Aspekte standortübergreifender mobiler Kommunikationsinfrastrukturen

Christian Grimm, Denis Göhr, Stefan Piger

Lehrgebiet Rechnernetze und Verteilte Systeme (RVS)
Universität Hannover
Schlosswender Straße 5
D-30159 Hannover
{grimm,goehr,piger}@rvs.uni-hannover.de

Abstract: Der vorliegende Beitrag stellt unterschiedliche Anforderungen dar, die sich aus Sicht der Betreiber bei der Öffnung von Campusnetzen für die mobile Nutzung ergeben. Dabei wird beispielhaft sowohl der authentifizierte Zugang zu öffentlich zugänglichen Netzen (z. B. WLANs) auf dem Campus, wie auch der Zugang von entfernten Standorten zu abgesicherten Institutsnetzen betrachtet.

1 Einleitung

Eine Zielvorstellung von Ubiquitous Computing ist, dass sowohl der Zugriff auf Ressourcen als auch die Erreichbarkeit eines Teilnehmers im Netz unabhängig von dem jeweiligen Aufenthaltsort möglich ist. Das Spektrum der Ressourcen umfasst Server für herkömmliche (z. B. WWW, Mail, NFS, FTP) und neue Dienste (z. B. Gatekeeper für VoIP, MCU für Videoconferencing) sowie Peripheriegeräte (z. B. Drucker). Eine erhöhte Komplexität ergibt sich dann, wenn ein Teil der Ressourcen am aktuellen Aufenthaltsort, ein anderer Teil gleichzeitig in der originären Herkunft, wie z. B. dem eigenen Institutsnetz, genutzt werden soll. Der hohe Anspruch einer uneingeschränkt ubiquitären Nutzung stellt, unter Beachtung notwendiger Sicherheitsaspekte, erhebliche Anforderungen an die zugrundeliegenden Dienste und Netze. In dem vorliegenden Beitrag werden grundlegende Betrachtungen einer standortübergreifenden mobilen Kommunikationsinfrastruktur anhand von zwei Problemstellungen durchgeführt.

Tabelle 1 zeigt zunächst eine Gegenüberstellung der Zugangstechniken, die heute bzw. mittelfristig in öffentlichen Netzen und in Campusnetzen verwendet werden.

	öffentliche Netze	**Campusnetze**
Festnetz	xDSL, ISDN, Modem	Fast Ethernet
Funknetz	GSM, GPRS, UMTS	WLAN, Bluetooth

Tab. 1. Zugangstechniken in öffentlichen Netzen und Campusnetzen

Auch wenn ein Teil der aufgeführten Zugangstechniken bereits über sicherheitsrelevante Merkmale wie Verschlüsselung auf Link-Ebene oder Authentifizierung des Endgerätes verfügt, zeigt dieser Beitrag die Grenzen der derzeitigen Mobilität auf und belegt die Notwendigkeit übergreifender Ansätze insbesondere für eine nutzerbasierte Authentifizierung. Für die weiteren Betrachtungen stehen daher weniger die eigentlichen Zugangstechniken, sondern vielmehr Verfahren zur Verschlüsselung und Authentifizierung auf Campusnetzen im Vordergrund.

2 Verschlüsselung und Authentifizierung

Tabelle 2 fasst gängige Protokolle zusammen, über die eine Verschlüsselung auf den jeweiligen Ebenen eines TCP/IP-Stacks durchgeführt wird. Die eigentlichen Algorithmen zur Verschlüsselung, wie z. B. RC4, werden dabei nicht betrachtet.

Ebene	**Protokoll zur Verschlüsselung**
Anwendung	SSL, SSH (Port Tunneling)
TCP	–
IP	IPsec, PPTP
Medium	WEP, WEP2, TKIP (IEEE 802.11i), SAFER+

Tab. 2. Einordnung von Protokollen zur Verschlüsselung

Die auf Medium-Ebene aufgeführten Protokolle werden ausschließlich für Bluetooth und WLAN verwendet. Unter dem Standard 802.11i soll zukünftig die Verschlüsselung in WLANs unabhängig von dem Übertragungsverfahren festgelegt werden.

Neben der Verschlüsselung stellt die zuverlässige Authentifizierung der Nutzer eine weitere grundlegende Anforderung an eine mobile Infrastruktur dar. Die möglichen Ansätze für eine Authentifizierung zeigt Tabelle 3.

Ebene	**Authentifizierung**		
	von	**Protokoll**	**anhand**
Anwendung	Nutzer	SSL, SSH	Username/Password, Zertifikate, asymmetrische Schlüssel, One Time Password (OTP), Secure ID (SID)
TCP	–	–	–
IP	Endgerät	–	IP-Adresse
	Nutzer	IPsec	Username/Password, Zertifikate, asymmetrische Schlüssel, Preshared Keys
		PPTP	Username/Password
Medium	Endgerät	–	MAC-Adresse
	Nutzer	IEEE 802.1x	Username/Password

Tab. 3. Einordnung von Verfahren zur Authentifizierung

Zwei alternative Zugangsverfahren zu einem WLAN werden in Abb. 1 dargestellt. In WLAN1 erfolgt eine Authentifizierung auf dem Access Point über die MAC-Adresse oder nach IEEE 802.1x durch Abfrage von Username/Password. Der DHCP-Server weist dem Endgerät eine IP-Adresse aus dem privaten Netz zu, die über Network Address Translation (NAT) auf eine öffentliche Adresse abgebildet wird. In WLAN2 wird dagegen zuerst eine IP-Adresse vergeben, bevor für den Aufbau des IPsec- bzw. PPTP-Tunnels eine Authentifizierung vorgenommen werden kann. Daraus folgt, dass innerhalb WLAN2 bereits ohne Authentifizierung der Teilnehmer kommuniziert werden kann. Weiterhin ist zu beachten, dass für den Aufbau der Tunnel in WLAN2 die Klienten über die entsprechenden Protokollstacks in dem Betriebssystem verfügen müssen. Demgegenüber erfolgt die Authentifizierung nach 802.1x über die Treiber der Interfaces.

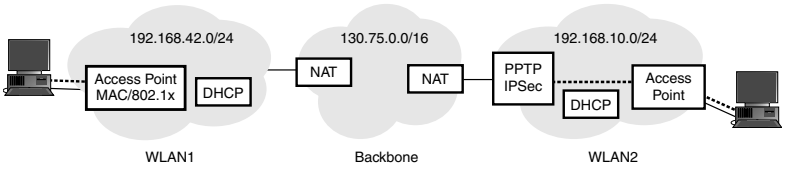

Abb. 1. Authentifizierter Zugang zu einem WLAN

Neben den dargestellten Verfahren kommt derzeit noch häufig eine Pseudo-Authentifizierung anhand von WEP-Schlüsseln zum Einsatz. Hierbei wird die Kenntnis der WEP-Schlüssel zur Verschlüsselung von Daten bereits als ausreichende Authentifizierung eines Teilnehmers angesehen. Da jedoch alle Teilnehmer über denselben, offengelegten WEP-Schlüssel verfügen müssen, eignet sich diese Methode, unabhängig von allgemeinen Sicherheitsbedenken gegenüber der WEP-Verschlüsselung, lediglich für spontane Meetings mit eingeschränktem Nutzerkreis. Eine Verwendung in kontrollierten öffentlichen Bereichen auf einem Campus scheidet dagegen aus.

3 Verwaltung von Informationen zur Authentifizierung

Aus der rechten Spalte von Tabelle 3 ergeben sich die Methoden, die für eine Authentifizierung verwendet werden können. Tabelle 4 enthält die Dienste, die die entsprechenden Informationen bereitstellen.

Authentifizierung	**Dienst**	
	lokal	**standortübergreifend**
Username/Password	NIS, Windows NT-Domäne	RADIUS, Diameter, COPS, Kerberos, Active Directory
Zertifikat	–	Public Key Infrastructure (PKI)
asymmetrische Schlüssel, Preshared Keys, OTD, SID	entsprechende Keyserver, z. B. ACE/Server	DNSsec (RFC 2065)
MAC-Adressen	Datenbank	–

Tab. 4. Bereitstellung von Informationen zur Authentifizierung

Die grundlegenden Prinzipien von Ubiquitous Computing fordern unter anderem, dass Nutzer nicht für jeden Zugang in ein fremdes Netz oder jeden Dienst unterschiedliche Kombinationen von Username/Password eingeben müssen. Auch aus Sicht der Betreiber ist es nicht erwünscht und langfristig sogar unsicher, dauerhaft vordefinierte Gast-Accounts bereitzuhalten. Daher ist mittelfristig eine standortübergreifende Infrastruktur zum Austausch von Informationen zur Authentifizierung erforderlich. Die rechte Spalte von Tabelle 4 führt die entsprechenden Dienste auf. Nach RFC 3127 eignen sich für eine gesicherte Übertragung von Username/Password derzeit jedoch lediglich Diameter (http://www.diameter.org/) und COPS (RFC 2748). Alternativ bietet sich die Authentifizierung über Zertifikate an, die jedoch den Betrieb einer PKI voraussetzt.

4 Zugang entfernter Teilnehmer

Abb. 2 zeigt die derzeit übliche Nutzung eines VPN-Gateways. Entfernte Teilnehmer (hier aus 3rd Site WLAN) schalten sich durch einen Tunnel über PPTP oder IPsec auf das VPN-Gateway auf. Hierdurch wird zum einen eine durchgehende Verschlüsselung zwischen Teilnehmer und VPN-Gateway auf IP-Ebene gewährleistet, zum anderen erhält der Teilnehmer eine IP-Adresse aus einem vorgegebenen Adresspool des Heimatnetzes.

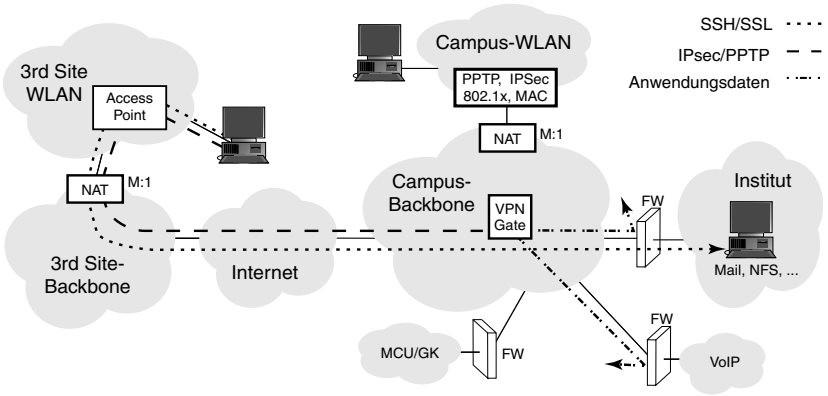

Abb. 2. Herkömmlicher Betrieb eines VPN-Gateways

Die an den Firewalls „abprallenden“ Verbindungen zeigen jedoch, dass auch diese Lösung Einschränkungen unterliegt. Auf Firewalls oder direkt auf den Servern in den Instituten werden in der Regel Zugriffe nur von Rechnern aus dem eigenen Institutsnetz gestattet, eine entsprechende Authentifizierung erfolgt anhand der IP-Adresse. Daher genügt die Vergabe von IP-Adressen aus einem öffentlichen Adresspool an entfernte Teilnehmer nicht, um an die Daten auf den Institutsrechnern zu gelangen.

Alternativ lässt sich die Firewall durch Tunnel auf Applikationsebene über SSL oder SSH durchbrechen. Das Tunneling von Firewalls stellt jedoch generell ein beträchtliches Sicherheitsrisiko dar, da eine Kontrolle der tatsächlich genutzten Applikationen sowie der übertragenen Daten verhindert wird. Das so genannte Port Forwarding über SSH erfordert zudem einen Account auf dem Endsystem.

Eine analoge Betrachtung kann auch für die Nutzung zentraler Dienste, wie z. B. Voice over IP oder Videoconferencing, durchgeführt werden. Kennzeichnend für diese Dienste ist, dass auch die Erreichbarkeit entfernter Teilnehmer aus dem Heimatnetz von Interesse ist. Entfernte Teilnehmer müssten sich hierfür auf dem Callmanager im Heimatnetz registrieren, um mit Hilfe von Softphones auf ihren Notebooks telefonieren zu können und unter ihrer bekannten Rufnummer erreichbar zu sein. Der Zugang zu den Servern in einer VoIP-Umgebung ist jedoch ebenfalls durch Firewalls geschützt, um nur registrierten Nutzern den Zugang zu der VoIP-Umgebung zu gestatten. Eine mobile Nutzung des VoIP-Dienstes wird unter den genannten Umständen daher unmöglich.

Ein erweitertes Konzept zum Einsatz von VPN-Gateways zeigt Abb. 3. Ausgehend von dem VPN-Gateway werden weitere Tunnel zu den Firewalls etabliert, so dass auch entfernte Teilnehmer mit vorgegebenen IP-Adressen aus dem Institutsnetz arbeiten können.

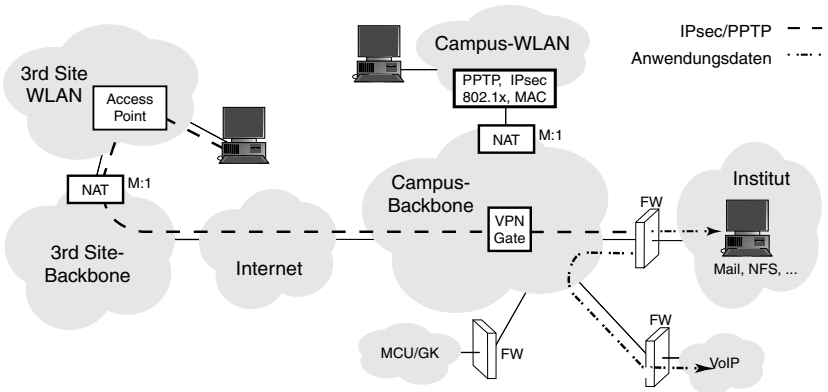

Abb. 3. Erweiterte Nutzung von VPN-Gateways

Das abgebildete Verfahren wurde am RVS erfolgreich prototypisch für den Einsatz auf dem Campus der Universität Hannover erprobt. Als VPN-Gateway kam ein Cisco VPN Concentrator 3030 zum Einsatz, die Firewall wurde durch einen Paketfilter mit FreeS/WAN (http://www.freeswan.org/) als Tunnelpunkt realisiert.

5 Zusammenfassung

Die aufgeführten Betrachtungen zeigen, dass auch mittelfristig keine einheitliche und einfach nutzbare mobile Kommunikationsinfrastruktur im Internet zur Verfügung stehen wird, die allen Anforderungen bezüglich Mobilität, Sicherheit und Komfort für Nutzer und Administratoren gerecht werden kann. Einen wesentlichen Baustein stellen dabei standortübergreifende Dienste zum Austausch von Informationen zur Authentifizierung dar. Dabei stehen nicht technischen Schwierigkeiten, sondern organisatorische Herausforderungen im Vordergrund. Um die Bildung von Insellösungen zu vermeiden, erscheint eine zentrale Koordinierung unumgänglich. Dagegen ist eine weitere Anforderung mobiler Nutzung, die Durchleitung entfernter Teilnehmer in die Institutsnetze, anhand der hier vorgestellten prototypischen Implementierung bereits mit vertretbarem Aufwand lösbar.