Secure Network Communications - Integration von R/3 in Produkte zur Netzwerksicherheit

Einleitung

Sicherheit im Sinne von Datenschutz (**Security**) gewinnt bei R/3-Kunden immer mehr an Bedeutung. Dies hat zwei Gründe:

- R/3 wird zur „mission-critical“ Anwendung, wenn Firmen ihre wichtigsten betriebswirtschaftlichen Prozesse mit R/3 bearbeiten.
- Programme und Daten sind in Client/Server-Umgebungen sehr viel größerer Gefahr durch Verlust, Veränderung und Ausspionieren ausgesetzt als in Mainframe-basierten Systemen.

R/3 verarbeitet hochsensitive Daten (z. B. Firmeninternas und personenbezogene Informationen). Dies erfordert, daß R/3 Sicherheit auch im Sinne von Datenschutz gewährleistet. Schon heute werden in R/3 eine Vielzahl von Sicherheitsmechanismen eingesetzt, um die Vertraulichkeit und Integrität der gesicherten Daten zu wahren:

- Authentisierung aller Benutzer durch Paßwörter
- R/3 Berechtigungskonzept
- Tätigkeitsprotokollierung (activity logging)
- Schutz der Kommunikation zwischen Frontend und Anwendungsserver durch Komprimierung der Daten

Um den wachsenden Anforderungen unserer Kunden nach Sicherheit auch in Zukunft gerecht werden zu können, hat SAP das Projekt „Secure Network Communications“ initiiert. Ziel des Projekts ist es, u. a. den Zugang zum R/3 über die Frontends und die Kommunikation zwischen Frontend und Applikationsserver, also die dem Benutzer zugängliche Seite des R/3 Systems (siehe Bild 1), besser zu schützen. Hierbei soll in noch stärkerem Maße gewährleistet werden, daß sich nur autorisierte Benutzer am System anmelden können und daß die Daten während der Kommunikation über das WAN bzw. LAN nicht ausspioniert, verfälscht oder gelöscht werden können.

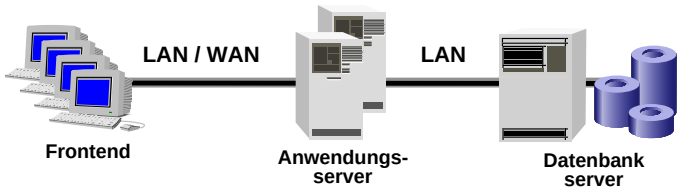

Bild 1: 3-Ebenen Client/Server Architektur von R/3

Innerhalb dieses Projekts wird SAP bis ca. Mitte 1996 im R/3 3.0-Release die Standardschnittstelle GSS-API (Generic Security Services API) implementieren, damit sich das R/3-System in Systeme zur unternehmensweiten Netzwerksicherheit integrieren kann (Beispiele für solche Netzwerksicherheitsprodukte siehe Punkt 2.1).

Die Integration von R/3 in Netzwerksicherheitssysteme hat zwei **große Vorteile** für den Kunden:

1. Die Sicherheit des R/3 wird weiter erhöht, da mit den unterstützten Sicherheitsprodukten **weitergehende Sicherheitsmaßnahmen** realisiert werden können.

- ❑ Es besteht die Möglichkeit, die gesamte Kommunikation zwischen Frontend und Anwendungsserver zu **verschlüsseln**. Damit wird ein höherer Schutz gegen Abhören und Verändern erreicht als durch Komprimierung.
- ❑ Paßworte werden nicht mehr über die Leitung geschickt.
- ❑ Manche Security-Produkte wie z.B. SecuDE (s. u.) ermöglichen den Einsatz von **Smart Cards** zur Authentisierung. Damit legitimiert sich der Benutzer nicht mehr nur durch das, was er weiß (Paßwort), sondern durch den Besitz einer entsprechenden Karte. Da auf einer Karte wesentlich längere Paßwörter gespeichert werden können als ein Benutzer sich merken kann, erhöht sich hierdurch der Schutz gegen das Erraten fremder Paßwörter.

2. Der Kunde kann **alle** Anwendungen in seiner Client/Server-Umgebung incl. R/3 **mit einem** Sicherheitssystem sichern und **verwalten**.

- ❑ Der Benutzer braucht sich nur noch einmal pro Sitzung bei einem Sicherheitssystem anmelden und kann dann alle Services der Client/Server-Umgebung nutzen **(Sign-on)**. Mehrmaliges Anmelden incl. der Verwaltung von mehreren Paßwörtern im System entfällt. Dadurch dürfte auch die Bereitschaft der Benutzer größer werden, längere und kompliziertere Paßwörter zu wählen oder auch kürzere Gültigkeitsintervalle für ein Paßwort zu akzeptieren.
- ❑ Der Systemadministrator muß ebenfalls nur noch **ein** Sicherheitssystem bedienen und pflegen. Die Userprüfung kann aus dem R/3-System herausgelegt werden. Paßwortprüfungen auf leicht zu erratene Paßwörter und sonstige Sicherheitsprüfungen müssen nur in einem Sicherheitssystem durchgeführt werden. (Die Berechtigungsprofile und die Benutzerstammsätze müssen jedoch weiterhin im R/3 selbst gepflegt werden, da innerhalb des R/3 das R/3-Berechtigungskonzept verwendet wird.)

Da davon auszugehen ist, daß Sicherheit in naher Zukunft ein immer wichtigeres Entscheidungskriterium beim Kauf von betriebswirtschaftlicher Anwendungssoftware werden wird, trägt SAP mit dem Projekt „Secure Network Communications“ diesem Trend schon jetzt Rechnung.

An dieser Stelle sei noch darauf hingewiesen, daß Kunden, die ausschließlich an Leitungsverschlüsselung interessiert sind, selbige schon heute mit Hilfe von Crypto-Boxen erreichen können. Diese Hardwarelösung ist für SAP völlig transparent und zeichnet sich durch ihre Schnelligkeit aus. Von Nachteil sind die hohen Anschaffungskosten.

Angestrebte Security-Produkte

Für die unternehmensweite Netzwerksicherheit von C/S-Systemen betrachtet SAP folgende Produkte (in der Version, die R/3 benötigt, gibt es diese Produkte bisher bestenfalls als Beta-Versionen):

- Kerberos 5 vom MIT,
- SecuDE 5.x von der GMD,
- DCE von der OSF und
- Sesame von Bull, ICL, SNI.

Den Anfang macht SAP mit dem Support für Kerberos und SecuDE. Für beide werden bis Mitte 1996 Implementierungen auf allen derzeitigen R/3 3.0-Applikationsserver-Plattformen (verschiedene UNIX-Betriebssysteme und Microsoft NT) vorliegen. Bei den Frontend-Plattformen werden diese beiden Netzwerk-Security-Produkte mit Sicherheit Windows 95, Windows NT und Motif unterstützen.

Integration von R/3 in die Produkte zur Netzwerksicherheit

Die oben genannten Produkte bieten Dienste an

- für die Authentisierung der Benutzer/Programme/Ressourcen und
- für die Übertragung der Daten
  (als Klartext mit Integritätsprüfung und/oder verschlüsselt).

Eine Anwendung muß sich diesen Netzwerkprodukten unterordnen, damit

- die Kommunikation gesichert werden kann,
- die Kunden-Administratoren die Möglichkeit haben, die Authentisierung zentral zu pflegen,
- Single Log-on Features realisiert werden können.

Das Projekt „Secure Network Communications“ hat das Ziel, ein komplettes R/3-System Kerberos 5-fähig zu machen.

Dies bedeutet, daß alle Teile der Basis erweitert werden müssen, die Kommunikation durchführen: Frontend, Applikationsserver, RFC, SAPLPD und Gateway.

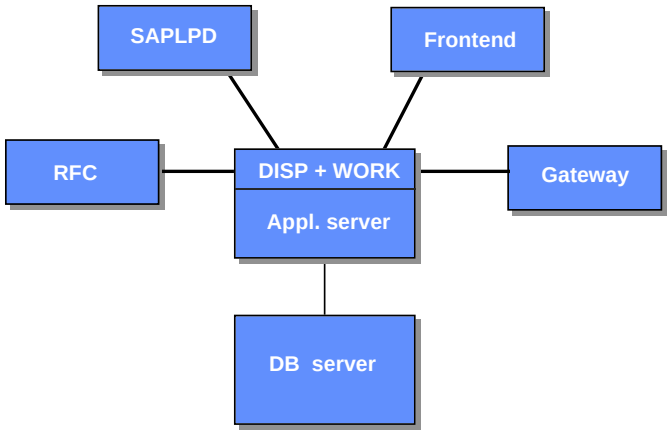

Bild 2: Übersicht über die von SAP zu sichernden Verbindungen

Die Verbindung zwischen Datenbankserver und Applikationsserver ist vom jeweiligen Datenbank-Hersteller zu sichern, da die Kommunikation auf dem Applikationsserver hin zur Datenbank vom Datenbank-Requester durchgeführt wird.

Das R/3-Berechtigungssystem wird nicht nach außen gelegt, sondern nur die Benutzerprüfung.

Auf den R/3-CDs wird keine Verschlüsselungssoftware ausgeliefert.

Die CDs enthalten nur die Schnittstellen zu den unterstützten Produkten und evtl. eine Beispielsource zum Bau eines Adapters an weitere Produkte.

Kunden, die ein unterstütztes Netzwerk-Security-Product einsetzen wollen, müssen sich dieses beim jeweiligen Hersteller besorgen. Auf diese Weise wird den sehr strengen und verschiedenartigen gesetzlichen Regelungen im Bereich Kryptologie Genüge getan.

Voraussetzungen an das R/3-System

- R/3-Release: **3.x**
- Frontend-Betriebssystem:
  - **Windows 95** oder
  - **Windows NT 3.5** oder
  - X11 R5 / **Motif** 1.2 - Client

(für OS/2 Version 3.0 bzw. Apple-OS System 7.5 können zur Zeit noch keine sicheren Aussagen gemacht werden.)

Technische Information

Es gibt auf dem Markt bereits Produkte zu Errichtung einer unternehmensweiten Netzwerksicherheit: allen gemeinsam ist aber, daß ihre Installation *allein* die (Un-)Sicherheit bestehender Applikationen nicht beeinflußt. Damit die Sicherheitsfunktionen genutzt werden können, muß die gesamte Netzwerk-Kommunikation der Applikation umgerüstet werden. D. h. für jedes

Produkt sind extra Anpassungen an der Applikation notwendig, die sich je nach Architektur des Security-Produktes unterschiedlich stark auf den gesamten Kommunikationsmechanismus der Applikation auswirken.

Erst in jüngster Zeit verhandelt man über eine standardisierte Security-API mit einem einheitlichen Kommunikationsmodell, um von den speziellen Produkten und ihren Eigenarten zu abstrahieren. Die Standardisierungs-Vorschläge einer „generischen Sicherheits-Schnittstelle“ (Generic Security Services API / GSS-API) werden von der Arbeitsgruppe CAT (Common Authentication Technologies) des IETF (Internet Engineering Task Force) erarbeitet.

In dieser Arbeitsgruppe sind z.B. Firmen / Organisationen wie Cybersafe, DEC, HP, IBM, MIT, OpenVision, OSF und SUN vertreten. Ein großer Teil der Diskussionen orientiert sich an den Sicherheitsmechanismen von Kerberos 5, weil dieses in Produkten aller genannten Firmen als (eine mögliche) Sicherheitstechnologie enthalten ist.

Die Programmier-Schnittstelle **GSS-API Version 1** wurde im September 1993 als Internet-RFCs-1508 & 1509 herausgegeben und ist unter anderem implementiert in:

Kerberos 5	vom MIT,	
DCE 1.1	von OSF	(Ende 1995 verfügbar von den Herstellern DEC, HP, IBM. Planung auch von SUN und SNI),
SESAME 3	(SESAME Version 3 soll noch 1995 erscheinen).	

Bedeutung der Namen und Abkürzungen:

RFC	=	Request for Comments (eine Sammlung von Artikeln und Dokumenten, in denen die gültigen Internet-Standards, geplante Standards und allgemeine das Netz betreffende Dinge enthalten sind). (Es besteht kein Zusammenhang mit dem SAP-RFC.)
MIT	=	Massachusetts Institute of Technology.
Kerberos	=	Ein am MIT entwickeltes Netzwerk-Authentifizierungs system für ein offenes Netz (in der griechischen Sage ist es der Name des dreiköpfigen Hundes, der den Eingang zur Hölle bewacht).
GMD	=	Gesellschaft für Mathematik und Datenverarbeitung.
SecuDE	=	Netzwerk-Sicherheits-Produkt der GMD („Security Development Environment“).
OSF	=	Open Software Foundation (darin arbeiten u.a. mit: IBM, Hewlett-Packard und DEC).
DCE	=	Middleware zur Entwicklung von verteilten Systemen von der OSF („Distributed Computing Environment“).

SESAME = Name des Projektes innerhalb des europäischen RACE-Programms für ein sicheres Netzwerk.

= Name der daraus entstandenen Security-Architektur.

= ein „construction kit“, das in Produkten von ICL, Bull und Siemens genutzt (werden) wird.

Beim Entwurf der GSS-API Version 1 hatte man in erster Linie an die einfachste Form von Client-Server Kommunikation gedacht und eine Kompatibilität auf Source Level geschaffen. Auf Unix-Plattformen ermöglicht die Spezifikation mit gewissen Einschränkungen auch Kompatibilität für Object Level und Shared Libraries — für andere Plattformen sind dagegen genauere Spezifikationen notwendig. Der Entwurf einer Microsoft Windows DLL Schnittstelle wurde im Februar ’95 veröffentlicht, an einer DLL-Schnittstelle für den Apple MacIntosh wird gearbeitet.

Die GSS-API Version 1 reicht für die komplexen Kommunikationsbeziehungen des R/3 nicht aus. Aus der GSS-API Version 2 benötigt R/3 u.a. die Funktionen `gss_export_sec_context()` und `gss_import_sec_context()`, um den Endpunkt einer gesicherten Verbindung über Prozeßgrenzen weiterzureichen. Die zusätzlich notwendige Funktionalität aus der **GSS-API Version 2** wird auf jeden Fall in MIT’s Kerberos 5 zur Verfügung stehen, die GMD wird diese Funktionalität ebenfalls in ihr Produkt SecuDE einbauen. Sowohl Kerberos 5 vom MIT als auch SecuDE 5.x von der GMD werden bis Mitte 1996 für SAP-Kunden auf dem Markt verfügbar sein. Bis sich die derzeit im Status eines Internet Drafts befindliche Spezifikation der GSS-API V.2 in anderen auf dem Markt befindlichen Produkten (DCE, SESAME, ...) niederschlägt, wird wohl noch einige Zeit vergehen - bei DCE ist damit nicht vor Ende ‘96 zu rechnen.

Bild 3 veranschaulicht, wie ein R/3-System über einen Adapter die zusätzliche Funktionalität eines Netzwerk-Security-Produktes in Anspruch nehmen könnte. Der Adapter ist vom Hersteller des jeweiligen Security-Produktes zu bauen und muß von der SAP zertifiziert werden. Die SAP selbst wird defaultmäßig ihr R/3-System ohne zusätzliche gesicherte Netzwerk-Kommunikation installieren.

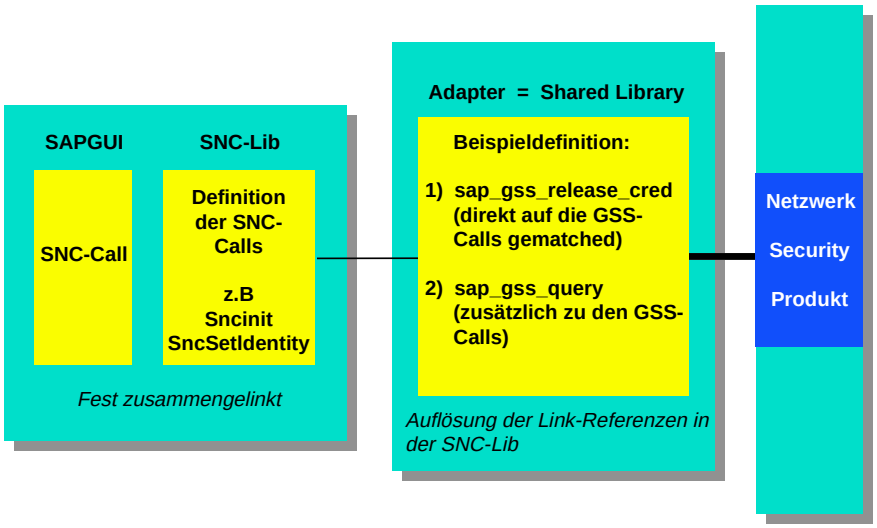

Bild 3: Die technische Schnittstelle zu den Security-Produkten

Mit Sicherheit wird „Security“ nicht umsonst sein, sondern Performance kosten. Zum Glück fallen die Performancekosten jedoch an den Stellen in der Architektur des R/3-Systems an, die man sehr gut skalieren kann, nämlich den Applikationsservern.

Verschlüsselung kostet generell Performance — unabhängig davon, ob diese innerhalb des R/3-Systems oder von Netzwerk-Security-Produkten gemacht wird. Netzwerk-Security-Produkte sind meist sogar besser optimiert als proprietäre Lösungen, so daß unser Ansatz, die Dienste der Security-Produkte über die GSS-API zu nutzen, sicher die bessere Alternative darstellt (Jeder macht das Business, das er am besten beherrscht.).

Durch die Benutzung der GSS-API hat der Kunde die Auswahl unter verschiedenen Security-Produkten und hat so die Gewähr, stets nachprüfbar technologisch die neuesten Entwicklungen zu erhalten.

Außerdem erlaubt die GSS-API, daß der Kunde wählen kann zwischen verschiedenen Sicherheitsstufen:

- Kommunikation wie bisher
- externe Authenthisierung
- Integritätsprüfung
- Verschlüsselung.

Ansprechpartner bei SAP

B. Esslinger,	Chief Security Officer SAP
A. Niedermaier,	Technologie Marketing
C. Schramm,	Basis Vertrieb

Glossar der SAP-Begriffe

RFC	Remote Function Call
SAPLPD	Line Printer Daemon

Literaturhinweise

Die folgenden Hinweise sind zum Teil mit kurzen Anmerkungen versehen und durch Angaben ergänzt, welchem Leserkreis SAP die Hinweise zuordnen - *MA* für Manager, *PJ* für Projektleiter.

1. „SAP R/3 Software Architcture“; Functions in Detail Brochure; SAP; June 1994; (für alle).

2. Kaufmann et al: „Network Security“; Prentice Hall; 1995; Kap.1, S. 1-35; (für *MA*).

   - ❑ 1. Kapitel bietet eine allgemeine Übersicht
   - ❑ insgesamt ein sehr kompetentes Buch
   - ❑ es behandelt fast alle relevanten Punkte

3. K. Russel: „Distributed and Secure“; Byte; June 1994; S. 165-178; (für *MA*).

   - ❑ guter Überblick

4. Citibank N.A. / Coopers&Lybrand / Microsoft Corporations: „Microsoft Windows NT 3.5: Guidelines for security, audit and control“; Microsoft Press; 1995; (für *MA* + *PJ*).

   - ❑ 1. Kapitel betont die Besonderheiten bei C / S-Systemen im Vergleich zu Mainframes oder Single-Host-Systemen

5. Cheswick, Bellovin: „Firewalls & Internet Security“; Addison-Wesley; 1994; (für *PJ*).

6. Garfinkel, Spafford: „Practical UNIX Security“; O’Reilly; 1991; (für *PJ*).

   - ❑ behandelt vor allem die Sicherheit eines UNIX-Hosts.