Mobile Virtuelle Private Netze

Prof. Dr. Torsten Braun, braun@iam.unibe.ch, und Marc Danzeisen, danzeis@iam.unibe.ch, Institut für Informatik und Angewandte Mathematik, Universität Bern

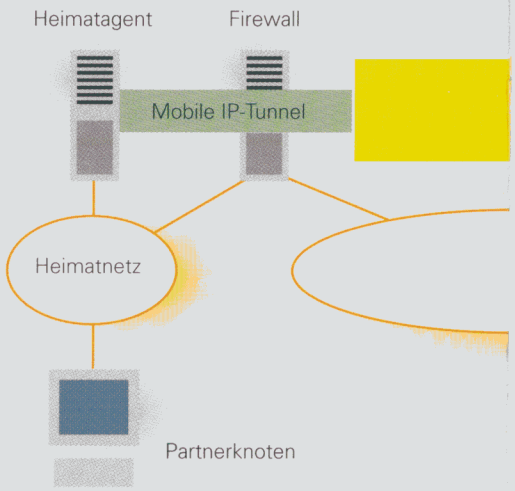
Drahtlose lokale Netze erlauben die Mobilität von Studierenden und Dozierenden innerhalb eines Hochschul-Campus. Um die Mobilität zwischen verschiedenen Hochschulen zu ermöglichen, sind IP-Protokollerweiterungen wie Mobile IP oder IP Security notwendig, falls mobile Benutzer auf durch Firewalls oder Paketfilter geschützte virtuelle private Netze ihrer Heimatuniversität zugreifen wollen. Der Artikel geht auf Mobile IP und IP Security ein und beschreibt einen prototypisch implementierten Lösungsansatz.

Motivation

Immer mehr Hochschulen installieren drahtlose lokale Netze (wireless local area networks, WLANs) flächendeckend auf dem Campus, um mit tragbaren Rechnern ausgestatteten Studierenden und Dozierenden den Zugang zum lokalen Hochschulnetz bzw. dem Internet zu ermöglichen. Ein grosses Problem ist dabei die Sicherheit: Zunächst ist zu vermeiden, dass Daten und Passwörter in Klartext über ein drahtloses Netz übertragen werden. Ausserdem sind zugriffsberechtigte Benutzer zu identifizieren, um ihnen die Kommunikation über drahtlose Netze zu gestatten. Dabei sollten die Benutzer einerseits im Idealfall auf dieselben Ressourcen zugreifen können, wie wenn sie sich an einem ans Festnetz angeschlossenen Arbeitsplatzrechner im Pool-Raum oder im Büro befinden würden, andererseits muss aber sichergestellt werden, dass nur berechtigte Benutzer die dazu notwendigen Kommunikationsdienstleistungen in Anspruch nehmen dürfen. So lernt im drahtlosen Netz der ETH Zürich (http://wireless.ethz.ch) ein Rechner seine IP-Adresse über das Dynamic Host Configuration Protocol (DHCP). Der Rechner, von dem aus sich ein(e) Studierende(r) per TELNET oder SSH auf einem Server erfolgreich anmeldet, erhält dann für eine beschränkte Zeit Zugriff auf das ETHZ-Netz. Voraussetzung für die Netzbenutzung ist ein entsprechender Account auf dem Server.

Zukünftig besteht jedoch zunehmender Bedarf, nicht nur den lokalen Studierenden und Dozenten, sondern auch Besuchern anderer Universitäten den drahtlosen Zugriff auf das Hochschulnetz zu ermöglichen. Beispiele sind Studierende, welche sich als Austauschstudenten oder Gasthörer einzelner Vorlesungen temporär auf dem Campus aufhalten, oder Forscher, die im Rahmen von Kooperationsprojekten zu Arbeitssitzungen oder längeren Forschungsaufenthalten eine Partneruniversität besuchen und dabei permanent auf die Rechen- und Datenressourcen ihrer Heimatuniversität Zugriff haben wollen. Demgegenüber sehen sich immer mehr Hochschulen gezwungen, Firewalls, Paketfilter und virtuelle private Netze (virtual private networks, VPNs) zu installieren, um ihre Netze gegenüber Sicherheitsangriffen von aussen oder vor unberechtigtem Zugriff auf zu schützende Daten zu sichern.

Wünschenswert wäre jedoch, dass sich z.B. die Studierende der Universität Bern, die sich in der Pause zwischen zwei Vorlesungen mit ihrem Laptop gerade in einer Cafeteria der ETH Zürich aufhält,



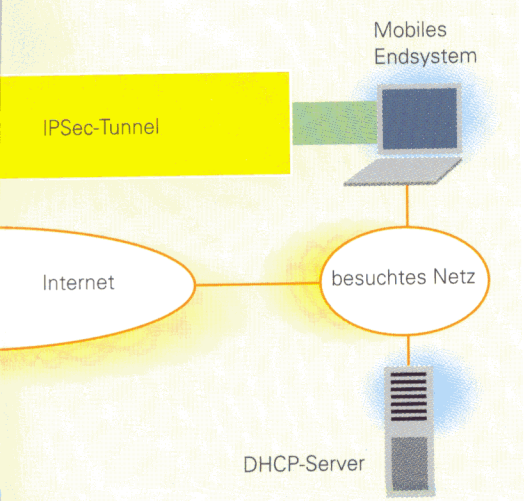
mit einem Labor-Server in einem Paketfilter-geschützten VPN der Universität Bern verbinden könnte, um ihre Praktikumsaufgaben zu bearbeiten. In der geschäftlichen Welt würde ein entsprechendes Beispiel darin bestehen, dass ein Berater während eines Kundenbesuchs über das drahtlose Netz des Kunden und das Internet auf einen Firewall-geschützten Server innerhalb des Firmen-VPNs zugreifen möchte. Zur Lösung dieser nicht trivialen Probleme existieren bereits standardisierte Internet-Protokolle. Hierbei sind insbesondere Mobile IP zur Unterstützung der Mobilität sowie die IP Security-Protokollfamilie zur Unterstützung sicherer Kommunikation über das Internet zu nennen.

IP Security

Die IP Security-Protokollfamilie – kurz IPSec – bietet im wesentlichen die folgenden Funktionalitäten: Authentifizierung durch den Authentication Header (AH), Verschlüsselung mit optionaler Authentifizierung durch die Encapsulating Security Payload (ESP) sowie sicheren Schlüsselaustausch durch Internet Key Exchange. AH und ESP können dabei entweder in einem Transport- oder Tunnel-Modus arbeiten. Im Tunnel-Modus wird das gesamte ursprüngliche Paket als Nutzlast für die Verschlüsselung und die Authentifizierung betrachtet und mit einem neuen IP-Header zu einem neuen IP-Paket ergänzt. Das ursprüngliche IP-Paket wird in diesem Fall über einen IP-Tunnel übertragen. Beim Transport-Modus werden die zusätzlichen Authentifizierungs- und Verschlüsselungsinformationen an den IP-Header bzw. an das Paketende angehängt.

Typischerweise generieren Sender und Empfänger über Schlüsselaustauschprotokolle geheime, symmetrische Schlüssel oder diese werden manuell konfiguriert. Bei der Verschlüsselung werden die Daten mit Hilfe des Schlüssels durch den Sender chiffriert, der Empfänger stellt mit einer Umkehroperation die ursprünglichen Daten wieder her. Ein möglicher Angreifer, welcher den Datenverkehr zwischen Sender und Empfänger abhört, kann dann nur die chiffrierten Daten erkennen. Zur Authentifizierung berechnet der Sender mit dem Schlüssel und den Paketdaten die Authentifizierungsdaten und fügt diese in den Authentication Header ein. Der Empfänger führt genau dieselben Operationen über die empfangenen Daten aus und vergleicht berechnete und empfangene Authentifizierungsdaten. Bei Übereinstimmung geht der Empfänger davon aus, dass die Daten unverfälscht übertragen wurden und von demjenigen Sender erzeugt wurden, welcher durch die Quell-IP-Adresse identifiziert wird und sich im Besitz des geheimen Schlüssels befindet.

Bei Secure Mobile IP werden für die Verbindung zwischen mobilem Endsystem und Heimatagent zwei Tunnel benutzt.



Mobile IP

Ziel von Mobile IP ist es, mobile Endsysteme dahin gehend zu unterstützen, dass diese weiterhin mit der Heimatadresse IP-Pakete senden und an die Heimatadresse gesendete IP-Pakete empfangen können. Die zentrale Komponente in Mobile IP ist der im Heimatnetz des mobilen Endsystems angesiedelte Heimatagent. Dieser muss ständig über den aktuellen Aufenthaltsort des mobilen Endsystems unterrichtet sein, damit an die Heimatadresse des mobilen Endsystems gesendete IP-Pakete an dieses weitergeleitet werden können.

Bei einem IP-Subnetzwechsel muss ein mobiles Endsystem zunächst z.B. über DHCP eine für den Aufenthalt in diesem Subnetz temporär gültige Adresse erlangen. Danach muss es sich beim Heimatagenten registrieren und dabei diesem die temporäre Adresse mitteilen. Diese Registrierung ist sehr sicherheitskritisch: Die Registrierungsnachricht enthält deshalb Authentifizierungsinformationen, um sicherzustellen, dass sie vom korrekten Endsystem stammt. Nach Erhalt der Registrierungsnachricht wird der Heimatagent sämtliche im Heimatnetz für das mobile Endsystem ankommende Nachrichten filtern und an dieses weiterleiten. Für das Weiterleiten wird das Original-Paket in ein neues IP-Paket eingepackt, wobei das neue Paket die Heimatagenten-Adresse als Quelladresse und die temporäre Adresse als Zieladresse enthält. Zwischen Heimatagent und mobilem Endsystem entsteht somit ein Mobile IP-Tunnel. In der Rückrichtung, d.h. vom mobilen Endsystem zu einem Partnerknoten, können Pakete grundsätzlich direkt geschickt werden, wobei dann die Heimatadresse als Quelladresse dient. Dies führt zum sogenannten Dreiecks-Routing, da die Pakete vom Partnerknoten an das mobile Endsystem und zurück einen Weg entlang des Dreiecks Partnerknoten -> Heimatagent -> mobiles Endsystem -> Partnerknoten nehmen. Dies kann jedoch gerade bei Firewalls oder Paketfiltern zu Problemen führen, da ein Paket vom mobilen Endsystem an den Partnerknoten eine topologisch nicht korrekte Quelladresse enthält. Daher sollten in solchen Szenarien Pakete auch in der Rückrichtung, also vom mobilen Endsystem aus, über einen Tunnel gesendet werden. Da man aber annehmen muss, dass der Partnerknoten Tunnels nicht unterstützt, werden Pakete vom mobilen Endsystem über einen Tunnel zum Heimatagenten geschickt, welcher diese an den Partnerknoten weiterleitet.

In gewissen Szenarien, z.B. wenn mobiles Endsystem und Partnerknoten nahe beieinander liegen, der Heimatagent aber weit entfernt ist, macht es Sinn, den Paketaustausch zu optimieren, um eine direkte Kommunikation ohne den Heimatagenten zu ermöglichen. Solche Optimierungen müssen jedoch vom Partnerknoten unterstützt werden.

Secure Mobile IP

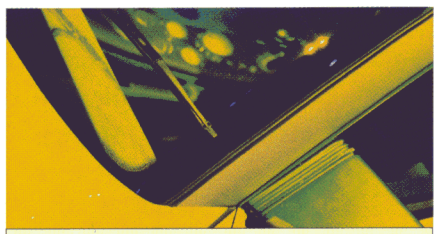
Im Rahmen des vom Schweizerischen

Nationalfonds geförderten Verbundprojekts «Advanced Network and Agent Infrastructure for the Support of Federations of Workflow Trading Systems» wurde eine auf IPSec und Mobile IP aufbauende Lösung für das Problem des Zugriffs auf Firewall-geschützte VPNs durch mobile Benutzer entwickelt und in Kooperation mit der Swisscom AG prototypisch implementiert.

Um mit IPSec sicheren Zugriff auf geschützte Netze zu gewähren, wird zwischen dem mobilen Endsystem und der Firewall des privaten Netzes ein IPSec-Tunnel aufgebaut. Nur wenn das Endsystem eine gültige Security Association mit der Firewall besitzt, werden die empfangenen Pakete entschlüsselt und in das private Netz weitergeleitet. Eine Security Association stellt dabei eine unidirektionale Beziehung zwischen Sender und Empfänger dar und ist durch verschiedene Parameter wie Authentifizierungs-, Verschlüsselungsalgorithmen, Schlüssel, Schlüssellebenszeiten usw. beschrieben. Sobald ein IPSec-Tunnel zur Firewall aufgebaut ist, können die authentifizierten Pakete wie die Mobile-IP-Registrierungsnachrichten durch diesen zum Heimatagenten in das private Netz gelangen. Bei diesem Konzept wird Mobile IP also durch einen IPSec-Tunnel gesichert. Es wird daher auch als Secure Mobile IP (SecMIP) bezeichnet. Das Bild zeigt die beiden bei SecMIP benutzten Tunnel.

Wenn sich das mobile Endsystem von einem WLAN-Zugang zum anderen bewegt und sich das IP-Subnetz ändert, braucht es eine neue in diesem Subnetz temporär gültige Adresse. Danach wird der bisherige IPSec-Tunnel durch einen neuen ersetzt und mit Hilfe der Mobile-IP-Registrierung dem Heimatagenten die neue temporäre Adresse mitgeteilt. Der Heimatagent ist dann in der Lage, an die Heimatadresse gesendete Pakete zu filtern und an das mobile Endsystem weiterzuleiten. Umgekehrt leitet der Heimatagent vom mobilen Endsystem empfangene Pakete an einen Server im privaten Netz exakt in derselben Form weiter, als ob sich das mobile Endsystem im Heimat-VPN befinden würde.

Die SecMIP-Implementierung unterstützt verschiedene drahtlose Netztechnologien wie WLAN, HSCSD und GPRS. Die Implementierung kann dabei die bezüglich verschiedener Parameter (z.B. Bandbreite, Kosten) am besten geeignete Technologie bestimmen und die entsprechende Netzwerkkarte zum Aufbau der SecMIP-Verbindung in das Heimatnetz selektieren. Damit kann dem Benutzer eine beinahe uneingeschränkte und transparente Mobilität zur Verfügung gestellt werden. So kann der Gastdozent auch den lokalen Ethernet-Anschluss verwenden, um das Herunterladen seiner Datei zu beschleunigen, ohne sich erneut beim Datei-Server anmelden zu müssen. Mit SecMIP kann ein technologieübergreifender Zugang bereitgestellt werden. Durch die Verwendung von IPSec zwischen dem mobilen Endsystem und der Firewall wird eine von der benutzten Netztechnologie unabhängige Ende-zu-Ende-Sicherheit gewährleistet, was speziell bei Sicherheitsmängeln existierender drahtloser und drahtgebundener Netze wesentliche Vorteile bietet.



Glossar

AAA	Authentication, Authorisation and Accounting
AH	Authentication Header
DHCP	Dynamic Host Configuration Protocol
ESP	Encapsulating Security Payload
GPRS	General Packet Radio Service
HSCSD	High-Speed Circuit Switched Data
IP	Internet Protocol
IPSec	IP Security
LAN	Local Area Network
SecMIP	Secure Mobile IP
SSH	Secure Shell
TELNET	Terminal Emulation Network
VPN	Virtual Private Network
WLAN	Wireless LAN

Zusammenfassung und Ausblick

Die zunehmende Verfügbarkeit von WLAN-basierten Internet-Zugängen in Universitäten verbessert den Internet-Zugriff von mobilen Benutzern, aber auch im öffentlichen Bereich setzen sich solche Technologien immer mehr durch. Gerade an stark frequentierten öffentlichen Plätzen wie Bahnhöfen, Haltestellen oder Einkaufszentren gibt es bereits WLAN-Zugänge oder werden solche aufgebaut. Damit erhalten geschäftliche Anwender die Möglichkeit, über drahtlose Netzzugänge und das Internet auf ihr VPN zuzugreifen. Die oben beschriebene SecMIP-Lösung könnte zum Beispiel eingesetzt werden, um den sicheren Zugriff auf ein VPN an der Universität Bern über das drahtlose LAN an der ETH Zürich zu ermöglichen, vorausgesetzt die Studierende hat die Berechtigung, das ETH-WLAN zu benutzen. Dies erfordert aber ein vorheriges Registrieren beim Server der ETH. Denkbar wäre auch, dass der Server der ETH einen Server der Uni Bern kontaktiert, um die Berechtigung der Studierenden zu überprüfen. Geeignete Protokolle hierzu werden durch die IETF in der Arbeitsgruppe Authentication, Authorisation and Accounting (AAA) entwickelt. III

Mobile virtual private networks

Wireless local networks allow students and lecturers to roam within a university campus. However, IP protocol extensions such as Mobile IP and IP Security are required when mobile users want to access to firewall or packet filter protected virtual private networks at their home university. The article describes Mobile IP and IP Security and outlines a solution implemented as a prototype.