# Modernes Identitäts- und Profildatenmanagement

## Fehlendes Sicherheitsbewusstsein erschwert die Nutzung von mobilen Multimediadiensten

Mario Hoffmann, Jens Heider, Max Larsson
Fraunhofer Institut für Sichere Telekooperation
Rheinstraße 75
D-64295 Darmstadt
[hoffmann|heider|larsson]@sit.fraunhofer.de

**Abstract:** „Wissen ist Macht" gilt im Internet gleichermaßen für Anwender als auch für Anbieter kontextabhängiger mobiler Multimediadienste. Auf der Benutzerseite erfordert der Zugriff auf eine Vielzahl von Einzeldiensten und der damit einhergehenden Profildatenflut ein kontrollierbares und transparentes Pseudonym-, Profildaten- und Identitätsmanagement. Gleichzeitig verlangen dieselben Daten auf der Anbieterseite ein zuverlässiges, vertrauenswürdiges Authentisierungs-, Autorisierungs- und Abrechnungssystem für erbrachte Dienstleistungen.

Dieser Beitrag diskutiert das oben skizzierte Spannungsfeld zwischen dem Schutz der Privatsphäre und der informationellen Durchdringung von Dienstanwendern, beginnend mit einer kurzen Bestandsaufnahme der heutzutage im Internet hinterlassenen, personenbezogenen digitalen Spuren. Besondere Beachtung findet dort eine neue Qualität, die erst durch die Nutzung von Location Based Services entsteht. Daran anschließend stellt Kapitel 3 konkrete Projekterfahrungen mit aktuellen Bedrohungen für die Integrität und Authentizität von Benutzerdaten und Dienstleistungen vor. Ein Fazit und eine Zusammenfassung runden diesen Beitrag ab.

## 1 Einleitung

„Wissen ist Macht" gilt im Internet gleichermaßen für Anwender als auch für Anbieter kontextabhängiger mobiler Multimediadienste. Seit der Einführung von multimedia-fähigen, tragbaren Endgeräten und aus frühen Modemtagen bekannten Übertragungs-geschwindigkeiten, gewinnt die Markteinführung – trotz der „Henne-Ei"-Problematik – für entsprechend angepasste Dienstportale, wie iMode von E-Plus oder Vodafone-live!, zunehmend an Performanz. Der Kontextabhängigkeit kommt dabei eine Schlüsselrolle zu. Für so genannte Location Based Services wird der Kontext beispielsweise durch den gegenwärtigen Ort und ggf. noch die aktuelle Tageszeit bestimmt. Darüber hinaus wächst die Bedeutung des semantischen Rahmes eines Dienstabrufs, wie im Falle der Unterscheidung eines dienstlichen oder privaten Kontextes.

Die Inanspruchnahme von Dienstportalen und von abonnierten Einzeldiensten erfordert aufgrund der damit einhergehenden Profildatenflut gleichermaßen – ob per Single-Sign-

On oder nicht – ein kontrollierbares und transparentes Pseudonym-, Profildaten- und Identitätsmanagement. *Kontrollierbar*, weil sich in Zeiten der Globalisierung der Speicherort und die weitere Verwendung von personenbezogenen Daten zunehmend sowohl der Kenntnis als auch der Einflussnahme des Nutzers entziehen. *Transparent*, weil die Verwaltung von personenbezogenen Daten auf der Benutzerseite einerseits nachvollziehbar und andererseits benutzerfreundlich – d.h. ohne erkennbaren Mehraufwand – möglich sein muss.

Gleichzeitig verlangen dieselben Daten auf der Anbieterseite nach einem zuverlässigen und vertrauenswürdigen Authentisierungs-, Autorisierungs- und Abrechnungssystem (AAA) für erbrachte Dienstleistungen. Die elektronische Speicherung und maschinelle Auswertung von Benutzerdaten, Surfverhalten und Verbindungsdauer führen jedoch über den eigentlichen Abrechnungszweck hinaus zu überaus detaillierten Benutzer- und Gruppenprofilen. Wie viele von uns täglich auf das Neue erfahren müssen, werden diese hauptsächlich zur Marktanalyse und -steuerung, zu einem zielgerichteten Marketing und zur Beurteilung und Vorhersage von Einzelverhalten verwertet. Der immense Wert dieser Informationen und Analysen auch für Staatsorgane ist beispielsweise in den USA an einer bemerkenswerten Branche erkennbar (siehe dazu [Str03]).

In diesem Beitrag ist das oben skizzierte Spannungsfeld zwischen dem Schutz der Privatsphäre und der informationellen Durchdringung von Dienstnutzern zunächst Gegenstand einer kurzen Diskussion der heutzutage im Internet hinterlassenen, personenbezogenen digitalen Spuren. Daran anschließend stellt Kapitel 3 dann konkrete Projekterfahrungen mit aktuellen Bedrohungen für die Integrität und Authentizität von Benutzerdaten und Dienstleistungen vor. Ein Fazit und einige Empfehlungen runden diesen Beitrag ab.

## 2 Die Datensammlungen mobiler Multimediadienste

Schon heute sorgen intelligente Data-Mining- und Personalisierungswerkzeuge dafür, dass Anwender individuell auf sie zugeschnittene Dienstportale vorfinden, die weit über Hinweise der Form „Leser dieses Buches interessierten sich auch für ...“ hinausgehen. Zu diesem Zweck werden zwar schon seit Bestehen des Internets sowohl auf technischer Ebene als auch auf Anwendungsebene Daten bei der Nutzung des Internets zunehmend mit modernen Methoden des Data Mining gespeichert und verarbeitet. Seit jenem schicksalhaften 11. September 2001 erfährt das Thema jedoch zusätzlich eine gesellschaftspolitische Dimension, die staatlichen Behörden national unterschiedlich weitreichenden Zugriff auf personenbezogene Daten gestatten. Zu den bevorzugten Daten gehören:

- Verbindungsdaten, wie digitale Identität (IP-Adresse), Form und Dauer,
- Surfverhalten, wie Typ, Anzahl und die Reihenfolge angeklickter Inhalte, sowie die Verweildauer
- Informationen über das Betriebssystem, den verwendeten Browser sowie dessen Einstellungen und installierte Plugins

- Zugriff auf Benutzerkonten (in einfachen Fällen beinhalten diese den Namen, den Vornamen, die e-Mail-Adresse und die Kreditkartennummer)
- Verfolgung des Sessionmanagements mit Hilfe von Cookies
- Historie bestellter Güter mit Querverbindungen zu Kunden mit ähnlichem Profil
- Verfahren zur statistischen Marktanalyse
- Scannen von e-Mails nach Schlüsselwörtern

Siehe dazu auch [SH00a], [SH00b] und [SH03].

Im Falle des mobilen Zugriffs entsteht in Zukunft darüber hinaus eine neue Qualität von Profildaten, in dessen Verlauf die auf obige Art entstehenden detaillierten digitalen Profile durch die genaue Lokalisierung mobiler Endgeräte (z.B. bei Location Based Services) angereichert werden. Der digitalen Identität wird hiermit eine wichtige Größe der realen Welt hinzugefügt: der – bei Verwendung von GPS – bis auf wenige Meter genaue Aufenthaltsort zum Zeitpunkt der Dienstinanspruchnahme.

Um Missverständnissen und falschen Erwartungen an dieser Stelle vorzubeugen: es gibt keine totale Anonymität im Internet. Der Einsatz beispielsweise von Anonymisierern zur Verschleierung von IP-Adressen, die Sperrung von Cookies und Java-Skript oder die Wahl von zusammenhangslosen Pseudonymen führt zwar zu einer gewissen Anonymität, schließt jedoch die Nutzung von kostenpflichtigen Diensten von vornherein aus. Auch viele andere Webseiten sind unter diesen Bedingungen nur noch eingeschränkt empfehlenswert. Ein bestimmter Teil unserer Identität wird uns also immer auf unserer Reise durch das Internet begleiten und dort zurückbleiben. Diese Erkenntnis muss uns aber nicht davor zurück halten, mehr Kontrolle über das *wo, was, wann* und *wofür* einzufordern. Denn bei einem entsprechend großen Angebot gleichwertiger Dienste gibt es vielleicht einige, die sich mit weniger persönlicher Offenbahrung zufrieden geben.

Für modernes Profildaten- und Identitätsmanagement – gleich, ob beim Anwender, beim Dienstleister oder Zugangsbetreiber – fehlt jedoch gerade in Zeiten der zunehmenden Integration des Internets in mobile Endgeräte vieler Orten noch das entsprechende Bewusstsein und die Sensibilität gegenüber den zahlreichen Bedrohungspotentialen. Vom Missbrauch und der Kompromittierung personenbezogener Daten bis zur Umgehung der Abrechnung von kostenpflichtigen Diensten findet sich gegenwärtig noch die gesamte Bandbreite an sicherheitsrelevanten Szenarien. Zur Illustration erläutert das folgende Kapitel einige aus aktuellen Projektergebnissen abgeleitete prinzipielle Bedrohungs- und Missbrauchspotenziale sowohl für den Endanwender als auch für den Dienstanbieter und Mobilfunkbetreiber. Allzu präzise Beschreibungen fielen bedauerlicherweise den Vertraulichkeitsvereinbahrungen laufender Verträge zum Opfer.

# 3 Identitätsübernahme und Vertrauensverlust

Die Frage nach dem *wo* beruht für individuelles Identitäts- und Profildatenmanagement zur Zeit in den meisten Fällen auf dem Vertrauen in die Dienstanbieter bzw. die Mobilfunkbetreiber, die zunehmend in die Rolle des Dienstanbieters drängen, d.h. Profildaten werden irgendwo im Netz gespeichert (Alternativen zeigt [H03b]). Geht das Vertrauen wie im Falle kompromittierter persönlicher Daten verloren, wird dem Geschäftsmodell des Dienstanbieters schlimmstenfalls die Grundlage entzogen.

Eine wichtige vertrauensfördernde Maßnahme wäre die Gewährleistung der Authentizität der Identität des Anbieters gegenüber dem Benutzer, was aber beispielsweise das GSM-Netz auf rein technischer Ebene gar nicht leisten kann. Ist eine Authentifizierung gegenüber dem Benutzer nicht vorhanden oder kann diese – wie in Abschnitt 3.2 dokumentiert – leicht vorgetäuscht werden, kann der Benutzer nicht zwischen vertrauenswürdigen Diensten und manipulierten Angeboten unterscheiden. Gleich ob durch persönliches, finanzielles oder kriminelles Interesse motiviert, dient die Vortäuschung oder Übernahme der Identität eines Dienstanbieters für eine ganze Reihe von Benutzertäuschungen. Dass jedoch auch die neue Generation an leistungsfähigen Endgeräten ihren Beitrag hierzu leistet, zeigt zunächst der folgende Abschnitt.

## 3.1 Missbrauchspotentiale mobiler Endgeräte

Frühere Publikationen, wie [H02a], stellten bereits ausführlich die mangelnden Sicherheitsmechanismen bei mobilen Endgeräten und Übertragungswegen dar und kritisierten, dass Anwender oftmals in Eigenverantwortung zusätzliche Software und Hardware für ihren Schutz installieren müssen. Die folgenden Abschnitte beschränken sich aus diesem Grund auf neuere Untersuchungen, die insbesondere die aktive Dienstnutzung betreffen.

Moderne mobile Endgeräte bieten heute eine für den mobilen Benutzer kaum noch überschaubare Vielzahl von Funktionen und Merkmalen an. Mit der Leistungssteigerung der Einzelkomponenten wie Prozessor, Speicher und Display wurde die Grundlage zu komplexeren Funktionalitäten gelegt, wie das moderne Betriebssystem Symbian OS und eine integrierte Java Virtual Maschine (MIDP) zeigen. Im Gegensatz zu früheren Geräten mit einfachem Funktionsumfang, mit dem gerade einmal Telefongespräche geführt und SMS geschrieben werden konnten, entpuppen sich heutige Geräte – mitunter verborgen vor dem Benutzer – als Organisations- und Kommunikationswunder. GSM (in Form von GPRS/HSCSD) und – in Kürze – UMTS stehen im Mobilfunkbereich und alternativ dazu W-LAN und Bluetooth im Nahfunkbereich zur Verfügung, um eine Verbindung mit einem Mobilfunk-/Dienstbetreiber herzustellen oder direkt mit anderen Benutzern und Geräten Kontakt aufzunehmen. Wenngleich diese Übertragungstechnologien noch nicht ausreichen, um all die Hochglanzfunktionalitäten zu realisieren, die während des UMTS-Hypes von Marketingabteilungen dankbar aufgenommen wurden, für Missbrauch und Täuschung genügen sie längst.

Insbesondere durch den Trend zum frei programmierbaren mobilen Endgerät, entstehen für die Mobilfunkbetreiber und ihre Kunden weitere Sicherheitsprobleme bei der Nutzung der mobilen Portale. Aktuelle Smartphone Betriebssystemen wie Symbian 7.0 und Smartphone 2002 bieten nicht nur umfangreiche Programmschnittstellen zu den internen Endgeräte-Ressourcen, sondern ermöglichen auch den Zugriff auf die Kommunikationsfunktionen. Auch die zunehmende Integration von Java mittels MIDP und herstellerspezifischen Erweiterungen, zur Unterstützung aller Endgerätefunktionen, birgt in der Kombination mit den erweiterten Kommunikationsmöglichkeiten zu Diensten aus Onlineportalen und dem Internet die Gefahr der unbemerkten, unautorisierten Nutzung der Dienste zu Ungunsten des Anwenders.

Die so erweiterte Funktionalität der Endgeräte und die frei verfügbaren offene Programmierumgebungen bieten nicht nur Möglichkeiten zur Schaffung neuer Anwendungsgebiete. Sie stellen durch den steigenden Funktionsumfang, die Programmvielfalt und die damit verbundene Komplexität der Konfiguration und Nutzung den Benutzer vor das Problem bei steigendem Risiko nach wie vor selber für die Sicherheit des Endgeräts verantwortlich handeln zu müssen.

Ein weiterer Aspekt betrifft die Integration von Lokalisierungstechnologie. Diese für die präzise Nutzung von ortsbasierten Diensten notwendige und wünschenswerte Funktionalität wird momentan zum größten Teil durch die Mobilfunkbetreiber angeboten, die notwendigerweise ständig diejenige Funkzelle bestimmen können, in der sich Mobilfunkteilnehmer aufhalten. Wie bereits in Kapitel 2 angedeutet, erwächst daraus die Bedrohung für den Dienstnutzer, dass ehemals unabhängige Einzelaspekte zu einem Gesamtprofil geformt werden. Durch eine Hand laufen Gewohnheiten bei der Dienstnutzung, die Chronologie der physischen Aufenthaltsorte und die Abrechnung von kostenpflichtigen Diensten. Selbst Strafverfolgungsbehörden haben diese Möglichkeiten für sich erkannt und erstellen mit Hilfe von stillen SMS Bewegungsprofile von Verdächtigen ([Kre03]).

### 3.2 Benutzertäuschung durch fingierte mobile Dienste

Ein klassisches Vorgehen bei der Vortäuschung von falschen Identitäten ist die so genannte Man-in-the-Middle Attacke, bei der der Angreifer einem Nutzer die Identität des Zieldienstes sowie dem Dienst die Nutzeridentität vortäuscht, um die Interaktion mit dem Dienst mitlesen und manipulieren zu können. Möglich wird dies durch schwache oder nicht vorhandene Authentifizierung des Dienstanbieters, wie dies zurzeit in mobilen Netzen (insbesondere GSM) der Fall ist. Der Anwender muss in diesem Fall der Echtheit der Identität des Anbieters ohne Nachweis vertrauen. Die Netzbetreiber stützen sich in diesem speziellen Fall auf ihre geschlossenen Netze, die vor direktem Missbrauch durch Dritte von außen geschützt sind.

Der Angreifer muss seine Aktivitäten jedoch nicht innerhalb des geschützten, vom Mobilfunkbetreiber kontrollierten Bereichs durchführen. Durch die fehlende Authentifizierung kann ein Angreifer auf einem beliebigen externen Server durch die Erstellung von Diensten, die realen Diensten nachempfunden sind, den Benutzer bereits sehr

wirksam täuschen. Durch eine Umleitung eines Benutzers, z.B. über eine WAP-PUSH Nachricht oder manipulierte Verbindungseinstellungen, können wichtige Passwörter und Informationen ausgespäht werden. Begünstigt wird dies, da aus Platzgründen die URL, die zumindest einen Hinweis auf den Zielort geben könnte, in den wenigsten Fällen direkt angezeigt wird. Harmlos wirkende Links entfalten mitunter Potenziale, die man sonst nur aus der Outlook-Explorer-Liaison kennt.

Darüber hinaus kann der Benutzer durch das Vertrauen in die vorgetäuschte Identität zu Aktionen und Einstellungen veranlasst werden, die für die Benutzer zu weiteren Gefahren führen, für den Angreifer jedoch finanzielle Vorteile bieten können. Der manipulierte Dienst dient dann als Zwischenstation der Interaktion mit dem eigentlichen Dienst. Damit die Täuschung nicht auffällt, werden die eingegebenen Informationen – wie bei Man-In-The-Middle-Attacken üblich – an den realen Dienst übergeben, sodass die eigentliche Dienstnutzung erfolgen kann und der Nutzer nicht misstrauisch wird.

Zwar existieren oberhalb der Transportschicht Protokolle zur Authentifizierung, die z.B. die Verwendung von Server-Zertifikaten über HTTP und WAP ermöglichen, doch werden diese zurzeit in den Portalen der Mobilfunkbetreiber noch nicht eingesetzt. Auch bei aktuellen Erweiterungen wie WAP-PUSH, bei denen neben Textinformationen auch Verknüpfungen zu Online-Angeboten auf das Endgerät übertragen werden können, fehlt, wie auch schon der SMS, die Möglichkeit die Absenderidentität sicher festzustellen.

Eine andere Täuschung des Benutzers besteht mittels Trojanern bei denen eine Schadsoftware innerhalb einer Nutzsoftware versteckt ist, die zur Installation auf dem Endgerät angeboten wird. Die installierte Software kann nun mit Hilfe der immer umfangreicher werdenden Programmierschnittstellen der Endgeräte auch unbemerkt Aktionen innerhalb von Online-Diensten ausführen, die von den Diensten nicht von autorisierten Aktionen des Benutzers unterschieden werden können. Auch die Nutzung von Passwörtern für die Dienstnutzung schafft hier kaum Abhilfe, da diese abhängig vom verwendeten Endgerät und Betriebssystem durch die Schadsoftware ausgespäht werden können.

Wie man erkennt, halten also all die bekannten Attacken aus dem Internet nun Einzug auf mobile Endgeräte. Ganz allmählich dringt dieser Fakt nun auch zu Betreibern und Anwendern durch, die sich bisher noch auf ihre abgeschotteten Mobilfunknetze verlassen konnten. Das abschließende Kapitel beschreibt nun wenigstens noch einige Strategien, die sich mobile Anwender und Anbieter je nach persönlichem Sicherheitsbedürfnis zu Eigen machen können.

# 4 Fazit – Strategien für partielle Sicherheit und Datenschutz

Der vertraute Umgang mit dem mobilen Endgerät suggerierte bislang eine speziell gesicherte Umgebung auch beim Zugang zum Internet. Mit dem Einzug des Internet auf mobile Endgeräte ist es jedoch mit der in sich geschlossenen Mobilfunkwelt vorbei. Mobile Endgeräte können nicht länger als sicher angesehen werden.

Zur Nutzung von ortsbasierten Diensten bietet sich – trotz erhöhtem Konfigurationsaufwand – GPS als passive Lokalisierungsquelle an. Zusätzlich lässt sich, obwohl der Trend aus Sicht der Mobilfunkbetreiber in die andere Richtung führt, eine Erhöhung der Diversifikation von Teilidentitäten realisieren, indem man bei der Nutzung auf nicht zentral verwaltete Einzeldienste Wert legt – so, wie man es im Umgang mit dem Internet schon gewohnt ist. So können die oben beschriebenen Bedrohungspotenziale im Vorfeld zumindest verringert werden.

Spezifikationen zum Identitäts- und Profildatenmanagment – wie das Protokoll P3P – sind ein Schritt in die richtige Richtung. Hier definiert ein Dienst explizit, welche Daten benötigt werden und was mit ihnen geschieht. Wenn dies mit den Richtlinien des Benutzers konform ist, werden Informationen ausgetauscht. Wenn nicht, hängt es von den Einstellungen eines Identitätsmanagers ab, ob die Benutzung verweigert, ein Pseudonym verwendet oder beim Benutzer nachgefragt wird. Bisher fehlt diesem Ansatz noch der durchschlagende Erfolg, da auch hier die Einhaltung der Richtlinien vor allem auf Vertrauen beruht.

Bleibt zu hoffen, dass in naher Zukunft der Trend, mobile Endgeräte mit immer mehr Funktionen auszustatten, auch die Integration der Smartcard-Technologie – über die SIM und USIM hinaus – beinhaltet (vgl. [H03b]). Signierte und von entsprechenden Zertifizierungsinstanzen beglaubigte Dienstanbieter und Anwender würden einem erheblichen Teil der heutigen Unsicherheiten, die durch Benutzertäuschung und der Übernahme einer falschen Identität entstehen, bei der Nutzung mobiler Dienste Abhilfe verschaffen.

## Literaturverzeichnis


[H03a] Mario Hoffmann, „MOBILE – Eine mehrseitig sichere Plattform für Location Based Services“, Münchner Kreis – „Mobil mit digitalen Diensten“, Feb 2003, München

[H03b] Mario Hoffmann, „Mehrseitig sichere mobile Anwendungen - Smartcards zur sicheren Nutzung von Location Based Services“, OMNICard 2003, Jan 2003, Berlin

[H02a] Mario Hoffmann, „Mehrseitig sichere Location Based Services – Endgeräte, Übertragungstechnik und Anwendungen“, „Geoinformation mobil“, Hrsg.: Alexander Zipf, Josef Strobel, Okt 2002, ISBN 3-87907-373-2

[J03] Uwe Jendricke, „Sichere Kommunikation zum Schutz der Privatsphäre durch Identitätsmanagement“, Dissertation, RHOMBOS-Verlag, Berlin, 2003, ISBN 3-930894-69-6

[SH00a] Christiane Schulzki-Haddouti (Hrsg.), „Vom Ende der Anonymität – Die Globalisierung der Überwachung”, Heise-Verlag, 2000, ISBN 3-88229-185-0

[SH00b] Christiane Schulzki-Haddouti, „Von wegen anonym ...“, Deutschland Radio, http://www.dradio.de/magazin/001122-01.html

[SH03] Christiane Schulzki-Haddouti, „Digitale Spuren”, Telepolis-Artikel, 31. Jan 2003, http://www.heise.de/tp/deutsch/inhalt/te/14052/1.html

[Str03] Matthias Streitz, „Big Brother Inc., die Gewinnmaschine”, Spiegel-Online, 07. Mai 2003, http://www.spiegel.de/wirtschaft/0,1518,247596,00.html

[Kre03] Stefan Krempl, Heise-mobil, „Staatsanwaltschaft kritisiert "Spitzel-SMS" der Polizei“, http://www.heise.de/mobil/newsticker/data/tol-06.04.03-001/