

Sicheres *Nomadic Computing* in Intranet-Umgebungen – Problemstellungen und Lösungskonzepte

Carsten Link, Norbert Luttenberger

Christian-Albrechts-Universität zu Kiel
Institut für Informatik und Praktische Mathematik
{cli,nl}@informatik.uni-kiel.de

Abstract. Im vorliegenden Beitrag werden das Anwendungsszenario *nomadic computing* und die sich daraus ergebenden Kommunikationsstrukturen dargestellt. Für die Probleme, die sich einem mobilen Computerbenutzer in fremden Intranets stellen, werden zwei Lösungsansätze vorgestellt, wobei besonders auf Sicherheitsprobleme eingegangen wird.

1 Einführung

Arbeit an wechselnden Aufenthaltsorten ist zu einem Kennzeichen moderner Formen der Arbeitsorganisation geworden. Bezüglich der technischen Arbeitsbedingungen bedeutet der temporäre Aufenthalt bei einer fremden Organisation für die betroffenen Mitarbeiter, die oftmals ihr persönliches und portables Rechensystem (Laptop, Notebook o.ä.) in die neue Umgebung mitbringen, daß sie im gastgebenden Intranet de facto von den Netzwerkdiensten abgeschnitten sind, die im Intranet der eigenen Organisation (dem Heimatnetz) angeboten werden. Aus naheliegenden Gründen werden diese Dienste im Heimatnetz gegen Zugriffe über das Internet abgeschottet. Ausgeschlossen vom Zugriff auf die von diesen Servern vorgehaltenen Informationen und Funktionen kann aber ein Mitarbeiter an seinem neuen Aufenthaltsort viele seiner Aufgaben nur sehr viel umständlicher erfüllen, oder er verliert den Kontakt zu internen Informationen in nicht akzeptablem Umfang.

Das vorgestellte Szenario fügt sich nahtlos in den Kontext ein, den Kleinrock 1997 unter dem anschaulichen Begriff *nomadic computing* allgemein zusammengefaßt hat [6]. Betont sei hier, daß wir speziell Nomaden betrachten, die sich innerhalb eines fremden Intranets aufhalten.

2 Problemstellung

In diesem Szenario ist es für Nomaden nicht sinnvoll, in einem gastgebenden Intranet die komplette Heimatumgebung wiederherstellen zu wollen; vielmehr ist davon auszugehen, daß der Nomade *dienstespezifisch* auswählen können muß, welche Dienste er aus welchem Netz von welchem Server beziehen will. Beispiel: Ein Nomade möchte unter Beibehaltung seiner e-Mail-Adresse den *mail service* nach wie

vor aus seinem Heimatnetz beziehen, während er sicherlich auf einen *print service* im gastgebenden Netz zugreifen will. In Kooperation mit der gastgebenden Organisation müssen also Dienste im gastgebenden Netz identifiziert werden, die möglichst äquivalent zu den „gewohnten“ Diensten im Heimatnetz sind. Ein schwierigeres Thema ist der *file service*. Aufgrund der heute meist noch geringeren Datenübertragungsraten und hohen Kosten in Weitverkehrsnetzen kann für den Nomaden eine Mischform sinnvoll sein: Durch das gastgebende Netz wird der Nomade mit Standardapplikationen der jeweiligen Umgebung versorgt, während er ausgewählte Arbeitsdateien z.B. von einem File-Server in seinem Heimatnetz beziehen kann. Um dem Nomaden Zugriff auf Dienste im Heimatnetz zu erlauben, müssen in der Regel zwei Firewall-Systeme durchdrungen werden, nämlich das Firewall-System des gastgebenden Netzes und des Heimatnetzes. Insbesondere das Firewall-System des Heimatnetzes muß dafür Zugriffe zulassen, die „normalerweise“ strikt unterbunden werden. Außerdem sollen Dienste benutzer- und dienstespezifisch zur Verfügung gestellt werden. Der Nomade muß gemeinsam mit seinem Gastgeber und dem Administrator des Heimatnetzes verabreden, auf welche Weise ein Zugriff auf welche Dienste erfolgen kann und soll. Die benutzten Sicherheitsparameter (Authentifizierung, Verschlüsselung, ...) hängen vom Benutzer, seinem Aufenthaltsort und dem genutzten Dienst ab. Entsprechende Festlegungen müssen vielmehr kooperativ von den beteiligten Parteien im Sinne der mehrseitigen Sicherheit [7] vorgenommen werden. Nur so können die Sicherheitsinteressen aller beteiligten Parteien durchgesetzt werden. Des weiteren stellen sich mit dem Gastarbeiter-Szenario Managementprobleme, die sich auf das Auffinden von Diensten, der Verwaltung von Zugriffsrechten und auf die Steuerung der anzuwendenden kryptographischen Mechanismen beziehen.

3 Lösungskonzepte

Im Folgenden werden zwei Lösungsansätze untersucht: eine konventionelle Client/Server-Lösung und ein Ansatz, der sich mobile Agenten zu nutze macht.

3.1 Konzept für eine Client/Server-basierte Lösung

Zur Herstellung einer dienstespezifischen Zugangsmöglichkeit für den Nomaden zu Diensten in seinem Heimatnetz werden zum einen die Firewall-Systeme des gastgebenden Netzes und des Heimatnetzes um kryptographische Funktionen zur Erreichung der dargestellten Schutzziele erweitert (*Nomadic Security Gateways*), zum anderen wird in die Kommunikation zwischen Client (im gastgebenden Netz) und Server (im Heimatnetz) ein Paar von zwei weiteren Instanzen eingeschaltet: ein allgemeiner *Proxy*, der auf dem System des Nomaden installiert ist, und ein *Proxy Client* im *Nomadic Security Gateway* des Heimatnetzes. Insgesamt ergibt sich durch diese Anordnung eine Architektur mit drei Schichten. Auf der Diensteschicht befindet sich der für Client/Server-Systeme übliche Austausch zwischen *requests* und *responses*. Auf der darunter liegenden Schicht findet eine Kommunikation zwischen dem Client auf dem Gastarbeitsplatz und dem *Proxy Client* im Heimatnetz des Nomaden statt. Durch die Einführung des *Proxy Client* wird sichergestellt, daß der

Nomade auch solche Server in seinem Heimatnetz erreichen kann, die „von außen“ nicht sichtbar sind, also z.B. interne WWW-Server, interne News-Server usw. Der *Proxy Client* agiert als Stellvertreter des Nomaden im Heimatnetz: Da er sich innerhalb des Heimatnetzes befindet, kann er auch interne Server ansprechen. Auf der dritten Schicht findet der eigentliche Nachrichtentransport statt. Der im Gastarbeitsplatz angesiedelte *Proxy* sorgt dafür, daß die ins Heimatnetz gerichteten *requests* mit Authentifizierungsinformation zur Auswertung in den beiden *Nomadic Security Gateways* versehen werden. Zur Erreichung der Schutzziele Vertraulichkeit, Integrität und Authentizität werden *requests* und *responses* im gastgebenden Netz und im Internet über *Security Associations* gemäß IPsec [5] transportiert.

Der *Proxy Client*, der als integraler Teil dieses *Nomadic Security Gateway* betrachtet wird, hat weiterhin die Aufgabe, die vom Gastarbeitsplatz erzeugte Authentifizierungsinformation auszuwerten und – wie oben dargestellt – einen *request* an den richtigen Server im Heimatnetz weiterzuleiten. Weiterhin werden *responses* vom *Proxy Client* in das gastgebende Netz zurückgeleitet, und zwar an den *Proxy* des Gastarbeitsplatzes. Durch die Einschaltung der Kommunikation über Proxies wird die angestrebte Dienstespezifität erreicht, obwohl auf der Netzwerkschicht die dienstunspezifischen Mechanismen von IPsec verwendet werden. Der Gast muß die Bereitstellung der von ihm jeweils benötigten Dienste mit einer entsprechenden Instanz in seinem Heimatnetz aushandeln. Dazu wird ein zu entwickelndes Management-Protokoll benötigt. Im Zuge der über dieses Protokoll vorzunehmenden Aushandlung werden die genannten Proxies instantiiert. Bei der Entwicklung der Client/Server-basierten Lösungen kann auf eine Vielzahl von Standards zurückgegriffen werden. Die wichtigsten sind IPsec [5] und die damit verbundenen Management-Protokolle.

3.2 Konzept für eine Lösung mit mobilen Agenten

Um mit Hilfe von Agenten [1], [2], [4], [8] die Dienste des Heimatnetzes nutzen zu können, ist es nötig, daß der Nomade eine Agenten-Laufzeitumgebung auf seinem Rechner installiert. Diese Umgebung erlaubt es dem Nomaden, Agenten zu starten, zu konfigurieren, mit einem Auftrag zu versehen und an eine Laufzeitumgebung innerhalb des Heimatnetzes zu schicken. Da das Heimatnetz sowie das gastgebende Netz jeweils über ein Firewall-System mit dem Internet verbunden bzw. von diesem getrennt sind, ist es ohne weiteres nicht möglich, Daten zwischen diesen Netzen zu übertragen. Daher ist es erforderlich, einen Tunnel zwischen den beiden geschützten Netzen herzustellen, um den Agenten-Laufzeitumgebungen die Kommunikation zu gestatten. Dieser Kommunikationskanal wird von den Laufzeitumgebungen benötigt, um Verwaltungsinformationen auszutauschen und den Agenten die Migration zu erlauben. Im Heimatnetz befindet sich wenigstens eine Laufzeitumgebung für Agenten, die den Agenten Zugang zu internen Diensten bietet. Der Einsatz von Agenten erlaubt eine sehr flexible und differenzierte Dienstnutzung. Dies ist einer der großen Vorteile des Agentenparadigmas. Zu den Nachteilen, die der Einsatz von Agenten mit sich bringt, gehören die sich ergebenden Sicherheitsrisiken, da mit Agenten aktive Elemente in den geschützten Bereich des Intranets gelassen werden. Es muß verhindert werden, daß externe Angreifer die Agenten-Laufzeitumgebungen nutzen, um „feindliche“ Agenten in ein geschütztes Netz zu schicken und sich damit Möglichkeiten zu erschließen, die bei Beschränkung auf eine Client/Server-Kommunikation durch das Firewall-System verwehrt wären. Im *nomadic computing*-

Szenario kann man diese Gefahren dadurch ausschließen, daß zwischen den beteiligten Netzen nur gegenseitig zertifizierte Agenten zugelassen werden. Weiterhin wird durch Authentifizierung sichergestellt, daß Verbindungen nur zwischen autorisierten Laufzeitumgebungen aufgebaut werden. Digitale Signaturen machen Manipulation von Agenten erkennbar und erlauben es, vertrauenswürdige Agenten zu kennzeichnen. Des weiteren schützt Verschlüsselung den Kommunikationskanal zwischen den Laufzeitumgebungen vor dem Einblick oder der Manipulation durch Angreifer aus dem Internet als auch aus dem gastgebenden Netz.

4 Fazit

In diesem Artikel wurden verschiedene Lösungsansätze vorgestellt, die jeweils Vor- und Nachteile aufweisen. Beiden Lösungen ist gemein, daß ein Mechanismus geschaffen werden muß, der autorisierten Benutzern das Überwinden von mehreren Firewall-Systemen gestattet. Ebenso ist bei beiden Lösungen ein administratives Regelwerk und Software zu dessen Durchsetzung nötig, welche den Umfang der Ressourcennutzung und deren Sicherheitsparameter benutzer- und dienstspezifisch festlegen. Die hier vorgestellten technischen Konzepte sollen in einem *nomadic computing*-Testbed praktisch realisiert werden, das für Demonstrationen und Evaluierungen zur Verfügung steht. Dabei soll vor allem ein Management von Zugriffsmöglichkeiten für beide Lösungsansätze unter den Prämissen der mehrseitigen Sicherheit geschaffen werden.

Literatur

- [1] Bradshaw, J.M.: *Software Agents*. Cambridge (Mass.) u.a. (MIT Press) 1997, ISBN 0-262-52234-9.
- [2] Franklin, S., Graesser, A.: Is it an Agent or just a Program?: A Taxonomy for Autonomous Agents. In: *Proceedings of the Third International Workshop on Agent Theories, Architectures, and Languages*. Springer 1996.
- [3] Hagen, L., Breugst, M., Magedanz, Th.: *Impacts of Mobile Agent Technology on Mobile Communication System Evolution*. IEEE Personal Communications, vol. 5, no. 4 (August 1998), pp. 56–69.
- [4] Jennings, N.R., Wooldridge, M.J.: *Agent Technology*. Berlin u.a. (Springer) 1998, ISBN 3-540-63591-2.
- [5] Kent, S., Atkinson, R.: *Security Architecture for the Internet Protocol*. RFC-2401, 1998.
- [6] Kleinrock, L.: *Nomadic Computing and Communications*.
elektronisch: <http://bob.nap.edu/readingroom/books/whitepapers/>
- [7] 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.
- [8] Vigna, G. (Ed.): *Mobile Agents and Security*. (Springer) 1998, ISBN 3-540-64792-9.