

Ein mehrseitig sicheres Abrechnungssystem für Wireless LAN Hotspots

Stephan Groß, Sabine Lein und Sandra Steinbrecher
Technische Universität Dresden
Fakultät Informatik
Institut für Systemarchitektur
D-01062 Dresden, Germany
{st.gross, sl15, steinbrecher}@inf.tu-dresden.de

Abstract: In jüngster Zeit nimmt die Verbreitung öffentlicher WLAN Hotspots immer mehr zu. Bisherige Systeme berücksichtigen jedoch den berechtigten Wunsch der Nutzer nach Schutz ihrer personenbezogenen Daten nur unzureichend. Wir stellen daher ein mehrseitig sicheres Abrechnungssystem vor, welches eine anonyme Hotspot-Nutzung ohne aufwändige Authentifizierung ermöglicht. Hierdurch wird sowohl die Erstellung von Nutzerprofilen erschwert als auch ein Roaming zwischen Hotspots unterschiedlicher Anbieter vereinfacht.

1 Einleitung

In den letzten Jahren hat sich immer mehr der Trend durchgesetzt, den Zugang zu elektronischen Diensten und Informationen jederzeit und überall verfügbar zu machen. Eine Möglichkeit hierfür bieten sogenannte Wireless LAN Hotspots, die an öffentlich zugänglichen Plätzen wie z.B. Flughäfen, Hotels und Bahnhöfen eine Verbindung mit dem Internet ermöglichen. Ungenügende Sicherheit gilt jedoch weiter als eines der entscheidenden Hemmnisse bei der Akzeptanz solcher Hotspots [BGM03]. In diesem Artikel stellen wir daher ein mehrseitig sicheres Abrechnungssystem für Wireless LAN Hotspots vor. Kapitel 2 fasst die Anforderungen an ein solches System aus Sicht der einzelnen Beteiligten zusammen. Danach gehen wir kurz auf die verschiedenen Abrechnungsarten in einem öffentlichen WLAN ein (Kapitel 3) bevor wir in Kapitel 4 unseren Entwurf beschreiben.

2 Anforderungen an ein sicheres Abrechnungssystem

Die an der Abrechnung der Nutzung von WLAN-Hotspots Beteiligten lassen sich in Dienstnutzer und Dienstbringer (bestehend aus Hotspot-Betreibern, Dienst Anbietern und Netzbetreibern) unterteilen. Die Hotspot-Betreiber werden im folgenden nicht weiter betrachtet, da sie nach unserer Definition lediglich die Lokalität für den Hotspot zur Verfügung stellen, während die technische Realisierung des Netzzugangs durch die Netzbetreiber er-

folgt. Von den Dienst Anbietern wird eine zentrale Abrechnungsinstanz zur Verfügung gestellt, um beispielsweise ein einfaches Roaming zwischen den Netzen unterschiedlicher Netzbetreiber zu ermöglichen. Die Grundlage des Systems bilden teilnehmerbezogene Kontextdaten, die für jede Kommunikationsverbindung erhoben werden. So muss sich ein Nutzer vor der ersten Nutzung eines Hotspots üblicherweise zunächst beim entsprechenden Dienstanbieter anmelden. Hierbei erhält er die erforderlichen Informationen für einen legitimen Zugang. Das In-Rechnung-Stellen der Hotspot-Nutzung erfordert eine Erfassung der jeweiligen Verbindungsdaten und ggf. eine nachträgliche Abrechnung gegenüber dem Dienstanbieter.

An den Schutz der verarbeiteten Daten stellen die Beteiligten je nach Interessenlage unterschiedliche Anforderungen. So wünscht der *Dienstanbieter* vorrangig eine sichere Abrechnung (inkl. Authentizität und Vertraulichkeit der Kontextdaten) sowie gleichzeitig eine Minimierung der anfallenden Kontextdaten. Dies ist beides auch im Interesse der *Dienstnehmer*. Zur Abrechnung des genutzten Dienstes benötigen sie zwar ein gewisses Maß an authentischen Verbindungsdaten, wodurch die Dienstanbieter ihnen gegenüber beobachtbar und Kontextdaten verkettbar werden. Je weniger Daten zur Bereitstellung und Abrechnung eines Dienstes jedoch anfallen, desto weniger kostet deren datenschutzgerechte Verarbeitung und Verwaltung. Wir nehmen im folgenden an, dass die geeigneten Maßnahmen eingesetzt werden, um Vertraulichkeit und Authentizität der vorhandenen Daten sicherzustellen. Damit bleibt der *zentrale Konflikt* im Sinne mehrseitiger Sicherheit zwischen dem Bedürfnis des Teilnehmers nach Minimierung der erhobenen Kontextdaten und dem gemeinsamen Wunsch von Dienstbringern und -nutzern nach Authentizität und Verbindlichkeit der Kontextdaten.

3 Analyse verschiedener Abrechnungsarten

Abrechnungsmöglichkeiten zur WLAN-Nutzung lassen sich unterscheiden nach dem Zeitpunkt der Zahlung in *Prepaid- und Postpaid-Abrechnung* (d.h. Zahlung vor oder nach Dienstanbieter), nach der Genauigkeit in *pauschale Abrechnung* (d.h. ein im voraus festgelegtes maximales Zeit- oder Volumenguthaben) oder *individuelle Abrechnung* (d.h. nur effektiv genutzter Umfang) sowie nach der Speicherung des Guthabens bei Prepaid-Verfahren in *zentrale Speicherung* (beim Dienstanbieter) und *dezentrale Speicherung* (lokal beim Nutzer). Je nach gewählter Abrechnungsart werden dabei die Schutzziele der beteiligten Akteure unterschiedlich gut berücksichtigt. Ein sinnvoller Kompromiss im Sinne mehrseitiger Sicherheit ist unserer Meinung nach die Entwicklung eines auf elektronischen Münzen basierenden Abrechnungssystems, bei dem der Dienstanbieter entsprechende Münzen ausgibt. Diese Münzen müssen nicht notwendigerweise unter der realen Nutzeridentität erworben werden. Stattdessen kann hierfür auch ein Pseudonym verwendet werden.

Ein derartiges WLAN-Abrechnungssystem kann in Identitätsmanagementsysteme [CK01] integriert werden, die die Verwaltung und den Wechsel von Nutzerpseudonymen zur Wahrung der Privatsphäre bieten, gleichzeitig aber Dienst Anbietern Zurechenbarkeit von in Anspruch genommenen Leistungen zu Pseudonymen garantiert. Zu diesen kann im Falle des Missbrauchs durch Identitätstreuhänder die zugehörige Nutzeridentität entlarvt werden.

Identitätsmanagement erlaubt unter einem Pseudonym die gleichen Aktivitäten auszuführen wie unter der eigenen Nutzeridentität, insbesondere die für Zurechenbarkeit erforderlichen Authentizitätsmaßnahmen. Voraussetzung pseudonymer Systeme ist immer eine zugrundeliegende anonyme Netzwerkstruktur, wie sie z.B. Mixe [Cha81] bieten. Um die Verkettbarkeit einzelner Transaktionen mit demselben Pseudonym auszuschließen, ist ein regelmäßiger Wechsel der Pseudonyme in genügend kleinen Abständen angebracht. Dies ist beispielsweise für jede Session an einem Hotspot bzw. Access-Point sinnvoll. Diesen Ansatz verfolgt auch die aus dem Mobilfunkbereich stammende Methode der temporären Pseudonyme [FJK⁺97].

4 Entwurf eines mehrseitig sicheren Abrechnungssystems

Abbildung 1 zeigt die Client-Server-Architektur unseres Systementwurfs. Die beteiligten Entitäten entsprechen dabei exakt den Partnern in dem allgemein beschriebenen Protokoll für elektronisches Geld nach Chaum [Cha83]. Der *Teilnehmer* entspricht dem Kunden, der sich die Münzen bei seiner Bank beschafft, um sie bei einem Händler einzulösen. Diese Aufgabe der Verwaltung einer elektronischen Geldbörse übernimmt die Instanz eines User-Clients auf seinem Endgerät. Der *Anbieter* entspricht der Bank, die signierte Münzen an den Kunden ausgibt sowie vom Händler übertragene Münzen verifiziert. Hierfür ist eine Instanz des Provider-Servers beim jeweiligen Anbieter zuständig. Der *Hotspot* entspricht dem Händler, welcher die Münzen entgegennimmt und sie von der Bank verifizieren lässt, um die Dienstleistung bereitzustellen. Demzufolge kontrolliert und überwacht eine Instanz des Access-Gateways die Bezahlung und den Zugriff auf das Internet am genutzten Hotspot.

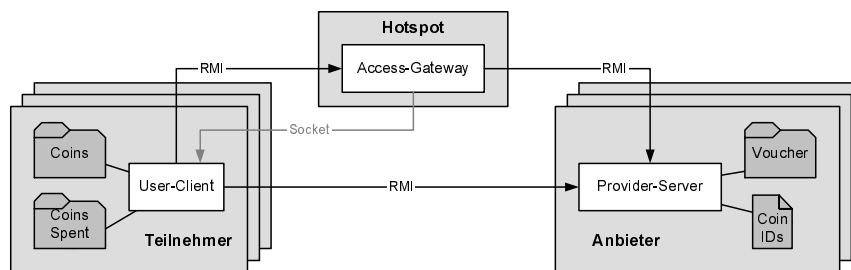


Abbildung 1: Grob-Architektur des Abrechnungssystems

Für den initialen (materiellen) „Wertaustausch“ erwirbt der Teilnehmer vom Anbieter einen Voucher. Dieser weist einen Code auf, der den Erwerb eines bestimmten Guthabens nachweist, das beim jeweiligen Anbieter (anonym) eingelöst werden kann. Die Kontrolle der Zugriffsberechtigung erfolgt über eine Firewall, welche dem Access-Point nachgeschaltet ist. Sobald eine vom Nutzer an das Gateway übertragene Münze vom jeweiligen Provider als gültig befunden und als »eingelöst« registriert wurde, wird dessen IP-Adresse

in der Firewall für die entsprechende Nutzungsdauer freigegeben.

Unsere prototypische Implementierung des Systems basiert auf einer Diffie-Hellman-Variante für Chaums blinde Signaturen, bei der die einzelnen Münzen allerdings keinen konkreten Münzwert aufweisen [Lau03]. Der modulare und objektorientierte Aufbau unserer Architektur ermöglicht jedoch die problemlose Erweiterung um weitere Verfahren zur Erzeugung und Überprüfung digitaler Münzen als auch zur Umsetzung variabler Münzwerte. Die Implementierung erfolgte in Java und verwaltet die einzelnen Münzen auf Nutzerseite mittels einer einfachen grafischen Benutzerschnittstelle in einer XML-Datenstruktur. Weitere Details zur Sicherheit und Nutzung des Systems finden sich in [Lei04].

5 Zusammenfassung und Ausblick

In dem vorliegenden Artikel haben wir dargelegt, dass bei den Beteiligten eines WLAN Hotspot-Szenarios weitgehend Einigkeit hinsichtlich zentraler Sicherheitsanforderungen besteht. Die Anonymität des Dienstanutzers steht jedoch scheinbar im Konflikt zum Wunsch unabdingbarer Abrechnungssicherheit des Diensteanbieters. Hierfür haben wir eine Lösung im Sinne mehrseitiger Sicherheit vorgestellt. Das von uns vorgeschlagene System verwendet dazu Chaums Konzept anonymer digitaler Münzen, ermöglicht aber auch den Einsatz anderer Verfahren. Darüber hinaus macht unser Ansatz eine aufwendige Authentifikation des Nutzers am Hotspot überflüssig, wodurch das Roaming zwischen Hotspots verschiedener Anbieter wesentlich vereinfacht wird.

Literatur

- [BGM03] Markus Buchwald, Klaus Greiber und Fritz Milosevic. Hotspot Report – Der Praxistest. Detecon International GmbH, November 2003.
- [Cha81] David Chaum. Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. *Communications of the ACM*, 24(2):84–88, 1981.
- [Cha83] David Chaum. Blind signatures for untraceable payments. In *Advances in Cryptology - Proceedings of Crypto '82*, Seiten 199–203, New York, 1983. Plenum Press.
- [CK01] Sebastian Clauß und Marit Köhntopp. Identity management and its support of multilateral security. *Computer Networks, Special Issue on 'Electronic Business Systems'*, (37), 2001.
- [FJK⁺97] Hannes Federrath, Anja Jerichow, Dogan Kesdogan, Andreas Pfitzmann und Otto Spaniol. Mobilkommunikation ohne Bewegungsprofile. In Günter Müller und Andreas Pfitzmann, Hrsg., *Mehrseitige Sicherheit in der Kommunikationstechnik: Verfahren, Komponenten, Integration*, Seiten 83–104. Addison Wesley Longman Verlag, 1997.
- [Lau03] Ben Laurie. Lucre: Anonymous Electronic Tokens v1.8. Bericht, Juni 2003. Erhältlich unter <http://anoncv.s.a.digital.co.uk/lucre> (Stand: 12.01.2005).
- [Lei04] Sabine Lein. Entwurf eines mehrseitig sicheren Abrechnungssystems für WLAN Hotspots. Diplomarbeit, Technische Universität Dresden, 2004.