

Sicherer mobiler Dienstzugang – Gastarbeitsplätze in Intranets

Secure Mobile Access to Network Services – Guest Desks in Intranets

(Wirtschaftsinformatik, Sonderheft 12/2000)

Norbert Luttenberger
Universität Kiel

Zusammenfassung

Projektbezogene Kooperationen zwischen unabhängigen Organisationen verlangen oftmals die temporäre Entsendung von Mitarbeitern einer oder mehrerer Organisationen in die Intranet-Umgebung eines gastgebenden Partners. Im vorliegenden Beitrag wird dargestellt, welche Sicherheitsprobleme von diesem Szenario ausgehen, insbesondere wenn die abgeordneten Mitarbeiter nach wie vor auf Dienste in ihrem *home intranet* zugreifen wollen und müssen. In Abgrenzung zu Techniken für die Mobilitätsunterstützung wird eine für diesen Fall angemessene und sichere Lösung für Konnektivität der Intranets entwickelt, und es werden Elemente für ein angepaßtes Dienstzugangsmanagement entworfen, die den Aufenthaltsort des Zugreifenden berücksichtigen.

Abstract

Project-oriented collaborations between independent organisations often demand a temporary delegation of staff members of one or more organisations into the intranet environment of one hosting partner. The paper discusses the security risks arising from this scenario especially when delegated staff need continuing access to services in their home intranets. In contrast to usual mobility support technologies, a secure solution for intranet connectivity adapted to this scenario is developed, and in above, elements for a tailored service access management are sketched, reflecting the location of the user requiring service access.

Stichworte

Gastarbeitsplätze, Intranets, Intranet-Konnektivität, *mobility management*, Dienstzugangsmanagement, Intranet-Sicherheit, mehrseitige Sicherheit, *Mobile IP*, *Service Location Protocol*, *Jini*, *IP Security Architecture*

Keywords

Guest desks, intranets, intranet connectivity, mobility management, service access management, intranet security, multilateral security, Mobile IP, Service Location Protocol, Jini, IP Security Architecture

Kernpunkte für das Management

Kooperationen zwischen unabhängigen Organisationen verlangen häufig die Entsendung von Mitarbeitern in die Intranet-Umgebung einer gastgebenden Organisation. Der Beitrag zeigt auf, wie die Einrichtung von Gastarbeitsplätzen für diese Situation sicher und wirkungsvoll durchgeführt werden kann:

- Bildung einer „Enklave“ im gastgebenden Intranet,
- Einschränkung der Mobilität auf freizügigen Netzzugang in Client/Server-Umgebungen,
- Herstellung der Konnektivität zwischen den Intranets der entsendenden und der aufnehmenden Organisation über die *IP Security Architecture*,
- Erweiterungen von Verfahren für das Dienstzugangsmanagement.

1 Das Szenario

In der Ära der wirtschaftlichen, wissenschaftlichen und politischen Globalisierung gewinnen projektorientierte Kooperationen zwischen Firmen, Organisationen und öffentlichen Einrichtungen eine zunehmende Bedeutung. Solche Kooperationsprojekte werden z.B. zwischen Firmen eingerichtet, die in einer Auftraggeber/Auftragnehmer-Beziehung zueinander stehen, etwa zwischen einem Hersteller kompletter Systeme und einem Lieferanten von Baugruppen. Solche Kooperationen werden aber auch von international agierenden Firmen eingegangen, die sich am Markt als Konkurrenten gegenüberstellen. Dann haben sie meist Entwicklungs- und Forschungstätigkeiten zum Gegenstand, Projektanteile also, die zeitlich vor einer Produktphase im engeren Sinne liegen.

Alle diese projektgebundenen Kooperationen haben einige gemeinsame Merkmale: Sie sind von klar befristeter Dauer; in der Projektdurchführung kann es mehrfach erforderlich sein, das Projektteam neu zusammenzusetzen, z.B. wenn bestimmte Spezialqualifikationen benötigt werden; und meistens erfordern diese Projekte auch die temporäre „Abordnung“ von Mitarbeitern aus einer Organisation in die Umgebung der kooperierenden Organisation, da die Verständigung durch den direkten persönlichen Austausch erheblich gefördert wird. Wissenschaftler, Ingenieure, Designer, Marketing-Spezialisten müssen also zeitweise beherbergt werden, d.h. es muß ihnen von der jeweils gastgebenden Organisation ein Arbeitsplatz, in der Regel ein Computer-Arbeitsplatz, zur Verfügung gestellt werden.

In diesem Beitrag soll geklärt werden, welche Anforderungen von der Einrichtung solcher Arbeitsplätze an die Netzwerkinfrastruktur der beteiligten Organisationen gestellt werden und wie entsprechende Lösungskonzepte aussehen. Wohlgedenkt geht es hier *nicht* um Anforderungen, die durch spezielle Arbeitsplätze, z.B. durch multimediale Arbeitsplätze mit CSCW-Applikationen (*Computer Supported Cooperative Work*), gestellt werden, sondern es geht um „konventionelle“ Computer-Arbeits-

plätze, deren Kern möglicherweise der vom Gast mitgebrachte portable Computer bildet. Dabei wird ein besonderer Fokus auf der Frage liegen, wie solche Arbeitsplätze unter Wahrung der Sicherheitsinteressen aller Beteiligten eingerichtet werden können.

In unserem Zusammenhang wird davon ausgegangen, daß die entsendende und die gastgebende Organisation separate Intranets betreiben. Gastarbeitsplätze sollen im Intranet der gastgebenden Organisation so eingerichtet werden, daß der Gast zum einen schnell auf ausgewählte Dienste im Intranet der gastgebenden Organisation zugreifen kann. Zum anderen soll für den Gast aber auch der Zugriff auf bestimmte Dienste in seinem *home intranet* erhalten bleiben. Zum Beispiel soll er von seinem Gastarbeitsplatz aus ggf. e-Mail von seinem „*home Mail-Server*“ abholen oder auf einen WWW-Server zugreifen können, der ansonsten nur *innerhalb* des *home intranet* zugänglich ist. Nur so bringt die Entsendung in die fremde Umgebung kein inakzeptables Abgeschnittensein von Informationen über Vorgänge in der eigenen Organisation mit sich. Neben diesen allgemeinen Diensten kann es für den Gast erforderlich sein, auf spezielle Applikationen, z.B. auf Datenbanken in seinem *home intranet* zuzugreifen, die Informationen zur Verfügung stellen, auf die er zur Erfüllung seiner Aufgabe nicht verzichten kann.

Innerhalb der so umrissenen Aufgabenstellung, die in [4] in das Gebiet *nomadic computing* [3] eingeordnet wird, lassen sich die folgenden Teilprobleme identifizieren, die gemeinsam angegangen werden müssen:

1. Es muß eine sichere Konnektivität zwischen dem gastgebenden Intranet und dem *home intranet* des Gastes hergestellt werden, d.h. es muß geklärt werden, welche über den „einfachen“ Anschluß beider Intranets an ein gemeinsames Netz hinausgehenden Maßnahmen erforderlich sind.
2. Für den Gast müssen einfache und sichere Mechanismen für das Auffinden und das Management von Diensten im gastgebenden Intranet zur Verfügung stehen, damit lästige Konfigurationsarbeiten entfallen können. Sinnvollerweise müssen sich diese Mechanismen auch auf Dienste im *home intranet* beziehen lassen, da dieses Intranet während der Abwesenheit des entsandten Mitarbeiters von Veränderungen betroffen sein kann.

Die Lösungen für diese beiden Teilprobleme sind so zu gestalten, daß durch die Beherbergung eines Gastes die Sicherheit des gastgebenden Intranet nicht beeinträchtigt wird. Ebenso wenig darf die Sicherheit des *home intranet* durch die Eröffnung von Zugriffsmöglichkeiten für den extern weilenden Mitarbeiter beeinträchtigt werden. Mit letzterem ist auch verbunden, daß die Information, die dieser Mitarbeiter aus dem *home intranet* abholt, vor Angriffen während der Übertragung geschützt wird.

Im vorliegenden Beitrag werden zunächst die auftretenden Sicherheitsprobleme analysiert. Im Mittelpunkt des dritten Abschnitts steht das Teilproblem „Konnektivität“; dabei geht es insbesondere um die Untersuchung existierender Lösungen aus dem Bereich des *mobile networking* auf ihre Eignung für das Gastarbeitsplatz-Szenario. Dabei ist es das Ziel, zu einer für dieses Szenario angemessenen Mobilitätsdefinition zu kommen. Im vierten Abschnitt werden Techniken für das Dienstemanagement dargestellt und Anforderungen an ein Sicherheitskonzept entwickelt, das die besondere Aufgabenstellungen des Gastarbeitsplatz-Szenarios berücksichtigt. Der Beitrag schließt mit einem Ausblick auf zukünftige Aktivitäten innerhalb des DFG-geförderten SECCO-Projekts, in dessen Rahmen die hier dargestellten Untersuchungen stattfinden.

2 Sicherheitsanalyse

2.1 Intranets

Entsprechend der üblichen Definition sind Intranets private Netze, in denen die vom Internet her bekannte Netzwerkarchitektur benutzt werden: Aufbauend auf TCP/IP werden in Intranets Informationsdienste wie WWW, ftp, e-Mail, News usw. als interne (und meist auch als externe) Dienste angeboten, zu denen in aller Regel bestimmte organisationsspezifische Dienste und Applikationen hinzukommen. In einem Intranet befinden sich schützenswerte Datenbestände, die außerhalb des Intranets nicht sichtbar werden dürfen.

Ein Intranet besteht ggf. aus mehreren miteinander verbundenen LANs. Oftmals wird innerhalb eines Intranet einer der in RFC-1918 [11] definierten privaten Adreßräume (zusammen mit einer Vorkehrung für die *address translation*) benutzt, um der Adreßknappheit in IPv4 zu begegnen. Die in einem Intranet verwendeten Adressen sind dann im öffentlichen Internet nicht sichtbar.

Intranets sind gegen das öffentliche Internet durch Firewall-Systeme abgeschottet. Diese Firewall-Systeme sollen verhindern, daß Unbefugte auf Datenbestände in einem Intranet zugreifen können. Firewall-Systeme führen die notwendigen Zugriffskontrollen mit unterschiedlichen Mechanismen durch; die wichtigsten sind die Paketfilterung (auf TCP/IP-Ebene) und die Kontrolle auf Dienstebene mit Hilfe von spezifischen *application-level gateways*.

Applikationen in Intranets kooperieren nach dem Client/Server-Modell: Auf den Arbeitsplatzrechnern der Benutzer sind Client-Applikationen installiert, die je nach Aufgabe verschiedene Dienste in Anspruch nehmen, die von den im Intranet vorhandenen Server-Applikationen erbracht werden. Server speichern Daten (File-Server, FTP-Archive, News-Server, WWW-Server), Server speichern Nachrichten (Mail-Server), Server drucken (Print-Server), Server stellen Datenbankinhalte und -abfragen zur Verfügung (Database Server), und Server sind ggf. für spezielle Applikationen eingerichtet (Application Server) usw. Ein Intranet-Benutzer kann ohne Zugriffe auf die von diesen Servern vorgehaltenen Informationen und Funktionen seine Aufgabe kaum erfüllen.

2.2 Sicherheitsimplikationen

Die Beherbergung eines Gastes hat differenzierte Sicherheitsimplikationen für das gastgebende Intranet, für das *home intranet* und für die durch das Internet transportierte Information.

Im gastgebenden Intranet wird die gastgebende Organisation trotz ihrer Gastgeberrolle nicht alle Bereiche ihrem Gast eröffnen wollen. Entsprechend dürfen vom Gast nur solche Dienste genutzt werden, die durch die gastgebende Organisation explizit freigegeben worden sind. Weiterhin müssen Kommunikationsvorgänge zwischen den Mitarbeitern der gastgebenden Organisation für den Gast unbeobachtbar und damit implizit vertraulich bleiben. Aus Sicht des Gastes gelten die gleiche Forderung in umgekehrter Richtung. Zur Erfüllung dieser Anforderungen wird die gastgebende Organisation für ihren Gast deshalb einen eigenen Netzbereich (eine „Enklave“) vorsehen, der vom übrigen Intranet durch ein internes Firewall-System abgeschirmt ist. Beim Aufenthalt mehrerer Gäste mit voneinander unabhängigen Arbeitsaufträgen sind entsprechende feinere Sicherungsgranularitäten erforderlich.

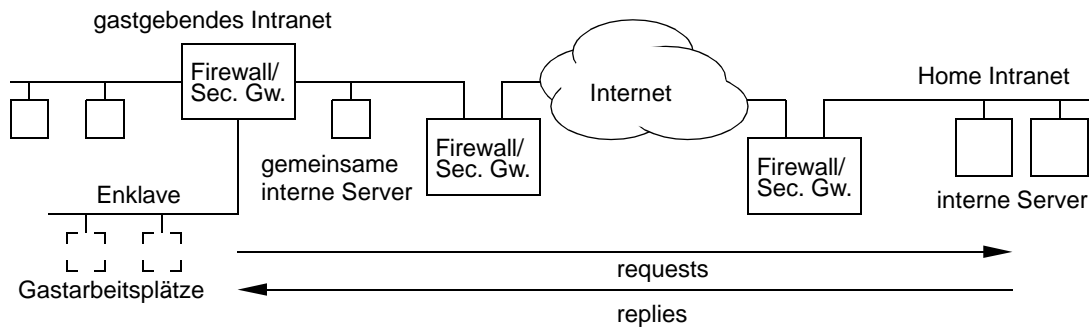


Bild 1: Zugriff eines Gastes auf Server in seinem *home intranet*

(Der Einfachheit halber werden Intranets als LANs mit Bustopologie dargestellt; zum Begriff *Security Gateway* (Sec. Gw.) s. auch 3.3)

Für den Zugriff auf Dienste im *home intranet* müssen also zwei oder mehr Firewall-Systeme durchdrungen werden, mindestens das Firewall-System des gastgebenden Netzes und das Firewall-System des *home intranet* (vgl. Bild 1). Insbesondere das Firewall-System des *home intranet* muß dafür Zugriffe zulassen (z.B. POP3-Requests auf einen internen Mail-Server), die „normalerweise“ strikt unterbunden werden. Dazu ist als Minimalanforderung in jedem Fall eine strenge Authentifizierung des Gasts im Firewall-System des *home intranet* erforderlich.

Die aus dem Heimatnetz abgeholte Information muß vertraulich, unverfälscht und verdeckt (zur Bedeutung dieser Begriffe s. unten!) durch das Internet transportiert werden. Im gastgebenden Intranet müssen die vom Gast importierten Informationen ebenfalls vertraulich und unverfälscht transportiert werden; hinzu kommt ggf. die Forderung nach Unbeobachtbarkeit durch die Mitarbeiter der gastgebenden Organisation.

Die für das Gastarbeitsplatz-Szenario zu berücksichtigenden Schutzziele beziehen sich in erster Linie auf die „üblichen“ Schutzziele Vertraulichkeit, Authentizität und Integrität der Kommunikation. Hinzu kommen ggf. weitere Schutzziele, die meist im Kontext des Begriffs „Privatheit“ diskutiert werden, z.B. Verdecktheit und Unbeobachtbarkeit [15]. Verdeckte Kommunikationsvorgänge laufen so ab, daß einem Externen die schiere Tatsache der Kommunikation verborgen wird. Im Umfeld unseres Szenarios bedeutet dies, daß einem Externen die Tatsache verborgen bleibt, daß es eine Kommunikation aus dem gastgebenden Netz in das *home intranet* gibt. Aus der externen Aufdeckung solcher Kommunikationsbeziehungen könnten unerwünschte Schlüsse auf Kooperationsbeziehungen zwischen den beteiligten Organisationen gezogen werden.

Der Gast und selbstverständlich auch seine Gastgeber sollen zusätzlich die Möglichkeit haben, ihre jeweils eigenen Kommunikationsbeziehungen bei Bedarf unbeobachtet durchzuführen: Es stehen ja keineswegs alle Kommunikationsvorgänge im Zusammenhang mit einer kooperativen Tätigkeit zwischen dem Gast und seinen Gastgebern.

Sinnvollerweise wird eine Lösung das generelle Konzept der mehrseitigen Sicherheit [6], [7], [8] aufzugreifen haben, das hier konkret vorsieht, daß der Gast gemeinsam mit den Systemadministratoren des gastgebenden Netzes und des *home intranet* Zugriffsrechte und zugehörige Sicherheitsmaßnahmen verabredet. Dabei kann keine der drei beteiligten Instanzen alleine entscheiden; alle Festlegungen müssen kooperativ erfolgen. Für die angesprochenen Verabredungen werden Mechanismen für das Dienstzugriffsmanagement benötigt, die im folgenden Abschnitt diskutiert werden.

3 Sichere Konnektivität in Intranet-Umgebungen

Damit ein Gast Dienste, die von seinem *home intranet* zur Verfügung gestellt werden, nutzen kann, muß zunächst eine Konnektivität vom Gastarbeitsplatz hin zum *home intranet* hergestellt werden. Aus heutiger Sicht lassen sich dafür im wesentlichen drei Techniken unterscheiden:

- Zugang über einen PSTN/ISDN-Einwahlknoten,
- Verwendung von Mobilitätsunterstützungstechniken und
- Verbindung der beiden Intranets auf der Basis eines dedizierten *Virtual Private Network*.

Diese drei Lösungen werden im folgenden auf ihre Eignung hin untersucht.

3.1 PSTN/ISDN-Einwahlzugänge

Oftmals wird für mobile Mitarbeiter, die sich außerhalb des eigenen Intranet (z.B. in einem Hotel) aufhalten, ein PSTN/ISDN-Einwahlzugang eingerichtet, der gegen mißbräuchliche Benutzung z.B. über einen RADIUS-Server (*Remote Dial-In User Service*, [12]) abgesichert ist. Gegen die Übertragung dieser Technik in das hier beschriebene Gastarbeitsplatz-Szenario lassen sich wichtige Argumente vorbringen: Bei Verwendung eines Einwahlzugangs würde der mobile Mitarbeiter an seinem Gastarbeitsplatz nicht nur einen Zugang zum Intranet der gastgebenden Organisation (in aller Regel also einen LAN-Zugang) benötigen, sondern auch einen davon separaten Zugang zum Telefonnetz oder ISDN.

Damit aber kann der mobile Mitarbeiter nicht mehr über einen einheitlichen Netzzugang auf Dienste zugreifen, sondern muß der Heterogenität des Netzwerkzugangs in einer komplexen Konfiguration seines Systems (Routing-Tabelle, *Name Service* usw.) Rechnung tragen. Das kann – u.a. in Abhängigkeit vom jeweiligen Betriebssystem – dazu führen, daß bei jedem Server-Zugriff entsprechende Umkonfigurationen vorgenommen werden müssen. Vor allem aber können solche Einwahlzugänge Kosten in nicht unbeträchtlicher Höhe erzeugen. Diese Gründe sprechen deutlich gegen Einwahlzugänge im Rahmen des Gastarbeitsplatz-Szenarios.

3.2 Mobile IP

Für das Internet ist im RFC-2002 eine Mobilitätsunterstützung unter dem Namen *Mobile IP* [9] definiert worden. Da in Intranets die gleiche Netzwerkarchitektur wie im Internet verwendet wird, erscheint es für unseren Zweck plausibel, hier das für das Internet definierte *Mobile IP* auf seine Eignung für das Gastarbeitsplatz-Szenario zu überprüfen. Im RFC-2002 wird ein auf das dargestellte Szenario passender Anspruch erhoben: „*A new, scalable, mechanism is required for accommodating node mobility within the Internet. This document defines such a mechanism, which enables nodes to change their point of attachment to the Internet without changing their IP address.*“ Die Vorstellung dahinter ist also, quasi mit einem Bein noch *home intranet* zu verbleiben, während man sich im gastgebenden Intranet aufhält. Ohne der detaillierten Argumentation vorwegzugreifen, soll hier schon gesagt werden, daß die *Mobile IP* zugrundeliegende Mobilitätsdefinition für unser Szenario problematisch ist.

Versucht man den eher vieldeutigen Begriff Mobilität in der Umgebung von Kommunikationsnetzen etwas „technischer“ zu fassen, so könnte eine Definition wie folgt lauten: In einem mobilen Netz¹ ist die Netzwerkadresse eines Teilnehmers unabhängig vom aktuellen Netzzugangspunkt. Innerhalb dieser Definition lassen sich mindestens drei nicht überschneidungsfreie Aspekte erkennen:

Freizügigkeit: Teilnehmer können wechselnde *points-of-attachment* ans Netz benutzen; dies ist unabhängig davon, ob es sich um ein drahtloses (Funk- oder Infrarot-) Netz oder um ein Festnetz handelt.

Erreichbarkeit: Ein mobiler Teilnehmer bleibt unabhängig von seinem jeweils aktuellen *point-of-attachment* (d.h. bei freizügigem Netzzugang) für andere Teilnehmer erreichbar, d.h. es kann eine Verbindung zu diesem Teilnehmer hin aufgebaut werden.

Beweglichkeit: Ein mobiler Teilnehmer kann einen laufenden Kommunikationsvorgang (eine *session*) auch dann zu Ende führen, wenn er während der *session* seinen *point-of-attachment* wechselt.

Die Freizügigkeit des Netzzugangs bildet den Kern der Definition des Begriffs Mobilität. Die Gewährleistung von Erreichbarkeit und Beweglichkeit kann man als Zusatzeigenschaften mobiler Netze betrachten, die auch z.B. in den ersten Mobilfunknetz-Varianten (A- und B-Netz) noch nicht erfüllt waren.

Soll ein mobiler Teilnehmer erreichbar sein, so muß im Netz sein Aufenthaltsort bekannt sein. Dazu verfügt das Netz über Aufenthaltsdatenbanken, in denen Informationen über den aktuellen Aufenthaltsort aller Teilnehmer enthalten sind, die von den Teilnehmern bzw. ihren Geräten über sog. Registrierungsprotokolle ständig aktualisiert werden. (In GSM-Netzen wird hier von *location update*-Protokollen gesprochen.) Teilnehmerbeweglichkeit erfordert im Netz darüberhinaus die Anwendung von sog. *hand-over*-Prozeduren, mit deren Hilfe ein Mobilitätsagent des mobilen Netzes einen Teilnehmer an einen anderen Mobilitätsagenten „weiterreichen“ kann.

Durch *Mobile IP* werden – global formuliert – die Mobilitätseigenschaften moderner Mobilfunknetze in die Internetumgebung übertragen, unabhängig davon, ob die mobilen Teilnehmer ihren Kontakt zum Internet über wechselnde *points-of-attachment* im Festnetz oder in einem Funknetz herstellen. (Teilnehmerbeweglichkeit kann dabei offensichtlich nur in einer Funknetzumgebung gewährleistet werden.) Insbesondere der Forderung nach Erreichbarkeit ist in *Mobile IP* große Aufmerksamkeit gewidmet worden: Ein mobiler Teilnehmer bleibt unter „seiner“ IP-Adresse² erreichbar, auch wenn er seinen Aufenthaltsort in ein anderes (Sub-) Netz verlegt. Dazu sieht *Mobile IP* vor, daß ein mobiler Teilnehmer in seinem *home network* durch einen sog. *home agent* vertreten wird, der alle an den mobilen Teilnehmer gerichteten Nachrichten entgegennimmt und an den aktuellen Aufenthaltsort nachsendet. Dazu muß der mobile Teilnehmer bei jedem Wechsel des Aufenthaltsorts eine entsprechende Aktualisierungsnachricht an den *home agent* schicken. Durch diese Technik kann – bezogen auf das oben dargestellte Gastarbeitsplatz-Szenario – also erreicht werden, daß ein mobiler Teilnehmer mit seinem *home intranet* verbunden bleibt.

Die gegenseitige Erreichbarkeit, die bei der Definition von *Mobile IP* in Analogie zu Mobilfunknetzen im Mittelpunkt der Bestrebungen stand, hat bei Sprach- und Datenkommunikation einen völlig verschiedenen Stellenwert. Sprachkommunikation ist *peer-to-peer*-Kommunikation, d.h. zwei gleichbe-

-
1. Sieht man von speziellen Satellitennetzen ab, so ist in Wirklichkeit selbstverständlich nicht das Netz mobil, sondern es sind die Teilnehmer, die mobil sind. Dennoch hat sich dieses Quidproquo eingebürgert und wird auch in diesem Beitrag verwendet.
 2. Das Possessivpronomen ist in Zusammenhang mit dem Terminus IP-Adresse in Anführungszeichen gesetzt, da es sich bei einer IP-Adresse nicht um eine persönliche Adresse handelt, sondern um die Identifikation eines Netzzugangspunktes.

rechtigte, kompatible Endsysteme kommunizieren miteinander, und die Initiative zum Aufbau einer Kommunikationsbeziehung kann gleichermaßen von beiden Endsystemen ergriffen werden. Dafür müssen beide Systeme erreichbar sein.

In der Rechnerkommunikation dagegen sind Dienste durch die Kommunikation zwischen Client- und Server-Applikationen definiert. Auf den Arbeitsplatzrechner der Benutzer, die ggf. von unterschiedlichen *points-of-attachment* aus arbeiten, sind Client-Applikationen installiert, während Server-Applikationen typischerweise auf stationären Systemen vorgehalten werden. Client-Applikationen treten mit Servern in unterschiedlichen Netzen in Kontakt. Entscheidend ist: In Client/Server-Umgebungen geht die Initiative zum Aufbau einer *session* immer vom Client und damit vom Arbeitsplatzrechner des Benutzers aus. Server werden nicht von sich aus aktiv, sondern warten auf eingehende *service requests*. Client und Server sind also keine *peers*.

Daraus läßt sich nun folgern, daß in Client/Server-Umgebungen der Aufenthaltsort der mobilen Einheit (Client) im Netz nicht ständig bekannt sein muß, da es keine spontane Kommunikation Server → Client gibt; Clients sind nicht das Ziel von Kommunikationsinitiativen. In dem Moment, wo eine Client-Applikation einen *service request* absetzt, enthüllt sie implizit – durch die *service request* enthaltene Absendeadresse – dem jeweiligen Server ihren *point-of-attachment* ans Netz. Im Gegensatz zu Clients müssen Server allerdings ständig erreichbar sein; ein *mobility management* für Server ist aber nicht erforderlich, da Server in aller Regel stationär sind. Zugespißt formuliert: Nicht die Erreichbarkeit von Benutzersystemen muß bei der Datenkommunikation unterstützt werden, sondern die Erreichbarkeit von Diensten und den zugehörigen Servern, unabhängig vom Aufenthaltsort des Benutzersystems. Zur Herstellung dieser Art von Erreichbarkeit ist ein „übliches“ *mobility management* nicht geeignet.

Wie steht es mit der Forderung nach Beweglichkeit? Typischerweise verbleibt ein Client bis zum Abschluß der Diensterbringung an seinem Aufenthaltsort, d.h., einmal begonnene *sessions* werden bei unverändertem Aufenthaltsort zu Ende geführt. Sollte es doch einmal erforderlich sein, auch bewegliche Benutzer zu unterstützen (man könnte sich z.B. Arbeitsplätze in schnellfahrenden Zügen vorstellen), dann kann als Zugang zum Netz in der Regel ein Mobilfunknetz à la GSM/GPRS bzw. UMTS benutzt werden. Dort erfolgt dann das *mobility management* innerhalb des *radio link* und nicht im Internet.

Die Übertragung eines aus dem GSM-Umfeld entlehnten *mobility management* in die Domäne der Internet-Datenkommunikation scheint damit nur in wenigen Sonderfällen geeignet, die im Gastarbeitsplatz-Szenario anfallenden Mobilitätsprobleme zu lösen, da es zu einseitig auf den Aspekt Erreichbarkeit hin ausgerichtet ist. Stattdessen wird eine Mobilitätsunterstützung benötigt, die den Aspekt der Freizügigkeit in den Mittelpunkt stellt.

3.3 VPN-basierte Lösung

Aus der Sicht heutiger Internet/Intranet-Netzstrukturen wird Mobilität im Sinne eines freien Zugangs zu Diensten und Servern von wechselnden *points-of-attachment* aus vor allem durch Sicherheitsmaßnahmen (d.h. insbesondere durch Firewall-Systeme) eingeschränkt, durch die Intranets gegen unberechtigte Zugriffe auf interne Server „abgeschottet“ werden. Dahinter steht eine grundsätzlich veränderte Auffassung von der Betriebsweise des Internets. Während man früher beim Internet von der Vorstellung eines *offenen Netzes* ausging, in dem alle Rechner für alle Benutzer erreichbar waren, gilt heute, daß die im Internet sichtbar gewordenen schwerwiegenden Security-Probleme eine Abkehr von

diesem Konzept mit sich gebracht haben. Wir haben es mit einer dichotomen Netzlandschaft zu tun: auf der einen Seite sichere, vertrauenswürdige Intranets, auf der andere Seite das öffentliche Internet, das lediglich als Verbindungsnetz gesehen wird, das unsicher und nicht vertrauenswürdig ist.

Zur Herstellung einer freizügigen Konnektivität zum *home intranet* muß deshalb in allererster Linie die Sicherheit der dort befindlichen Informationsressourcen sichergestellt werden. Hier wird dazu von einer Lösung ausgegangen, die auf der Basis der *IP Security Architecture* [2] beruht. Über die in dieser Architektur vorgesehenen Mechanismen können Daten verschlüsselt und authentifiziert in einem sog. *Virtual Private Network* (VPN) übertragen werden. Deshalb bildet ein VPN mit den konstituierenden *Security Associations* entsprechend [2] die „unterste Schicht“ der Kommunikationsarchitektur für das Gastarbeitsplatz-Szenario.

Allerdings sind die in der *IP Security Architecture* vorgesehenen Mechanismen zunächst noch nicht benutzer- und dienstespezifisch, so daß die pauschale Einrichtung eines VPN den jeweiligen Schutzinteressen der beteiligten Organisationen nur mangelhaft Rechnung tragen würde. Deshalb muß das vorgesehene VPN im Sinne der mehrseitigen Sicherheit kooperativ so eingerichtet werden, daß es

- nur von authentifizierten Benutzern
- in Abhängigkeit von deren aktuellen Aufenthaltsort (s.u.!)
- nur für bestimmte Dienste,
- die von bestimmten Servern zur Verfügung gestellt werden,

benutzt werden kann. Einige Kommentare zu diesen Anforderungen:

(1) Im Vorgriff auf diese Lösung sind die in Bild 1 dargestellten Firewall-Systeme zusätzlich als *Security Gateways* bezeichnet worden: Diese bilden die End- und Zwischenpunkte von gesicherten Übertragungswegen in VPNs. (2) Die gestellte Forderung nach Benutzer-Authentifizierung muß sich auf den Gast selber und nicht nur auf die von ihm verwendete IP-Adresse beziehen; der Gast verwendet ja eine IP-Adresse aus dem gastgebenden Intranet, aus der sich für das *home intranet* nicht direkt auf den Benutzer schließen läßt. (3) Die Unterscheidung zwischen Diensten und Servern ist zu treffen, da ggf. zwar bestimmte Dienste (z.B. ein Druckdienst) benutzbar sein sollen, aber dazu nur ausgewählte Server „freigeschaltet“ werden sollen. (4) Es muß auch der Fall berücksichtigt werden, daß sich im *home intranet* die Zuordnung von Servern zu Diensten in gewissen zeitlichen Abständen ändern kann.

Insbesondere die Herstellung einer dienstespezifischen Lösung stellt ein schwieriges Problem dar, da die IPsec-Architektur dienstespezifisch ist. In [4] wird eine Lösung dargestellt, in der die angestrebte Dienstespezifität durch die Einschaltung von Proxy-Clients und -Servers für die jeweiligen Dienste erreicht wird, obwohl auf der Netzwerkschicht die dienstespezifischen Mechanismen von IPsec verwendet werden. Hier soll im folgenden in Ergänzung dazu eine Lösung skizziert werden, die auf allgemeinen Mechanismen für das Dienstemanagement aufsetzt.

4 Dienstzugriffsmanagement für Gastarbeitsplätze

In [1] entwirft R. Kehr unter dem Stichwort „Spontane Vernetzung“ ein Bild zukünftiger Netzwerk-Infrastrukturen, in dem der Zugriff auf Dienste in einem Netzwerk „keinerlei Konfigurationen, keinerlei Administration“ erfordert. Offensichtlich sind solche Infrastrukturen auch für das Gastarbeitsplatz-Szenario erforderlich. Im folgenden sollen hier ebenso wie in [1] nur solche Aspekte diskutiert werden, die

oberhalb der Netzwerkebene liegen und sich mit dem Dienstzugriffsmanagement beschäftigen. Es soll dabei gezeigt werden, wie die angebotenen Infrastrukturen für das Dienstmanagement so eingebettet und ergänzt werden können, daß die oben angestrebte Dienstespezifität erreicht wird.

4.1 Existierende Lösungen

Mit dem Gastarbeitsplatz-Szenario stellen sich Managementprobleme, die sich auf das Auffinden von Diensten, auf die Verwaltung von Zugriffsrechten und auf die Steuerung der anzuwendenden kryptographischen Mechanismen beziehen. Die wichtigsten heute in diesem Umfeld diskutierten Lösungen sind das *Service Location Protocol* [13] und die von Sun entwickelte *Jini*-Technologie [10], [14]. (Für eine knappe Übersicht über diese Lösungen und über weitere Techniken sei auf [1] verwiesen.)

Das *Service Location Protocol* sieht ein URL-Schema für die Dienst-Identifizierung vor. Es ist derzeit ausschließlich für die Umgebung von lokalen Netzen definiert worden und kann im Umfeld des Gastarbeitsplatz-Szenarios u.a. verwendet werden, um dem Gast seine „Einrichtung“ im gastgebenden Intranet zu erleichtern.

Jini sieht die Bildung von Arbeitsgruppen aus Benutzern, Diensten und Geräten vor. Diese werden als kooperierende Java-Objekte modelliert. Der Zugang zu Diensten wird in einer *Jini*-Umgebung über Java-RMI realisiert.

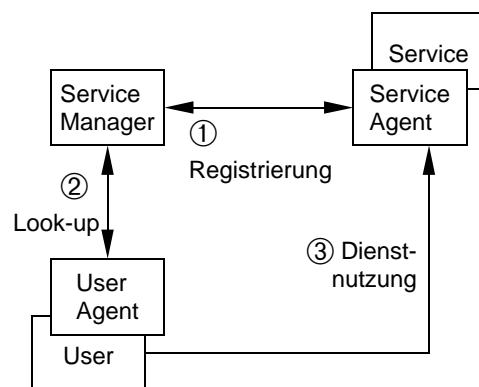


Bild 2: Grundstruktur Dienstmanagement

Beide Techniken nutzen – sehr global gesehen – eine ähnliche Konfiguration, bestehend aus einem zentralen Service-Manager, Service-Agenten und Benutzer-Agenten (Bild 2). Dienste werden initial über einen zugehörigen Service-Agenten bei einem zentralen Service-Manager registriert. Dort können sie dann von Benutzer-Agenten abgefragt werden. Ein so erreichbar gemachter Dienst kann schließlich (über den User-Agenten oder direkt) genutzt werden.

4.2 Erweiterungen für das Gastarbeitsplatz-Szenario

Ohne wegen des frühen Projektstandes bereits auf Details eingehen zu können, wird hier vorgeschlagen, die Funktionalität von Service-Managern so zu erweitern, daß sie den besonderen Anforderungen des Gastarbeitsplatz-Szenarios besser gerecht werden.

Es soll davon ausgegangen werden, daß ein Gast von seinem Gastarbeitsplatz aus den Service-Manager seines *home intranet* vor der Nutzung eines Dienstes im *home intranet* kontaktiert. Als ein Beispiel für eine notwendige Funktionserweiterung des Service-Managers diene die Formulierung von Regeln, mit denen der Service-Manager die Gewährung eines Zugangs zu Diensten und Servern im *home intranet* und die konkrete Form der Client/Server-Kommunikation (inkl. der anzuwendenden kryptographischen Mechanismen) vom Aufenthaltsort des Anfordernden abhängig macht. Dies ist sinnvoll, da es in Abhängigkeit von der Art des Kooperationsbeziehung, von der Dauer des Gastaufenthaltes und von einem unterschiedlichen Maß an Vertrauen zwischen den beteiligten Organisationen unterschiedliche Möglichkeiten und Notwendigkeiten gibt.

Damit kommt man zu einer Datenbank, die für jeden extern verweilenden Benutzer und für jeden zur Verfügung stehenden Dienst eine Menge von Regeln für den Zugriff aus unterschiedlichen Netzen umfaßt. Diese Datenbank enthält damit die im Sinne der mehrseitigen Sicherheit ausgehandelten Verabredungen in formaler Art. Vor dem ersten Dienste- bzw. Serverzugriff nach einem Wechsel des Aufenthaltsort muß der in einem fremden Netz angekommene Mitarbeiter sich bei dieser Datenbank mit seinem Aufenthaltsort registrieren. (Der aktuelle Aufenthaltsort kann ggf. anhand der (authentifizierten) Quelladresse der Registrierungsanforderung erkannt werden.) In Abhängigkeit vom jeweiligen Aufenthaltsort des Benutzers wird eine Entscheidung darüber getroffen, welche Dienste bzw. Server für einen bestimmten Benutzer aus einem anderen Netz zugänglich bleiben. Zur Illustration ein knappes Beispiel (in einer vorläufigen Syntax): Ein Benutzer U halte sich temporär im Intranet N1 auf. Die Datenbank enthalte für das Netz N1 den im folgenden skizzierten Eintrag:

```
for user U
  on registration request from intranet N1:
    ftp      permit;
    e-mail   permit service get: auth, crypt;
    http     permit service get: auth, crypt, cover;
    news     deny;
```

Im Klartext etwa: „Auf den ftp-Dienst darf der Benutzer unbeschränkt zugreifen; es gelten keine besonderen Sicherheitsmaßnahmen. e-Mail kann abgeholt, aber nicht gesendet werden; Authentifizierung ist erforderlich, die Nachrichten werden verschlüsselt transportiert. Lesende Zugriffe auf interne WWW-Seiten können mit Benutzerauthentifizierung weiterlaufen, der Transport soll verschlüsselt und verdeckt laufen. Der Zugang zum News-Server ist generell gesperrt.“ (Die letzte Regel kann als redundant betrachtet werden, da gelten soll, daß alles, was nicht explizit erlaubt ist, verboten ist.) In die dargestellten Regeln gehen die Identifier für die Ressourcen selbstverständlich nach der Syntax und Semantik des jeweiligen Service-Managers ein.

5 Ausblick

Im Rahmen des SECCO-Projekts soll ein Testbed aufgebaut werden, in dem insbesondere die dargestellten Konnektivitätsmechanismen und Managementverfahren untersucht werden können. Weiterhin soll untersucht werden, inwieweit sich eine alternative Lösung auf der Basis mobiler Agenten für den sicheren Zugriff auf Datenbestände im *home intranet* eignet (vgl. auch [4]).

Literatur

- [1] Kehr, R.: *Spontane Vernetzung*. Informatik Spektrum: 23, 3 (6/2000), 161–172.
- [2] Kent, S., Atkinson, R.: *Security Architecture for the Internet Protocol*. RFC-2401, 1998.
- [3] Kleinrock, L.: *Nomadic Computing and Communications*. In: NII 2000 Steering Committee, National Research Council (Ed.): *The Unpredictable Certainty - Information Infrastructure Through 2000. White Papers*. Washington (National Academy Press) 1997, ISBN 0-309-06036-2, pp. 335–342. Auch elektronisch: <http://bob.nap.edu/readingroom/books/whitepapers/>
- [4] Link, C., Luttenberger, N.: *Sicheres Nomadic Computing in Intranet-Umgebungen – Problemstellungen und Lösungskonzepte*. Eingereicht für die Konferenz „Kommunikation in Verteilten Systemen 2001“ (KiVS 2001, Hamburg).
- [5] Montenegro, G., Gupta, V.: *Sun's SKIP Firewall Traversal for Mobile IP*. RFC-2356, 1998.
- [6] Müller, G., Pfitzmann, A. (Eds.): *Mehrseitige Sicherheit in der Kommunikationstechnik (Bd. 1) – Verfahren, Komponenten, Integration*. Bonn u.a. (Addison-Wesley-Longman) 1997, ISBN 3-8273-1116-0.
- [7] Müller, G., Stapf, K.-H. (Eds.): *Mehrseitige Sicherheit in der Kommunikationstechnik (Bd. 2) – Erwartung, Akzeptanz, Nutzung*. Bonn u.a. (Addison-Wesley-Longman) 1998, ISBN 3-8273-1355-0.
- [8] Müller, G., Rannenberg, K. (Eds.): *Multilateral Security in Communications (Vol. 3) – Technology, Infrastructure, Economy*. München u.a. (Addison-Wesley-Longman) 1999, ISBN 3-8273-1360-0.
- [9] Perkins, C.: *IP Mobility Support*. RFC-2002, 1996.
- [10] Posegga, J.: *Jini: Infrastruktur für dynamische Dienste in verteilten Systemen*. Informatik Spektrum 22, 1 (2/1999), 43–44.
- [11] Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G. J., Lear, E.: *Address Allocation for Private Internets*. RFC-1918, Feb. 1996.
- [12] Rigney, C., Rubens, A., Simpson, W., Willens, S.: *Remote Authentication Dial In User Service (RADIUS)*. RFC-2138, April 1997.
- [13] Veizades, J., Guttman, E., Perkins, C., Kaplan, S.: *Service Location Protocol*. RFC-2165, June 1997.
- [14] Waldo, J.: *Jini Technology Architectural Overview*. <http://www.sun.com/jini/whitepapers/architecture.html>
- [15] Wolf, G., Pfitzmann, A.: *Charakteristika von Schutzzielen und Konsequenzen für Benutzungsschnittstellen*. Informatik Spektrum: 23, 3 (6/2000), 173 – 191.

Autor

Norbert Luttenberger studierte Elektrotechnik an der TU Braunschweig und arbeitete von 1977–84 als Automatisierungsingenieur bei der Siemens AG in Erlangen. 1984 wechselte er als wissenschaftlicher Mitarbeiter an den Lehrstuhl für Rechnerarchitektur und Verkehrstheorie (Prof. Dr. U. Herzog) der Universität Erlangen-Nürnberg, wo er 1989 zum Dr.-Ing. promoviert wurde. Danach war er am Europäischen Zentrum für Netzwerkforschung der IBM in Heidelberg in den Bereichen Multimedia-Kommunikation und Mobile Datenkommunikation tätig. 1995 wurde er auf die Professur für Datenübertragung und Netzwerke im Fachbereich Informatik der Fachhochschule Gelsenkirchen berufen. Seit Okt. 2000 bekleidet er die Professur für Kommunikationssysteme am Institut für Informatik und Praktische Mathematik der Christian-Albrechts-Universität zu Kiel.