between the distributed components of an R/3 system. SNC is built on the R/3 kernel based on standard GSS API V2, and allows you to increase the level of your SAP security via external security products — e.g., Single Sign-On, smart-card authentication, and encrypted communications.

Basis, User, Network, and Web administrators, along with the security and IT departments and SAP developers, are responsible for SNC. SNC can raise your system to high security standards because it can cover several layers, such as the presentation (authentication and Single Sign-On) layer, the remote communications layer, the network layer, and even the Internet layer.

You can find extensive information about SNC on SAP's security page at **http://service.sap.com/security**.

### *Secure Store and Forward (SSF)*

SAP's standard Secure Store and Forward offering provides the required support to protect R/3 data and documents as independent data units. You can use the SSF functions to "wrap" R/3 data in secure formats before the data is transmitted over insecure communications links. These secure formats are based on public and private keys using cryptographic algorithms.

Basis administrators and expert security consultants, with the help of the legal department, define and implement SSF.

> ✔ ***Tip***
>
> *While SAP provides a Security Library (SAPSECULIB) as a software solution for digital signatures, as well as standard support for SSF in certain application modules such as PDM or ArchiveLink, a high degree of protection is achieved only when private keys are secured using hardware devices such as smart cards.*

### *Digital Signatures*

SAP's standard digital signatures offering authenticates the R/3 data that is being transmitted and ensures that the senders (signatories) can be clearly determined. The subsequently assigned *digital envelope* ensures that the data contents will only be visible to the intended recipients. On SAP systems, digital signatures are based on SSF, but digital signatures based on public-key infrastructure can raise the system to a higher degree of security.

Basis administrators and expert security consultants, with the help of the legal department, define and implement digital signatures.

> ✔ ***Tip***
>
> *In certain countries, digital signatures can already be used legally as if they were handwritten. So, in security, digital signatures mean proof of obligation and non-repudiation.*

### *Single Sign-On (SSO) Solutions*

With SAP's standard Single Sign-On solutions, users only need to enter their passwords once, when they initially log on to the security system, or the operating system. The security system then generates "credential" information, so that the users can later automatically log onto other systems, such as R/3, without any password information being transmitted over the communication lines.

The Basis, User, Network, and Web administrators, together with the IT and security departments, are responsible for the implementation of Single Sign-On solutions.

You can find extensive information on Single Sign-On solutions on the security page of the SAP Service Marketplace (**http://service.sap.com/security**), in the Online Documentation, and in OSS note 138498.

**✔ *Tip***

*With R/3 and mySAP.com systems, there are many possibilities for Single Sign-On. Some of these are:*

- *External security products compliant with the SNC interface*
- *Using Central Administration*
- *Trusted systems*
- *Windows NT Security Provider*
- *Cookies*
- *Client certificates*
- *Using integration with LDAP servers*
- *SAP Logon Tickets*

### *Smart-Card Authentication*

SAP's standard smart-card authentication offering allows for a "safer" authentication process. The users use cards — "smart cards" — instead of passwords, to log on to the security system. No password information is transmitted over the communication lines. Because the smart cards are often protected with a password or PIN, it is much more difficult for someone to compromise a user's authentication information.

Basis and User administrators, along with the security and IT departments and legal experts, are responsible for implementing and maintaining smart-card authentication.

**✔ *Tip***

*The use of hardware devices such as smart cards is normally configured using an external security system based on the SNC interface.*

### *Encrypted Communications*

SAP's encrypted communications offerings secure the exchange of critical data. This is an important security aspect in e-commerce communications. You can use SAP's SNC solution and SSL protocol to encrypt the data being transferred via HTTPS connections. Data encryption ensures that the data being exchanged is secure, end-to-end, and protected from being intercepted.

As already mentioned, SAP does not directly include encryption software within their solutions, but provides the possibility of external security products that are compliant with SNC and SSF, so it can be used for authentication, for Single Sign-On, for digital signatures and envelopes, and so on.

My next book on mySAP.com (due out at the end of the year) is a collaborative work of many of my realTech colleagues. It includes a full chapter on specific procedures for approaching and handling the best practices in mySAP.com security.

## Conclusion

A comprehensive security strategy limits access at every security layer to only authorized users and/or authorized external systems. It also accounts for the overall *system landscape*: development systems, quality assurance system, productive system, and the Change and Transport System that operates between them, as well as any connected complementary systems, whether or not they belong to the SAP Business Framework (or Internet Business Framework) architecture. You want to be sure that certain protective procedures are set in place to guard against insecure programs or Trojan horses that may travel from one system to another.

I must stress that the goal is to identify not simply those measures that can best enforce your security policy, but the measures that will do so most efficiently. Efficiency in implementing and enforcing a security strategy means that you should avoid awkward procedures that obstruct or make users' jobs more difficult. You must always follow a principle of controls. By this I mean that your security strategy must strike a realistic balance between the control measures you require and the risks you agree to take.

Real-world threats are out there now — not looming in some futuristic science fiction scenario. Every organization has assets to protect from unauthorized entities. Reputation is one of those assets!

*José A. Hernández is Assistant Managing Director at realTech, an SAP partner and technical IT consulting firm specializing in R/3, mySAP.com, e-commerce, and the development of Enterprise Resource Management software. José joined realTech in December 1999, and is responsible for project management and consulting services for realTech customers in Spain.*

*José obtained experience in projects and building up business areas over the years while working for Ericsson, Telefónica Sistemas, and Digital Equipment/Compaq, before founding his own company, K2P, a knowledge management consulting firm. His last position at Compaq was as technical director for SAP projects.*

*José also published "The SAP R/3 Handbook" in 1997, which became the best-selling SAP book worldwide. In 1998 he published the first Spanish-language SAP book ("Así es SAP R/3"), and in 1999 José published his third book, "SAP R/3 Implementation Guide," as well as the second edition of "The SAP R/3 Handbook."*

*José can be reached at hernandez@realTech.de.*