Secure Network Communications - Integrating R/3 into Network Security Products

Introduction

Security in the sense of data protection is gaining more and more importance with R/3 customers. There are two reasons for this:

- R/3 becomes a "mission-critical" application if companies carry out their most important business processes with R/3.
- Programs and data are subject to a greater danger of loss, change and espionage in client/server environments than in mainframe based systems.

R/3 processes highly sensitive data (for example, company-internal and person-related information). This requires that R/3 also ensures security in the sense of data protection. A large number of security mechanisms are already in use in R/3, to preserve the confidentiality and integrity of the stored data:

- authentication of all users by means of passwords
- R/3 authorization concept
- activity logging
- protection of the communication between frontend and application server by compressing data.

To be able to conform to the growing security requirements of our customers, not only now but also in the future, SAP has started the "Secure Network Communications" project. The goal of the project is, among other things, to better protect the access to R/3 via the frontend and the communication between the frontend and the application server, hence the user-accessible side of the R/3 System (see figure 1). Here, it should be ensured to an even greater extent that only authorized users can log on to the system, and that the data on the WAN or LAN cannot be spied upon, falsified or deleted during communication.

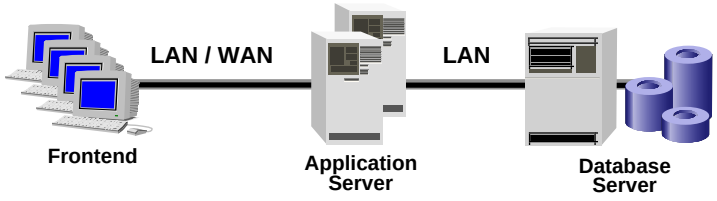

Figure 1: 3-Level Client/Server Architecture of R/3

Within this project, SAP will implement in R/3 Release 3.0 the GSS-API (Generic Security Services API), until approx. mid-1996, so that the R/3 System can be integrated in systems for company-wide network security (see point 2.1 for examples of these network security products).

The Integration of R/3 in network security products has two **significant advantages** for the customer:

1. The security of R/3 is increased further, since **further security measures** can be implemented using the security products supported.

- There is the possibility to **encrypt** the entire communication between the frontend and the application server. Greater protection against listening in and changing is achieved with this than using compression.

- Passwords are no longer sent over the link.

- Some security products, for example, SecuDE (see below) allow the use of **smartcards** for authentication. The users are no longer identified by what they know (password), but by ownership of a corresponding card. Since considerably longer passwords can be stored on a card than a user can remember, the protection against a guessing somebody's password is increased.

2. The customers can secure and **manage all** applications in their client/server environment, including R/3, **with one** security system.

- The user only needs to log on to a security system once per session, and can then use all of the client/server environment services **(sign-on)**. Repeated logging on, including management of several passwords in the system, is no longer necessary. In this way, the user should be more ready to choose longer and more complicated passwords, or to accept shorter validity intervals for a password.

- In the same way, the system administrator also only needs to operate and maintain **one** security system. The user check can be separated from the R/3 System. Checks for easily guessed passwords and other security checks need only be carried out in one security system. (However, the authorization profiles and user master records must still be maintained in R/3 itself, since the R/3 authorization concept is used within R/3.)

Since it must be assumed that security will become an increasingly important decision criterion when purchasing business application software in the near future, SAP has anticipated this trend with the "Secure Network Communications" project.

At this point it should be mentioned, that customers, only interested in encryption at the link layer, can achieve this already today through the use of crypto boxes. This hardware solution is totally transparent to SAP and has very high performance. A disadvantage are the high costs of acquisition.

The Security Products we are aiming for

SAP is looking at the following products for the company-wide network security of client/server systems (but in the version that R/3 needs, these products are only available, at best, as beta versions):

- Kerberos 5 from MIT,
- SecuDE 5.x from GMD,
- DCE from OSF and
- Sesame from Bull, ICL, SNI.

SAP is starting with support for Kerberos and SecuDE. By mid-1996, there will be implementations on all R/3 current 3.0 application server platforms (various UNIX operating systems and Microsoft NT). On the frontend platforms, both of these network security products will certainly support Windows 95, Windows NT and Motif.

Integration of the R/3 System into the Network Security Products

The above mentioned products offer services

- for the authentication of users/programs/resources and
- for the transfer of data
  (as plain text with an integrity check or encrypted).

An application must be subject to these network products so that

- communication can be secured,
- customer administrators have the option of maintaining authentication centrally,
- single logon features can be implemented.

The project "Secure Network Communications" aims to make a complete R/3 System compatible with Kerberos 5.

This means that SAP must extend the communication among all basic components of an R/3 system: frontend, application server, RFC, SAPLPD, and Gateway.

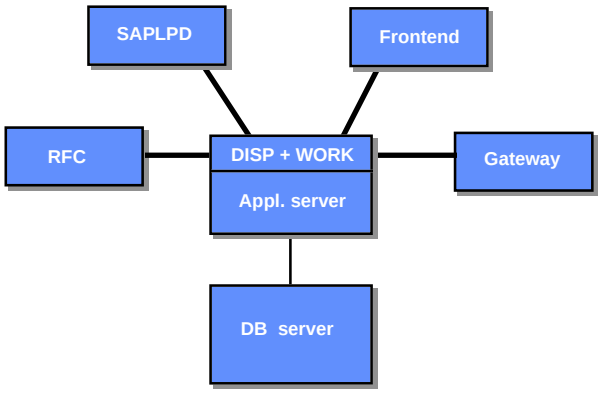

Figure 2: Overview of the links to be secured by SAP

The link between the database server and the application server has to be secured by the respective database producer since the communication from the application server to the database is carried out by the database requester.

SAP will not render the R/3 authorization management to external software, it will only externalize the user authentication.

No encryption software will be supplied on the R/3 CDs.

The CDs only contain the interfaces to the supported products and possibly a sample source for constructing adapters for other products.

Customers who want to use a supported Network Security Product must obtain this from the respective supplier. In this way, we can comply with very strict and widely varying legal requirements in the area of cryptology.

Requirements for the R/3 System

- R/3 release: **3.x**
- Frontend operating system:
  - **Windows 95** or
  - **Windows NT 3.5** or
  - X11 R5 / **Motif 1.2** - client

(at present, no definite statements can be made for OS/2 Version 3.0 or Apple OS System 7.5.)

Technical Information

There are already products on the market for establishing company-wide network security: a common feature of all of them, however, is that their installation *alone* does not influence the (in)security of existing applications. So that the security functions can be used, the entire network communication of the applications must be converted. That is, for every product, extra adjustments to the application are necessary, which have varying effects on the total communication mechanism of the application, depending on the architecture of the security product.

Only recently have people started discussing a standardized Security API with a standard communication model to abstract from the individual products and their characteristics. The standardization proposals of a "generic security interface" (Generic Security services API / GSS-API) have been defined by the CAT (Common Authentication Technologies) work group of the IETF (Internet Engineering Task Force).

This work group comprises representatives from companies / organizations such as Cybersafe, DEC, HP, IBM, MIT, OpenVision, OSF and SUN. A large part of the discussions were based on the security mechanisms of Kerberos 5 because this is contained as a (possible) security technology in the products of all the named companies.

The programming interface **GSS-API Version 1** was released in September 1993 as Internet RFCs-1508 & 1509 and is, for example, implemented in:

Kerberos 5	from MIT,	
DCE 1.1	from OSF	(available end 1995 from DEC, HP, IBM. Also planned at SUN and SNI),
SESAME 3	(SESAME Version 3 should appear in 1995).	

Meaning of names and abbreviations:

RFC	=	Request for Comments (a collection of articles and documents which concern the valid Internet standards, planned standards and general things concerning the network). (There is no relationship to SAP-RFC.)
MIT	=	Massachusetts Institute of Technology.
Kerberos	=	Network authentication system for an open network developed at MIT (in Greek mythology, this is the name of the three-headed dog that guards the entrance to hell).
GMD	=	Gesellschaft für Mathematik und Datenverarbeitung. (German National Research Center for Information Technology).
SecuDE	=	The GMD network security product ("Security Development Environment").
OSF	=	Open Software Foundation (members are among others: IBM, Hewlett-Packard and DEC).
DCE	=	Middleware for the development of distributed systems from OSF („Distributed Computing Environment“).

SESAME = Name of the project within the European RACE program for a secure network.

= Name of the security architecture resulting from this.

= a "construction kit", that is (or will be) used in products of ICL, Bull and Siemens.

When GSS-API version 1 was developed, the main consideration was the simplest form of client server communication, and compatibility was created on source level. On UNIX platforms the functional specification, with certain restrictions, also allows compatibility on the object level and for shared libraries — on the other hand, more precise function specifications are required for other platforms. The development of a Microsoft Windows DLL interface was published in February '95, a DLL interface for the Apple Macintosh is currently being worked on.

GSS-API Version 1 is not sufficient for the complex communications of R/3. Among other things, R/3 needs from GSS-API Version 2 the functions `gss_export_sec_context()` and `gss_import_sec_context()` to reach the endpoint of a secured connection via process limits. The additional required functionality from **GSS-API Version 2** will certainly be available with MIT's Kerberos 5, and SAPs partners at GMD will install this functionality in their product SecuDE too. Both Kerberos 5 from MIT and SecuDE 5.x from GMD will be available on the market to SAP customers by mid-1996. It will be a while before the functional specification of GSS-API V.2, which currently has the status of an Internet draft, is integrated in other products on the market (DCE, SESAME, ...) - not before end 1996 for DCE.

The following figure illustrates how an R/3 System could make use of the additional functionality of a network security product via an adapter. The adapter must be constructed by the producer of the respective security product and must be certified by SAP. SAP itself will install the R/3 System by default without additionally secured network communication.

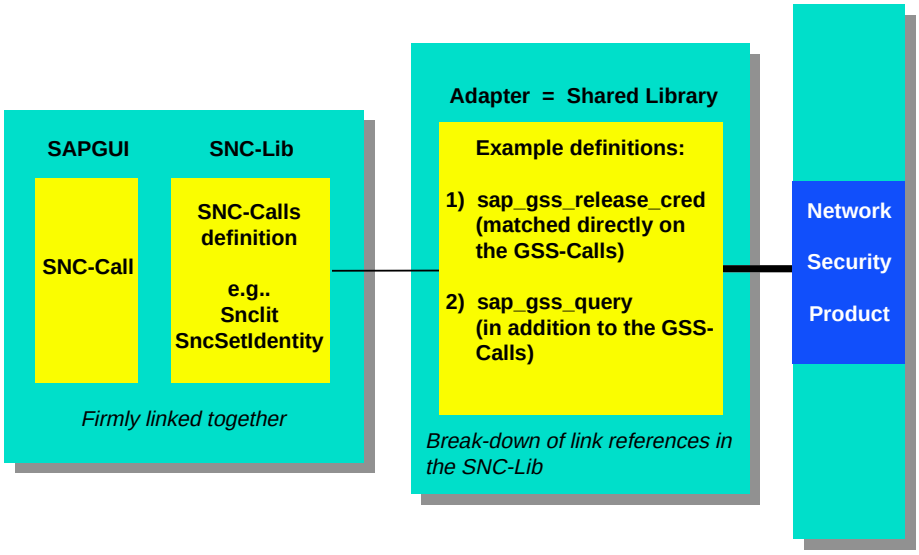

Figure 3: The Technical Interface to the Security Products

Undoubtedly you won't get security for "free" - it will definitely show up on the performance bill. Fortunately the above mentioned performance costs arise at a point in our R/3 architecture, which can easily be scaled, namely the application servers.

Encryption generally has performance costs regardless of whether it is carried out within the R/3 System or by network security products. Network security products are generally even better optimized than proprietary solutions, so that our approach of using the services of the security products via the GSS-API is certainly the best alternative (Each one does the business, he knows best.).

The use of the GSA-API offers our customers the choice between several security products. Moreover, that guarantees that he gets always the technologically up to date implementations.

In addition, the GSS-API allows the customer to choose between various levels of security:

- Communication as before
- External authentification
- Integrity checking
- Encryption.

Contact Persons at SAP

B. Esslinger,	Chief Security Officer SAP
A. Niedermaier,	Technology Marketing
C. Schramm,	Basis Sales and Distribution

SAP Glossary

RFC	Remote Function Call
SAPLPD	Line Printer Daemon

References

The following references are in part provided with short notes and are supplemented with readership indications - *MA* for managers, *PJ* for project managers.

1. "SAP R/3 software Architecture"; Functions in Detail Brochure; SAP; June 1994; (for all).

2. Kaufmann et Al: "Network Security"; Prentice Hall; 1995; Chap. 1 pp. 1-35; (for MA).

   - ❑ chapter 1 offers a general overview
   - ❑ a very competent book overall
   - ❑ deals with almost all relevant points

3. K. Russel: "Distributed and Secure"; Byte; June 1994; S. 165-178; (for MA).

   - ❑ good overview

4. Citibank N.A. / Coopers&Lybrand / Microsoft Corporations: "Microsoft windows NT 3.5: Guidelines for Security, Audit and Control"; Microsoft Press; 1995; (for *MA* + PJ).

   - ❑ chapter 1 stresses the special features of C / S systems compared to mainframes or single host systems

5. Cheswick, Bellovin: "Firewalls & Internet Security"; Addison-Wesley; 1994; (for PJ).

6. Garfinkel, Spafford: "Practical UNIX Security"; O'Reilly; 1991; (for PJ).

   - ❑ above all, deals with the security of a UNIX host.