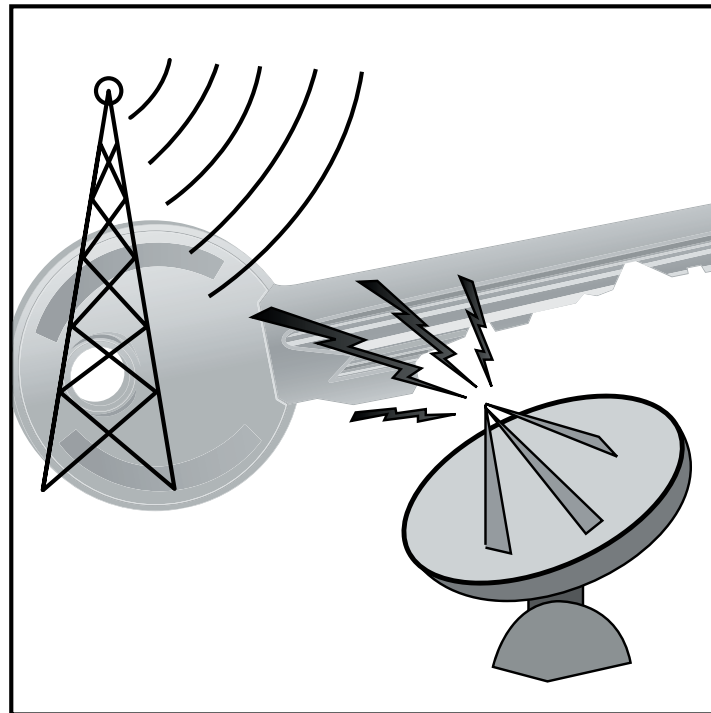


Sicherheitsaspekte öffentlicher Mobilfunknetze

Teil 1: Gefährdungen im öffentlichen Mobilfunk

von Dominik Zöller, Dr. Michael Wallbaum, Dr. Frank Imhoff



Der öffentliche Mobilfunk hat sich im Laufe seiner fünfzigjährigen Geschichte stark gewandelt. Vom handvermittelten, analogen A-Netz der 50er Jahre hin zum heutigen UMTS stieg die Leistungsfähigkeit der Netze im selben Maß wie ihre Beliebtheit. Mit der Einführung von GSM Anfang der 90er Jahre explodierten die Nutzerzahlen in ungeahntem Maß. Fallende Gebühren, die durch die

günstigere digitale Netz-Technologie und die Entwicklung von Endgeräten als Massenware möglich wurden, trugen ebenso zu dieser Entwicklung bei, wie der steigende Mobilitätsdruck auf Arbeitnehmer wie Privatpersonen.

Mittlerweile ist das Mobiltelefon zur weltweiten Nummer Eins in Sachen Sprachkommunikation avanciert. Gerade im ge-

schäftlichen Umfeld hat der Mobilfunk den Arbeitsalltag revolutioniert. Nie zuvor waren Mitarbeiter - unabhängig von ihrem Aufenthaltsort - derart in ihre Unternehmen eingebunden wie heute. Die Vorteile liegen auf der Hand. Anstelle starrer Terminplanungen kann jederzeit flexibel umdisponiert werden.

Schwerpunktthema



Dominik Zöllner ist seit 2006 Berater bei der ComConsult Beratung und Planung. Während seines Studiums konzentrierte er sich auf die Themengebiete der Kommunikationsnetze und der Betriebssysteme. Bei ComConsult ist er vorwiegend mit der Evaluierung, Planung und Ausschreibung professioneller Unified Communications, Kollaborations- und Video-konferenz-Systeme befasst.



Dr. Michael Wallbaum ist Senior Consultant der ComConsult Beratung und Planung GmbH. Er blickt auf jahrelange Projekterfahrung in Forschung, Entwicklung und Betrieb im Bereich mobiler Kommunikationssysteme, Voice-over-IP und Groupware zurück. Zu diesen Themenbereichen sind von ihm zahlreiche Veröffentlichungen und Buchbeiträge erschienen.



Dr. Frank Imhoff ist technischer Direktor und Senior Consultant der ComConsult Beratung und Planung GmbH. Er blickt auf jahrelange Erfahrung in Forschung, Entwicklung und Betrieb von lokalen Netzen, Voice-over-IP, Wireless Local Area Networks sowie anderen Mobilfunk- und Telekommunikationssystemen zurück. Zu diesen Themenbereichen sind von ihm bereits zahlreiche Veröffentlichungen erschienen und Seminare betreut worden.

Sicherheitsaspekte öffentlicher Mobilfunknetze Teil 1: Gefährdungen im öffentlichen Mobilfunk

Der Mitarbeiter steht immer in Kontakt zu seinem Heimatstandort oder der koordinierenden Zentrale. Kein Unternehmen kann es sich heute noch leisten, auf diese Flexibilität zu verzichten. Im Nachsatz zur Sprachkommunikation wurden in der Unternehmenswelt sehr bald auch mobile Datendienste populär. Heute ist der mobile Zugriff auf Email, Internet und Unternehmensdaten fast selbstverständlich. (siehe Abbildung 1)

Doch was ist der Preis der Mobilität? Wie steht es um den Schutz der Privatsphäre? Welche Eingriffe in die vermeintlich vertrauliche Unterhaltung am Mobiltelefon sind technisch möglich, welche gar erlaubt? Welche Konsequenzen hat die mobile Datenkommunikation für das Unternehmensnetz? Und wie kann die Vertraulichkeit technisch sichergestellt werden? Dieser zweiteilige Artikel soll die Risiken des Mobilfunks beleuchten und Anregungen geben, um eine sichere Nutzung zu ermöglichen. Der vorliegende erste Teil beschäftigt sich hierbei mit technischen Aspekten von Netzen und

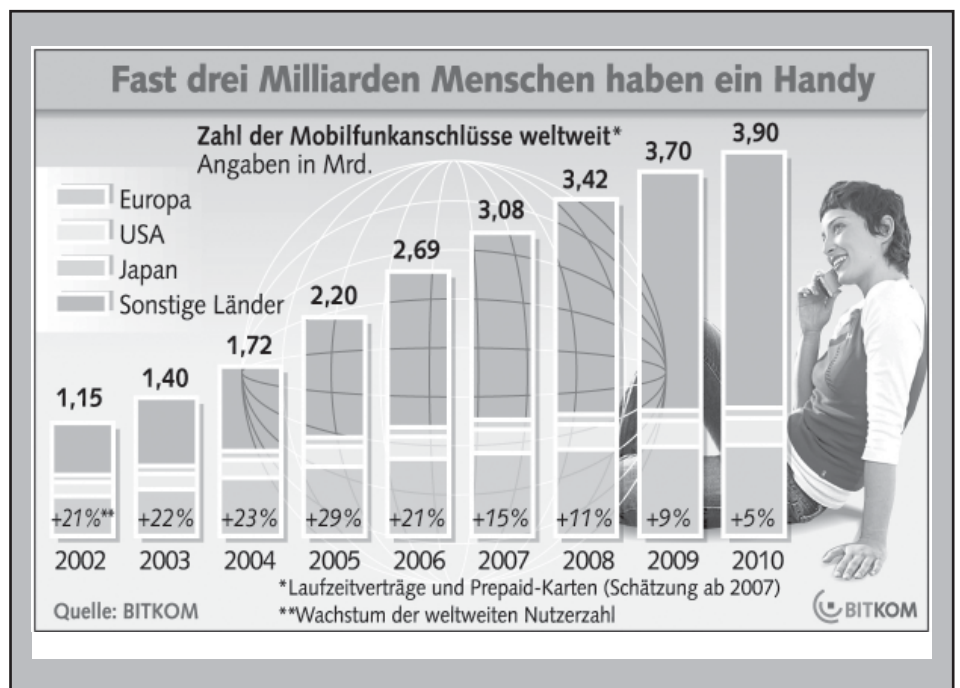


Abbildung 1 Weltweit steigen die Nutzerzahlen der Mobilfunknetze (Quelle: BITKOM)

Sicherheitsaspekte öffentlicher Mobilfunknetze - Teil 1

Diensten und den hieraus erwachsenen Gefährdungen für Privatsphäre und Datensicherheit. Im zweiten Teil werden dann Anregungen zur organisatorischen und technischen Absicherung mobiler Kommunikationsinfrastruktur gegeben.

Die Netze

Mobilfunknetze, wie wir sie heute kennen, basieren in erster Linie auf dem GSM-Standard. Zunächst nach der mit der Standardisierung befassten Group Spéciale Mobile benannt, steht GSM heute für „Global System for Mobile Communications“. Im GSM Standard sind sowohl die eingesetzten Verfahren zur Modulation der Übertragungskanäle und der Sprachcodierung als auch die grundlegende Architektur eines GSM-Netzes festgeschrieben. Zur Funkübertragung werden - in international verschiedenen Ausprägungen - die Frequenzbänder 900 MHz, 1800 MHz und 1900 MHz verwendet. Die verschiedenen Frequenzbänder werden anhand von Zeit- und Frequenzmultiplexing in einzelne Kanäle unterteilt (siehe Abbildung 2). So kann jede Basisstation (Base Transceiver Station, BTS) im BSS gleichzeitig einer Vielzahl von Endgeräten den Zugriff ermöglichen.

Ein GSM-Netz besteht aus verschiedenen Subsystemen, die unterschiedliche Aufgaben übernehmen. Das Base Station Subsystem (BSS) dient dabei den Nutzern als Zugriffspunkt. Es verbindet das Mobile Endgerät mit dem Network Subsystem (NSS) und dem Operations and Support System (OSS). Während das OSS alle

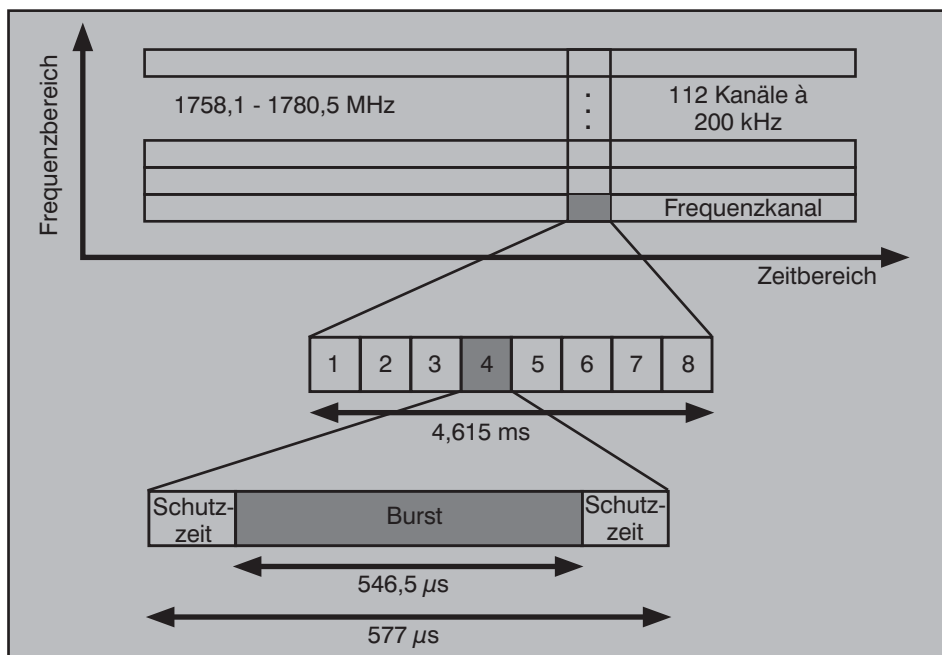


Abbildung 2: Kanalmodellierung bei GSM – Acht Zeitscheiben pro Frequenzkanal

für die Verwaltung eines Mobilfunknetzes notwendigen Komponenten enthält, bildet das NSS den eigentlichen Kern eines GSM-Netzes. In ihm werden Teilnehmer verwaltet, Authentisierungs- und Ortsinformationen gespeichert sowie die Vermittlung sämtlicher Sprachverbindungen vorgenommen.

Datendienste als Innovationstreiber

Um auch Datenanwendungen auf mobilen Endgeräten zu ermöglichen, wurde

der Standard nachträglich um ein weiteres Subsystem erweitert, das so genannte GPRS Core Network. General Packet Radio Service (GPRS) ist ein Standard, der das GSM-Netz zu paketvermittelter Datenübertragung befähigt. Das GPRS Core Network stellt dabei mittels entsprechender Gateways die Anbindung zu den Datennetzen anderer Provider und dem Internet her. (siehe Abbildung 3)

Die zunehmende Nutzung mobiler Datendienste zeigt aber bald die Grenzen des

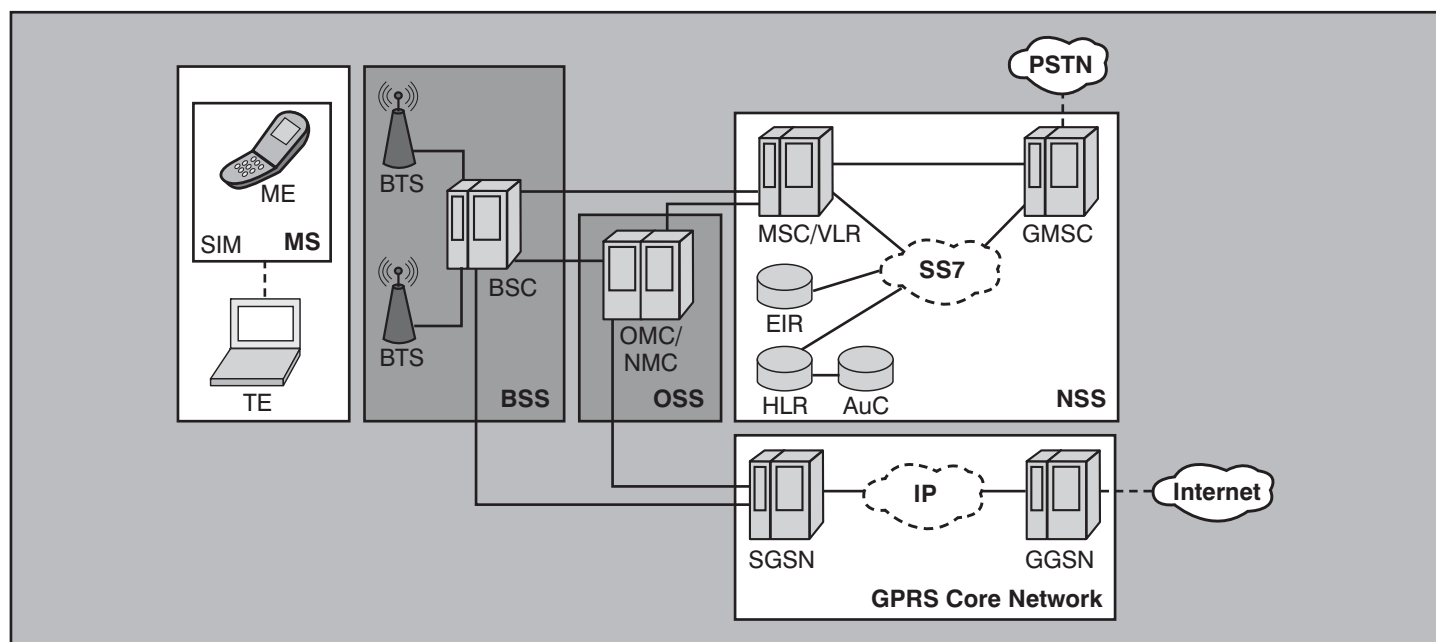


Abbildung 3: Architektur eines GSM- und GPRS-Netzes

Sicherheitsaspekte öffentlicher Mobilfunknetze - Teil 1

GSM-Standards auf. Mit einer Nettodatenrate von acht bis 20 kbit/s pro Kanal und begrenzter Kanalbündelung (maximal vier Kanäle für den Downlink) ergibt sich ein Maximaldurchsatz von 80 kbit/s pro Endgerät – ohne jegliche Fehlerkorrektur! Hinzu kommt, dass pro Funkzelle – abhängig von der Lizenz des Netzbetreibers – nur um die 100 Trägerfrequenzen mit je 8 Kanälen zur Verfügung stehen. Das begrenzt die Gesamtdatenrate auf in der Praxis höchst illusorische 16 MBit/s – für alle in der Zelle befindlichen Endgeräte. In Zeiten hochbitratiger Internetverbindungen muten diese Werte geradezu antiquiert an. Da verwundert es nicht, wenn es – insbesondere in Ballungsräumen – zu Engpässen kommt. Eine Weiterentwicklung der zweiten Generation der Mobilfunknetze (2G), wie GSM und GPRS auch genannt werden, war also dringend notwendig.

Attraktive Krücke

Die erste Stufe der Weiterentwicklung ist das so genannte EDGE, was für „Enhanced Data Rates for GSM Evolution“ steht. Ziel dieses Verfahrens war es, mit minimalen Änderungen am GSM-Netz eine Erhöhung der Datenraten zu erzielen. Hierzu setzt EDGE ein anderes Modulationsverfahren ein, was wahlweise zum GSM-spezifischen Verfahren verwendet werden kann und das – je nach verwendetem Codierungsschema – rund die dreifache Datenrate ermöglicht. Dabei bleiben Architektur und Multiplexing-Verfahren des GSM-Netzes unangetastet, was die Kosten für einen Ausbau niedrig hält. In vielen Fällen ist die Aufrüstung mit einem Software-Update erledigt. Daher rührt auch die häufige Bezeichnung 2.5G für EDGE, das in der Einführung preiswert und deshalb als Fallbacklösung beliebt ist, wenn sich der Ausbau von Netzen der dritten Generation wirtschaftlich (noch) nicht rechnet.

Da geht noch was!

Die aktuelle, dritte Generation der mobilen Kommunikationsnetze stellt das Universal Mobile Telecommunications System (UMTS) dar. UMTS bedient sich eines grundlegend anderen Multiplexing-Verfahrens, was die Extrapolation sich überlagernder Funksignale ermöglicht. Hierdurch ist keine Aufteilung in starre Kanäle mehr notwendig und die Datenrate kann auf Werte zwischen 144 und 384 kbit/s pro Endgerät erhöht werden. Im Gegensatz zu EDGE basiert UMTS nicht auf den herkömmlichen GSM-Netzen. Auch wenn sich architekturelle Gemeinsamkeiten finden, so unterscheiden sich doch sowohl die verwendeten Frequenzbänder (1920,3-1979,7 MHz und 2110,3-2169,7 MHz) als

auch die Übertragungstechnik grundlegend voneinander. Des Weiteren wurde in der Architektur der gestiegenen Bedeutung mobiler Datendienste Rechnung getragen, was sich im Zusammenführen der paketvermittelten und der leitungsvermittelten Dienste im UMTS Core Network niederschlägt.

Durch beständige Weiterentwicklung der Modulations- und Codierungsverfahren wurden die Datenraten der UMTS-Netze nochmals gesteigert, so dass heute mit dem High Speed Download Access (HSDPA) und dem High Speed Uplink Access (HSUPA) zwei Verfahren zur Verfügung stehen, mit denen Datenraten von momentan bis zu 3,6 MBit/s möglich sind. Diese als 3.5G bezeichneten Techniken stellen eine weitere Evolutionsstufe auf dem Weg zu zukünftigen Mobilfunknetzen dar. Der nächste Schritt wird das vom Standardisierungsgremium 3GPP (Third Generation Partnership Project) zum Kronprinz erklärte High Speed Orthogonal Frequency Division Multiplexing Packet Access (HSOPA) sein. Hinter diesem schwerfällig anmutenden Titel verbirgt sich eine Technologie, die maximale Datenraten in der Größenordnung moderner WLANs und darüber hinaus verspricht. All diesen Verfahren ist gemein, dass sie auf der Netzarchitektur des UMTS-Standards basieren und zu diesem kompatibel sind. Ob dies auch für die zukünftige vierte Generation der Mobilfunknetze gelten wird, ist unklar. Heiße Anwärter darauf, sich als Basistechnologie für diese zukünftigen Netze zu qualifizieren, sind neuere WLANs

der 802.11- und 802.16-Familien. Welche Technik hier schließlich das Rennen machen wird, liegt in der Hand der Arbeitsgruppe 3GPP Long Term Evolution (3GPP LTE).

Evolution? Aber sicher!

Das Tuning der Mobilfunk-Netze für schnelle Datendienste ist nur ein Aspekt von UMTS. Vielmehr wurden sowohl die Architektur als auch einzelne, teils sicherheitsrelevante Funktionen des Standards einer Generalüberholung unterzogen. Dabei zog man zum Teil die Konsequenzen aus bekannt gewordenen Sicherheitslücken des GSM-Standards und trug gleichzeitig dem - gerade im Geschäftsbereich - steigenden Bedarf an gesicherter Datenübertragung Rechnung.

Beispielhaft sieht man dies am Vergleich der eingesetzten Authentisierungs- und Verschlüsselungsverfahren. Zur Authentisierung wird vom Netzbetreiber eine Zufallszahl generiert und an das zu authentisierende Endgerät geschickt. Sowohl auf Seiten des Netzbetreibers als auch auf Endgeräteseite wird hieraus ein 32 Bit langer Wert berechnet. Dies geschieht nach GSM-Spezifikation anhand des Algorithmus A3. Im Endgerät ist hierfür die SIM-Karte zuständig, die neben dem für diese Berechnung zuständigen Prozessor auch den Subscriber Authentication Key Ki des Mobilfunkteilnehmers enthält. Dieser liegt auch auf Seiten des Netzbetreibers (im so genannten Authentication Center (AuC), einer Entität im NSS) vor und wird auf bei-

Jetzt Leser werden**Der Netzwerk Insider**

Der Netzwerk Insider erscheint 12 Mal im Jahr im PDF-Format und informiert Sie per eMail über die Hintergründe aktueller Netzwerk-Technologien. Jeden Monat werden zwei Themen gewählt, über die in ausführlicher Form topaktuelle Insider-Informationen gegeben werden. Der Netzwerk-Insider vertritt die Sichtweise von Technologie-Anwendern und bewertet Produkte und Technologien im Sinne der wirtschaftlichen und erfolgreichen Umsetzbarkeit in der täglichen Praxis. Durch seine strenge wirtschaftliche Unabhängigkeit (keine Hersteller-Anzeigen) kann er es sich leisten, Schwachstellen und Nachteile offen anzusprechen. Der Netzwerk-Insider ist bekannt für seine kritische, herstellerneutrale und fundierte Technologie-Bewertung.



Hier können Sie sich zum Netzwerk Insider kostenlos und ohne jede Verpflichtung registrieren lassen:

<http://www.comconsult-akademie.de/de/Registrierung.php>

Sicherheitsaspekte öffentlicher Mobilfunknetze - Teil 1

den Seiten mit in die Berechnung einbezogen. Nach erfolgreicher Berechnung sendet das Endgerät den Wert an das Authentication Center, wo ein Vergleich stattfindet. Stimmt das Ergebnis mit dem im AuC generierten Wert überein, gilt das Endgerät als erfolgreich authentisiert und darf sich am Netz anmelden. Nach demselben Verfahren wird anhand des Algorithmus A8 ein 64 Bit langer Sitzungsschlüssel generiert. Dieser wird dann von beiden Seiten zur Verschlüsselung von Sprach- und Datenverkehr auf der Luftschnittstelle eingesetzt. Die Verschlüsselung findet mit Hilfe von Algorithmus A5 statt, von dem verschiedene Varianten existieren. (siehe Abbildung 4)

An den oben beschriebenen Verfahren gibt es eine Reihe von Kritikpunkten:

- Der Subscriber Authentication Key ist ein so genanntes Shared Secret: Die Kenntnis dieses Schlüssels ermöglicht die Übernahme der Identität eines Mobilfunkteilnehmers. Wenn also das Network Subsystem unzureichend abgesichert ist, könnte ein Angreifer oder Innentäter Zugriff auf sämtliche Shared Secrets erhalten. Damit wäre er in der Lage, innerhalb des GSM-Netzes die Identität jedes beliebigen Kunden anzunehmen.
- Die Algorithmen A3 und A8 sind im GSM Standard nicht exakt festgeschrieben. Der Netzbetreiber kann eine „geeignete“ Implementierung wählen. Diese Idee stammt offensichtlich aus einer Zeit, als proprietäre Implementierungen noch als implizit sicher galten.
- Einige Varianten des zur Verschlüsselung verwendeten Algorithmus A5 sind unsicher. Variante A5/0 beispielsweise ist eine Platzhalter-Funktion, die überhaupt nicht verschlüsselt. Die Varianten A5/1 und A5/2 sind Stromchiffren, die heute als unsicher gelten. Da ein Wechsel der verwendeten Variante durch das Betreibernetz initiiert werden kann, ist eine zuverlässige Verschlüsselung nicht gewährleistet. Erst die im Zuge von UMTS auch für GSM standardisierte Variante A5/3 (auch Kasumi genannt) ist nach heutigem Stand der Technik als sicher anzusehen.
- Die Authentisierung ist einseitig: Zwar wird der mittels A3 generierte Wert vom Endgerät an das AuC geschickt und dort auf Richtigkeit überprüft. Umgekehrt findet eine solche Überprüfung aber nicht statt.

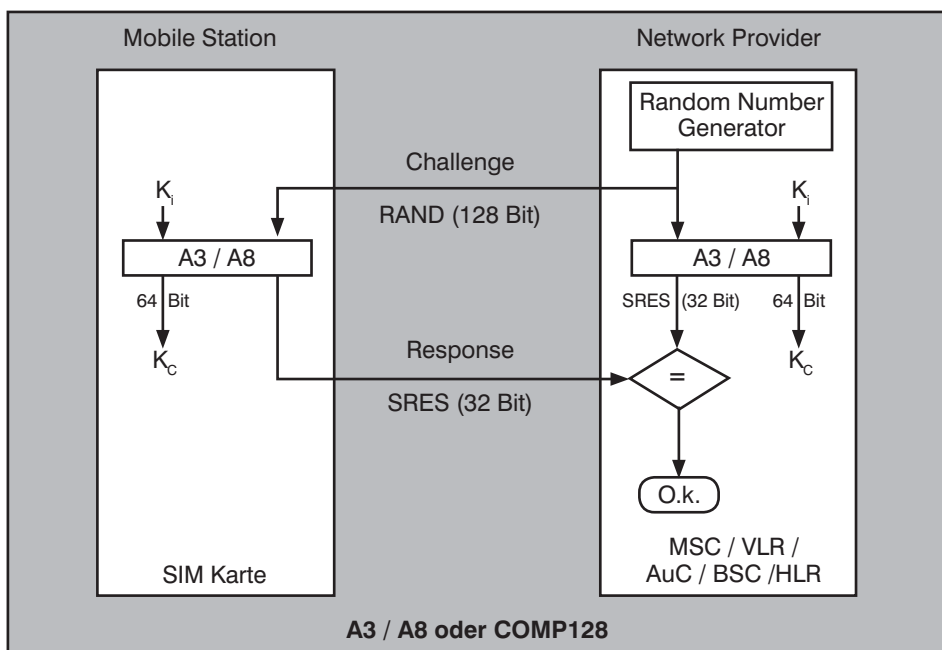


Abbildung 4: Authentisierung und Schlüsselgenerierung nach den Algorithmen A3 und A8

Der Grund für den letzten Kritikpunkt liegt auf der Hand: Beim Entwurf von GSM stand offensichtlich im Fokus, das Netz vor seinen Teilnehmern zu schützen. Es sollte sichergestellt werden, dass kein Teilnehmer sich unberechtigt Zugriff auf das Mobilfunknetz erschleicht und damit den kommerziellen Interessen der Netzbetreiber schadet. Auf die Idee, dass es nötig sein könnte, den Teilnehmer vor dem Netz zu schützen, kam zu diesem Zeitpunkt wohl niemand.

Catch me, if you can!

Ein Beispiel für einen Missbrauch dieser Schwachstelle ist der so genannte IMSI-Catcher. IMSI steht hierbei für International Mobile Subscriber Identity, also der weltweit eindeutigen Kennung des Mobilfunkteilnehmers. Das Prinzip ist einfach: Der IMSI-Catcher verhält sich gegenüber dem Endgerät wie die Basisstation eines Mobilnetzbetreibers. Durch erhöhte Sendeleistung „unterdrückt“ er das Signal der in der Umgebung befindlichen Basisstationen (BTS). Dadurch versucht das End-

Verbesserte Sicherheit durch UMTS

Authentisierung: Im Gegensatz zu GSM findet bei UMTS eine gegenseitige Authentisierung von Endgerät und Basisstation (Node-B) statt. Dadurch werden Man-in-the-Middle Attacken wirkungsvoll unterbunden.

Verschlüsselung: Während ursprünglich für GSM nur nicht offengelegte und - nachgewiesenermaßen - unsichere Stromchiffren (A5/1, A5/2) zur Verfügung standen, wurde im Zuge der Standardisierung von UMTS ein neuer Blockchiffre eingeführt. Der „KASUMI“ (japanisch „verschleierte“) genannte Algorithmus fand im Nachhinein als A5/3 auch bei GSM Verwendung. Aus Gründen der Abwärtskompatibilität kann aber auf alte, unsichere Verfahren zurückgegriffen werden.

Verschlüsselte IMSI: Im Gegensatz zu GSM findet die Übertragung der IMSI (International Mobile Subscriber Identity) niemals im Klartext, sondern immer in Form der verschlüsselten EMSI (Encrypted Mobile Subscriber Identity) statt. Das erschwert die Zuordnung von Kennung und Teilnehmer und das Fälschen der Teilnehmererkennung erheblich.)

Temporäre IMSI: Wie auch in neuen Releases des GSM Standard vorgesehen, wird im Laufe der Verbindung zum Mobilfunknetz die IMSI regelmäßig gewechselt. Was bei GSM die TMSI (Temporary Mobile Subscriber Identity) ist, nennt sich unter UMTS TEMSI (Temporary Encrypted Mobile Subscriber Identity). Das regelmäßige Durchwechseln der TEMSI erschwert die Entschlüsselung der EMSI zusätzlich.

Sicherheitsaspekte öffentlicher Mobilfunknetze - Teil 1

gerät, sich am IMSI-Catcher anzumelden. Dieser erhält so Kenntnis über die IMSI eines Teilnehmers. Ortung und Zuordnung der IMSI zu einer Person stellen dann kein Problem mehr dar. Außerdem können die Anmeldeinformationen vom IMSI-Catcher zur echten BTS durchgeleitet werden, er verhält sich also gegenüber dem Netzwerk wie ein Endgerät. So passieren alle relevanten Daten den IMSI-Catcher, statt direkt zwischen Endgerät und BTS ausgetauscht zu werden – eine klassische Man-in-the-Middle Attacke. Falls das Endgerät und die Basisstation es zulassen, kann die Verschlüsselung auf A5/0, also unverschlüsselte Übertragung zurückgefahren werden. Andernfalls können die mitgelesenen Informationen nach einer der bekanntgewordenen Angriffsmethoden auf die Stromchiffren A5/1 und A5/2 in Echtzeit entschlüsselt werden.

Für den behördlichen und nachrichtendienstlichen Einsatz eingeschränkt zulässig, ist der Betrieb solcher Geräte in Deutschland für Privatpersonen und Unternehmen untersagt. Aber zu glauben, ein Angreifer mit der notwendigen kriminellen Energie ließe sich hiervon abhalten, wäre mehr als blauäugig. Die notwendige Technik ist zwar alles andere als preisgünstig, aber je nach Ausführung ist sie teilweise sogar im europäischen Ausland legal zu beziehen – bequem per Internet und frei Haus. Was gerade im Bereich der Industriespionage mit einem abhörtauglichen IMSI-Catcher angerichtet werden kann, mag sich niemand gerne vorstellen. Gespräche sensiblen Inhalts zwischen Mitgliedern der Geschäftsleitung aufzeichnen? Ein Bewegungsprofil der Patrouille des Werkschutzes erstellen? Vertrauliche Geschäftsbeziehungen anhand sozialer Netze rekonstruieren? Mit dem Zugriff auf Teilnehmerkennungen und Ortsinformationen sind solche Attacken auf ein Unternehmen problemlos möglich.

All das würde verhindert, wenn sich die Basisstation ihrerseits gegenüber dem Endgerät authentisieren müsste. Dem wurde mit dem UMTS-Standard Rechnung getragen. Die Authentisierung des Endgeräts wird erst initiiert, wenn sich die Basisstation (in UMTS-Nomenklatur Node-B) anhand eines Authentication Token erfolgreich gegenüber dem Endgerät ausgewiesen hat. Das grundlegende Verfahren entspricht im Prinzip dem von GSM, ist aber durch die beidseitige Authentisierung deutlich sicherer. Zusätzlich werden personenbezogene Daten wie die IMSI niemals unverschlüsselt übertragen und können so nicht in die Hände eines Angreifers gelangen. Nach dem Aushan-

deln der Verbindung und Authentisierung anhand der Encrypted Mobile Subscriber Identity (EMSI) wird im Folgenden auf die TEMSI (Temporary EMSI) zurückgegriffen. Diese wird anhand von zufälligen Parametern zyklisch gewechselt, was ein Abhören und Orten des Nutzers zusätzlich erschwert. Die Aufgaben der SIM-Karte bei Authentisierung und Verschlüsselung übernimmt im UMTS-Standard das so genannte Universal Subscriber Identity Module (USIM), welches eine Teileinheit der Universal Integrated Circuit Card (UICC), der Nachfolgerin der herkömmlichen SIM-Karte, ist. Auch die Verschlüsselung wurde verbessert, der unter dem Namen Kasumi (japanisch für „verschleiert“) bekannte Algorithmus ist ein Blockchiffre, dessen Quellen komplett offen gelegt wurden. Er wurde unter dem Namen A5/3 nachträglich in den GSM-Standard aufgenommen.

Flashback

All diese Verbesserungen könnten die Luftschnittstelle nach heutigem Stand vor unbefugtem Zugriff schützen. Wenn da nicht das Problem der Abwärtskompatibilität wäre. Aus wirtschaftlichen Gründen erfolgte kein kompletter Austausch der bestehenden GSM-Infrastruktur durch UMTS-Technologie. Weder sind UICC und USIM flächendeckend im Einsatz, noch wurden alle BTS durch UMTS Node-B ausgetauscht. Selbst wenn dies kostenneutral zu realisieren wäre – ein Teil der Kunden verfügt zwar bereits über UMTS-fähige Endgeräte nutzt dieses Netz aber

für kaum mehr als gelegentliches Surfen. Die höheren Kosten schrecken viele Anwender gerade im privaten Bereich noch ab. Sicherheitsaspekte fallen bei Vertragsabschluss in der Regel kaum ins Gewicht. Auch wenn die Zahlen der UMTS-Nutzer beständig steigen (siehe Abbildung 5), ist ein Großteil der Verträge noch auf die Nutzung von GSM beschränkt.

So bleibt den Netzbetreibern nur eine Möglichkeit: Der Austausch der Infrastruktur wird stückweise vollzogen, so dass lange Zeit ein Parallelbetrieb notwendig ist. Viele der neuen Sicherheitsfeatures wurden auf diesen Mischbetrieb ausgelegt. Netz wie Endgeräte unterstützen gleichermaßen den Rückfall in alte GSM-Marotten. Dieser Sachverhalt wird sich erst ändern, wenn alle Kunden auf die neue UMTS-Technologie umgestellt wurden. Doch bis dahin wird vermutlich bereits ein Netz der vierten Generation im Aufbau begriffen sein. Wenn man davon ausgeht, dass in der Zukunft auch bei UMTS Sicherheitsmängel aufgedeckt werden, so stünde man hier erneut vor derselben Problematik.

Intelligente Infrastruktur

Auch wenn die Luftschnittstelle der Mobilfunkkommunikation natürlich besonderen Gefährdungen ausgesetzt ist: auch die fest verdrahtete Infrastruktur der Netzbetreiber bedarf eines kritischen Blicks. Welche Daten werden hier über den Kunden vorgehalten? Wer hat auf welche Daten Zugriff? Wie bereits erwähnt unterteilt sich

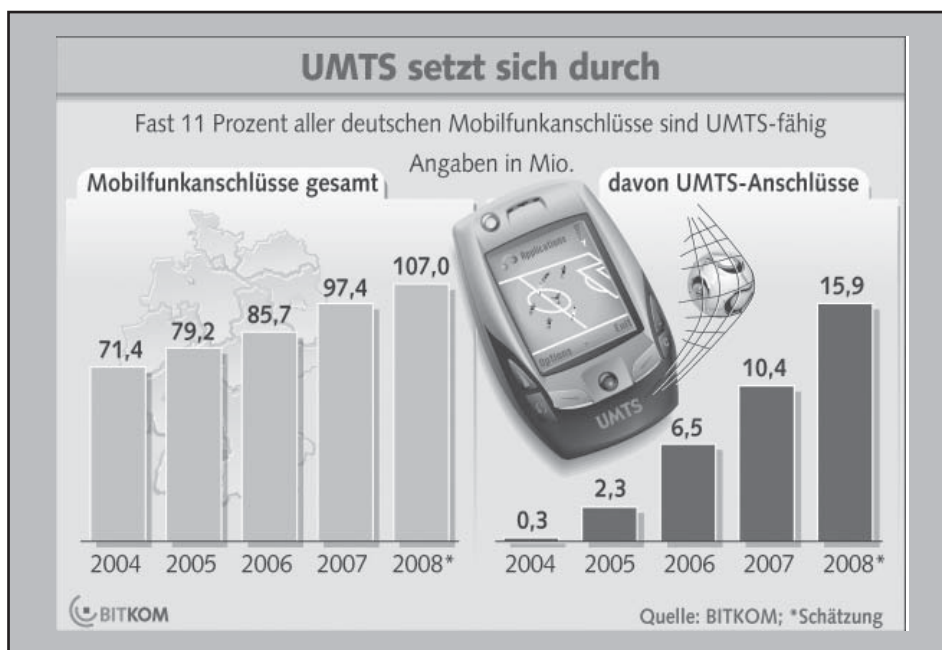


Abbildung 1 Weltweit steigen die Nutzerzahlen der Mobilfunknetze (Quelle: BITKOM)

Sicherheitsaspekte öffentlicher Mobilfunknetze - Teil 1

das Netz eines Mobilfunkbetreibers in verschiedene Funktionsgruppen. Auch wenn sich die Nomenklatur und konkrete Architektur zwischen GSM/GPRS/EDGE und UMTS in Details unterscheiden, so ist der grundlegende Aufbau doch soweit identisch, dass die wichtigsten Komponenten gemeinsam betrachtet werden können.

Die erste Funktionsgruppe, mit der das Endgerät in Berührung kommt, ist das Base Station Subsystem (BSS), dessen UMTS Äquivalent das Radio Network Subsystem ist. Beide bestehen aus mehreren Basisstationen (Base Transceiver Station (BTS) bzw. Node-B) und einem Controller (Base Station Controller (BSC) bzw. Radio Network Controller (RNC)). Die Summe all dieser Subnetze ergibt das GERAN bzw. UTRAN eines Providers (GSM/EDGE Radio Access Network / UMTS Terrestrial Radio Access Network). Hier werden keine Daten über den Teilnehmer vorgehalten. Wichtig ist allerdings, dass jedes dieser Subnetze sich in ein oder mehrere so genannte Location Areas (LA) aufteilt, die über die Location Area Identity (LAI) identifiziert werden können. Hierüber und über zusätzliche Informationen, z.B. die verwendete Basisstation und sogar die zuständige Sektorantenne, kann eine grobe Ortsbestimmung des Teilnehmers geschehen. All diese Informationen werden im Network Subsystem (NSS) für das Routing ein- und ausgehender Anrufe und zu Abrechnungszwecken benötigt.

Wer weiß was?

Die aktuelle LAI eines Teilnehmers wird im NSS mit anderen Daten des Teilnehmers

verknüpft. Dazu zählen das verwendete Endgerät (International Mobile Equipment Identity, IMEI), die Teilnehmer Identifikation (IMSI), Shared Secret sowie allgemeine Verbindungsdaten, wie z.B. Dauer und Ziel eines Telefongesprächs. All diese Daten werden in verschiedenen Datenbanken gespeichert (siehe Kasten „Datenbanken im Mobilfunknetz“), auf die Mobile Switching Center (MSC) und Global MSC (GMSC), welche für das Routing zuständig sind, zugreifen. Aber auch administrative Komponenten aus dem Operations and Support System (OSS) können auf diese Daten zugreifen. Neben der Verwaltung der Teilnehmer und Abrechnung der Verbindungen werden in diesem Teil des Netzes auch Mechanismen zur staatlichen Kontrolle der Netze implementiert. Dazu zählen die per Gerichtsbeschluss erwirkbaren Abhörmaßnahmen durch polizeiliche oder geheimdienstliche Stellen (engl. Lawful Interception) ebenso, wie die durch die EU-Richtlinie 2006/24/EG ab dem 01.01.2009 vorgeschriebene Vorratsdatenspeicherung. Lässt man die Bedenken der Datenschützer einmal außen vor und unterstellt die Rechtsstaatlichkeit dieser Maßnahmen, so ändert dies nichts an der Tatsache, dass die Datenbanken der Mobilfunkbetreiber extrem sensible Daten beinhalten.

Die Mehrheit der Mobilfunkteilnehmer wird – vermutlich zu Recht – die Meinung vertreten, dass sie vor dem Staat nichts zu verbergen haben und die Speicherung von Verbindungsdaten oder das gezielte Abhören von Tatverdächtigen einen Beitrag zur Inneren Sicherheit leisten können. Ein Stückchen Privatsphäre im Tausch ge-

gen ein Stückchen Sicherheit. Eine durchaus nachvollziehbare Haltung. Richtig brisant wird es dann, wenn nicht der Staat, sondern eine nicht rechtlich legitimierte Instanz Zugriff auf diese Daten erhält. Für sich genommen ist die IMSI oder LAI eines Teilnehmers noch keine Information von großer Tragweite. Sprengstoff wird daraus erst durch die Verknüpfung der Daten vieler Teilnehmer untereinander. So lassen sich nicht nur Bewegungsprofile Einzelner, sondern ganze soziale Netzwerke mit allen Interaktionen der Individuen, wie etwa persönlichen Treffen an einem bestimmten Ort oder geführten Telefongesprächen, rekonstruieren. Besteht dann noch die Möglichkeit, diese Netze mit Inhalten zu verknüpfen - ob das nun das Konsumentenverhalten oder der Inhalt eines Telefongesprächs ist - lässt sich ein exaktes Bild über Gewohnheiten und Aktivitäten von Mobilfunkteilnehmern erstellen. Dies kann, gerade im geschäftlichen Umfeld, weitreichende Konsequenzen haben. Vertrauliche Informationen zu Geschäftsbeziehungen und Kunden sowie Intellectual Property stehen zur Disposition.

Jenseits aller orwellischen Paranoia wird hieran eines deutlich: Die Nutzung von Mobilfunknetzen setzt Vertrauen voraus. Vertrauen in die Einhaltung rechtsstaatlicher Rahmenbedingungen und in die Gewissenhaftigkeit der Mobilfunkprovider. Gewissenhaftigkeit sowohl in Bezug auf die Absicherung der Datenbanken als auch in die Auswahl der Mitarbeiter mit Zugriff auf die sensiblen Kundendaten. Die Möglichkeit von Innentätern, ob sie nun eigene Interessen oder die des Konzerns verfolgen, besteht. Das zeigte im Mai dieses Jahres eindrucksvoll die Affäre um die Deutsche Telekom. Der Vorwurf lautete, dass Mitarbeiter der Deutschen Telekom Kunden- und Verbindungsdaten zur Auswertung an ein externes Unternehmen weitergegeben hätten. Ziel der Aktion war es offensichtlich, Verbindungen von Vorstandsmitgliedern zu Journalisten offenzulegen, um so undichte Stellen im Konzern zu lokalisieren. Auf wessen Betreiben und in welchem Maßstab das geschah, ist eine Frage, die Staatsanwaltschaften und Gerichte noch länger beschäftigen wird. Es ist zu vermuten, dass zumindest Namen, IMSIs und aufgezeichnete LAIs sowie Verbindungsdaten der betroffenen Kunden das Unternehmen verließen. Nicht, dass eine interne Auswertung dieser Daten etwa legal wäre, aber dass die sensiblen Daten einfach an einen externen Dienstleister gegeben wurden, macht die Angelegenheit besonders delikat.

Datenbanken im Mobilfunknetz

AuC - Authentication Center: Neben den Funktionen zur Teilnehmerauthentifizierung enthält das AuC auch eine Datenbank mit den Shared Secrets aller Teilnehmer. Insiziert werden sie über die zugehörige IMSI.

EIR - Equipment Identity Register: Enthält die IMEI aller im Netz angemeldeten Endgeräte. Über eine Whitelist, eine Greylist und eine Blacklist wird zwischen zugelassenen, zu überprüfenden und gesperrten (z.B. als gestohlen gemeldeten) Endgeräten differenziert. Dieses Verzeichnis zu führen stellt die GSM-/UMTS-Architektur frei.

HLR - Home Location Register: Im Home Location Register werden alle den Teilnehmer betreffenden Daten dauerhaft gespeichert. Darunter fallen IMSI, Rufnummer des Teilnehmers (Mobile Station ISDN Number) sowie Ortsinformationen in Form der aktuellen Location Area Identity (LAI). Auch für den Teilnehmer freigeschaltete Dienstmerkmale, Gebührendaten und ein Verweis auf das aktuell genutzte VLR sind im HLR enthalten.

VLR - Visitor Location Register: Enthält eine temporäre Kopie der - für das Routing relevanten - Nutzerdaten aus dem HLR, um die Mobilität des Nutzers sicherzustellen. Bei Wechsel in eine Location Area, für die ein anderes VLR zuständig ist, werden die Daten in das ab sofort zuständige VLR transferiert.

Sicherheitsaspekte öffentlicher Mobilfunknetze - Teil 1

Das Beispiel zeigt uns, dass Datensicherheit ein relevantes Thema ist, was - wenn auch oft viel zu spät - den Kunden der Mobilfunkbetreiber am Herzen liegt. Es ist somit zu hoffen, dass die Mobilfunkunternehmen den entstandenen Image-Schaden als Anlass nehmen, um ihre Sicherheitsmaßnahmen einer Revision zu unterziehen. Vielleicht setzt auch der ein oder andere in Zukunft stärker auf Transparenz als Marketinginstrument. Die Kundschaft jedenfalls ist sensibilisiert.

Ferngesteuerte Endgeräte

Neben den unvermeidlich anfallenden Kundendaten gibt es in Mobilfunknetzen auch einige vermeidbare Sicherheitslücken. Was Kunde und Betreiber gleichermaßen zu Komfort verhelfen sollte, erweist sich manchmal als Fallstrick. Moderne Endgeräte sind kleine Computer, die dementsprechend auch über eine Firmware und ein Betriebssystem verfügen. Darüber hinaus kann je nach Endgerät eine Vielzahl von Einstellungen getroffen werden. Falsche Konfiguration kann dazu führen, dass das Endgerät in seiner Leistungsfähigkeit eingeschränkt wird oder ein bestimmter Dienst nicht genutzt werden kann. Dabei kann den wenigsten Kunden zugemutet werden, die neueste Version des Betriebssystems auf ihrem Handy selbst zu installieren. Auch das Wälzen von seitenlangen Konfigurationsleitfäden mit Empfehlungen des Mobilfunkbetreibers ist nicht gerade der Traum jedes Kunden. Den neuesten Sicherheits-Patch für das Betriebssystem installieren? Wäre schön, wenn der Provider das übernehmen könnte.

Technisch ist das ohne weiteres möglich. Neben dem „Branding“, also dem Präparieren der Endgeräte nach Betreibervorgaben, das vor der Auslieferung des Endgeräts an den Kunden vorgenommen wird, setzen viele Anbieter Techniken ein, die unter dem Begriff „Over-the-Air-Programming“ (OTA) zusammengefasst werden. Während beispielsweise per FOTA (Firmware over the Air) Patches und ganze Firmware-Pakete installiert werden können, bietet OTAPA (OTA Parameter Administration) die Möglichkeit, Konfigurationsdaten von Endgeräten zentral zu verwalten. Nur so ist es etwa möglich, die korrekte Konfiguration der GPRS-Verbindung wiederherzustellen, wenn ein Kunde diese durch ein paar unbedachte Tastendrucke ungültig gemacht hat. Kritisch wird es dann, wenn dies vom Teilnehmer unbemerkt und vielleicht auch unaufgefordert passiert.

Die Angriffsmöglichkeiten sind vielfältig. Eine manipulierte Firmware einzuschleusen, die beispielsweise die Aktivitäten des

Nutzers am Endgerät protokolliert oder gar Daten kopiert, wäre wohl der Worst Case eines Angriffsszenarios. Aber auch viel trivialere Eingriffe, etwa die Fehlkonfiguration der Internetverbindung, können schwerwiegende Folgen für die Datensicherheit haben. So könnte ein Angreifer die Adresse eines Proxy konfigurieren, über den er die Kontrolle besitzt. Alle Daten würden umgeleitet und könnten - falls sie nicht einer Ende-zu-Ende-Verschlüsselung unterliegen - im Klartext mitgelesen werden. Das gilt gleichermaßen für geschäftliche oder private Emails wie auch für das Surfen im Internet. Beispiele wie dieses ließen sich noch viele nennen. Der Einsatz von OTA und FOTA ist - auch wenn er noch so nutzbringend sein mag - äußerst sensibel und bedarf entsprechender Schutzmechanismen durch den Provider. Eine Offenlegung der Schnittstellen und Sicherungsmaßnahmen und der Verzicht auf „unsichtbare“ Konfigurationsänderungen würden dem Kunden zumindest das Gefühl zurückgeben, die Kontrolle über sein Endgerät zu besitzen.

Kompromittierbare Dienste

Die Benutzung von Mobiltelefonen birgt aber auch andere Gefährdungen, jenseits derer die in der Natur der Netze begründet liegen. Von den Netzbetreibern selbst oder von externen Dienstleistern erbrachte Sprach- und Datendienste haben ebenfalls ihre sicherheitstechnischen Tücken.

Netzbetreiber und Endgerätehersteller bieten ihren Kunden in der Regel eine

Vielzahl von Komfortfeatures und Leistungsmerkmalen. Ob Push-To-Talk (PTT) oder automatische Rufannahme: ein vorsichtiger und bewusster Umgang mit solchen Leistungsmerkmalen ist - gerade im geschäftlichen Umfeld - dringend zu empfehlen. Versehentlich oder durch Manipulation eine falsche Rufnummer einer PTT Gruppe hinzugefügt - wer kann schon abschätzen, was der unerwartete Adressat mit dem Gehörten anzufangen weiß? Ein gutes Beispiel sind Telefonkonferenzen, welche als Leistungsmerkmal im Betreibernetz zur Verfügung gestellt werden. Ob ein Anrufer zuvor eine Konferenzschaltung mit einem weiteren - unerwünschten - Zuhörer initiiert hat, ist nicht immer feststellbar. Kurze Piepsgeräusche beim Eintritt in eine Telefonkonferenz werden oft eher als Störung im Netz oder als Akku-Warnung des eigenen Endgeräts interpretiert. Möglichkeiten, sich gegen solche Mithörer zu schützen, hat der einzelne Teilnehmer nicht.

Ähnliches gilt für die Nutzung aller im Mobilfunknetz erbrachten Dienste. Ob Sprach-, Messaging- oder Datendienst: viele Verfahren haben Schwächen, die ein Angreifer ausnutzen kann, um in den Besitz sensibler Informationen zu gelangen. Wichtig ist, sich klar zu machen, dass Mobil-Telefonie nicht sicherer sein kann als die Festnetz-Telefonie. Zu der Angreifbarkeit der Luftschnittstelle und den Eigenarten des Vermittlungsnetzes gesellen sich dieselben Probleme, die auch im Festnetz existieren. So beschränkt sich die verschlüsselte Übertragung - falls über-

Jetzt Leser werden

Der Netzwerk Insider

Der Netzwerk Insider erscheint 12 Mal im Jahr im PDF-Format und informiert Sie per eMail über die Hintergründe aktueller Netzwerk-Technologien. Jeden Monat werden zwei Themen gewählt, über die in ausführlicher Form topaktuelle Insider-Informationen gegeben werden. Der Netzwerk-Insider vertritt die Sichtweise von Technologie-Anwendern und bewertet Produkte und Technologien im Sinne der wirtschaftlichen und erfolgreichen Umsetzbarkeit in der täglichen Praxis. Durch seine strenge wirtschaftliche Unabhängigkeit (keine Hersteller-Anzeigen) kann er es sich leisten, Schwachstellen und Nachteile offen anzusprechen. Der Netzwerk-Insider ist bekannt für seine kritische, herstellerneutrale und fundierte Technologie-Bewertung.



Hier können Sie sich zum Netzwerk Insider kostenlos und ohne jede Verpflichtung registrieren lassen:

<http://www.comconsult-akademie.de/de/Registrierung.php>

Sicherheitsaspekte öffentlicher Mobilfunknetze - Teil 1

haupt eine solche ausgehandelt wurde – ausschließlich auf die Luftschnittstelle. Ab diesem Zeitpunkt unterliegt das Gespräch denselben Gefährdungen wie im öffentlichen Telefonnetz. Eine Ende-zu-Ende-Verschlüsselung muss separat von beiden Teilnehmern ausgehandelt und technisch umgesetzt werden. Der technische und finanzielle Aufwand ist nicht unerheblich und in den seltensten Fällen für Privatleute interessant oder erschwinglich. Aber auch im Geschäftsumfeld lohnt sich die Investition selten, geschweige denn, dass sie flächendeckend für alle potentiellen Gesprächspartner umgesetzt werden könnte. Das Stichwort lautet hier „erhöhter Schutzbedarf“. Welche Informationen derart sensibel sind, dass sie durch teure Investitionen geschützt werden müssen liegt dabei - über die gesetzlichen Bestimmungen, etwa zum Schutz von Kundendaten, hinaus – im Auge des Betrachters.

Nachrichtendienstlich

Ebenfalls unsicher ist die Benutzung von Messaging-Diensten. Der beliebte Short Message Service (SMS) oder auch Enhanced Message Service (EMS, eine Aneinanderreihung von SMS) sind dafür gute Beispiele. Die Kurznachrichten von maximal 160 Zeichen pro SMS werden nicht über die eigentlichen Sprach- oder Datenkanäle des GSM-Netzes übertragen. Vielmehr wird für die Übertragung auf die Steuerkanäle zurückgegriffen, über die normalerweise Aufgaben die Signalisierung von Anrufen abgewickelt werden. Diese unterliegen prinzipiell derselben Verschlüsselung auf der Luftschnittstelle, wie Sprach- und Datenkanäle des GSM-Netzes, sind also als potentiell unsicher einzustufen. Darüber hinaus kann als Fallback auf einen gänzlich unverschlüsselten Steuerkanal zurückgegriffen werden, was beispielsweise bei zu hoher Auslastung der regulären Übertragungswege der Fall ist. Der Inhalt der SMS selbst bleibt unverschlüsselt und geht in dieser Form durch die Luft und über sämtliche Server und Gateways auf dem Weg zum Empfänger. Sich per SMS auf einen Kaffee zu verabreden, ist also bestimmt unkritisch. Auf diesem Wege Geschäftsgeheimnisse auszutauschen, ist mit Sicherheit keine gute Idee.

Was allgemein für Email in puncto Sicherheit gilt, muss so oder ähnlich auch für den mobilen Zugriff auf Email beachtet werden. Bedenkt man, wie wenig verbreitet die Verschlüsselung des Email-Verkehrs momentan ist, scheint hier kein gesteigerter Bedarf nach Schutz zu bestehen. In Wahrheit ist aber eher die fehlen-

de Verbreitung der notwendigen Schutzmechanismen der Hemmschuh. Was nützt es mir, meine Email zu verschlüsseln, wenn der Adressat sie nicht entschlüsseln kann? Während unternehmenssintern das Rollout einer sicheren Email Lösung kein Problem darstellt, Bedarf es beim Emailverkehr mit Kunden, Partnern und Zulieferern erheblichen organisatorischen Aufwands, um eine konsistente Lösung zu gewährleisten. Aus diesem Grund wird oft auf Verschlüsselung der Inhalte verzichtet. Solange sich die Übertragung der Emails in einer geschützten Umgebung wie z.B. einem Unternehmensnetz abspielt, ist dies in vielen Fällen hinnehmbar. Im Fall mobiler Email findet dieser Zugriff aber immer von außerhalb statt. Es ist daher wichtig, die Übertragungswege zwischen Mailserver und mobilem Endgerät zu betrachten und hier entsprechende Schutzmaßnahmen zu treffen.

Push Mails

Grundsätzlich unterscheiden sich zwei Verfahren beim mobilen Zugriff auf Emails. Klassischerweise baut der Client in regelmäßigen Abständen eine Verbindung zum Mailserver auf und „fragt“ nach neuen Emails. Dieses Verfahren unterscheidet sich nicht von dem des „normalen“ Emailclients eines externen Mitarbeiters. Der Zugriff kann durch verschiedene architektonische und verschlüsselungstechnische Maßnahmen gegen Manipulation abgesichert werden. Beispiele wären das Bereitstellen eines gespiegelten Email-Servers in der „Demilitarisierten Zone“ (DMZ), Authentisierung per Zertifikat und das Einrichten eines sicheren Übertragungstunnels für den Abruf von Mails. Nachteile des Verfahrens sind die häufigen – und meist überflüssigen – Datenverbindungen, welche zwischen Client und Server etabliert werden. Was im LAN

oder auch WAN Bereich kaum ins Gewicht fällt, kann im mobilen Einsatz hohe Kosten verursachen. Da die Netzbetreiber häufig pro angefangene Dateneinheit fester Größe abrechnen, entstehen schnell hohe Verbindungsentgelte. Längere Intervalle für die Serverabfrage sind nur bedingt sinnvoll, da Mails nicht mehr zeitnah empfangen werden und der Sinn des mobilen Einsatzes damit verloren gehen würde

Daher erfreut sich die zweite, passive Variante großer Beliebtheit: Push Mail. Bei diesem Verfahren initiiert nicht der Client, sondern der Server die Übertragung neuer Emails. Das passiert entweder per SMS oder über eine dauerhaft bestehende, virtuelle Netzwerkverbindung. Die verschiedenen Verfahren hierfür wurden von der Open Mobile Alliance (OMA) standardisiert. Für die eigentliche Datenübertragung kommt dann eines von vielen Synchronisierungsprotokollen zum Einsatz. Als Beispiel sei das ebenfalls von der Open Mobile Alliance entwickelte SyncML genannt. Darüber hinaus existiert eine Vielzahl proprietärer Protokolle. Für Signalisierung und Übertragung kann, je nach Vorgaben des Unternehmens und des Netzbetreibers, ein so genanntes Network Operation Center (NOC) zugeschaltet werden.

Das NOC wird vom Mobilfunkanbieter oder einem Drittanbieter zur Verfügung gestellt. Der bekannteste Vertreter einer solchen Drittanbieter-Lösung ist „Blackberry“ der Kanadischen Firma Research in Motion (RIM). RIM betreibt dazu u.a. NOCs in Kanada und in Großbritannien. Alle zwischen Mailserver und mobilem Endgerät ausgetauschten Daten passieren dabei das jeweils zuständige NOC, so dass hier eine geeignete Ende-zu-Ende-Verschlüsselung genutzt und dem

Beim **Advanced Encryption Standard** (AES) handelt es sich um ein symmetrisches Kryptosystem, das als Nachfolger für DES bzw. Triple DES (3DES) im Oktober 2000 vom US-amerikanischen National Institute of Standards and Technology (NIST) als Standard verabschiedet wurde. AES ist ein Blockchiffre und verfügt über eine feste Blockgröße von 128 Bit und eine variable Schlüssellänge von 128, 192 oder 256 Bit. Anhand der Schlüssellänge wird zwischen den drei AES-Varianten AES-128, AES-192 und AES-256 unterschieden.

Für AES sind bisher keine Master-Keys oder andere Verfahren bekannt, die ein Aufbrechen der AES-Verschlüsselung in einem überschaubaren Zeitraum erlauben. Der Algorithmus ist frei verfügbar und darf ohne Lizenzgebühren eingesetzt werden.

AES wird u.a. bei der Verschlüsselung für Wireless LAN (802-11i / WPA2), bei SSH und bei IPsec sowie zur Verschlüsselung diverser komprimierter Datearchive verwendet (z.B. bei 7-Zip). Auch in der Europäischen Union gehört AES zu den empfohlenen kryptografischen Algorithmen (siehe EU-Projekt NESSIE, IST-1999-12324)

Sicherheitsaspekte öffentlicher Mobilfunknetze - Teil 1

Anbieter eine besondere Vertrauensstellung eingeräumt werden muss. Ansonsten wäre denkbar, dass im NOC Emails zumindest temporär zwischengespeichert und so dritten zugänglich gemacht werden könnten. Blackberry und anderen Push-Mail-Diensten ist diese Befürchtung häufig vorgehalten worden. Vor allem, weil zunächst nur unzureichende Verschlüsselungsmethoden (z.B. Triple DES) verwandt worden sind. Inzwischen bietet Blackberry daher auch für besonders hohe Sicherheitsansprüche eine AES-Verschlüsselung.

Bei Blackberry werden die Private Keys für die Verschlüsselung jedem Benutzer individuell zugewiesen. Vor ihrer Übertragung werden die Daten vom Blackberry Enterprise Server (BES), der sich innerhalb des geschützten Unternehmensbereich, hinter der unternehmenseigenen Firewall mit einem privaten Key verschlüsselt und können erst auf dem Handheld des Empfängers gelesen werden. Jeder Schlüssel wird dabei ausschließlich in der sicheren Sphäre des entsprechenden Endgerätes hinterlegt. Aus diesem Grund ist auch dringend die Nutzung von Blackberry-Endgeräten zu empfehlen, da ansonsten kaum die Unversehrtheit des Schlüssels auf dem Endgerät gewährleistet ist.

Nach heutigem Stand der Technik gibt es keine Mechanismen, an diesen privaten Key heranzukommen. Nur die IT-Abteilung des Nutzers kann auf die Keys der einzelnen Anwender zugreifen, und selbst der Hersteller der Push-Mail-Lösung, bei Blackberry also RIM selbst, ist angeblich unter keinen Umständen in der Lage, Zu-

gang zu dem privaten Key zu bekommen oder die Nachrichten des Kunden zu lesen.

Jedoch hat beispielsweise Frankreichs Staatspräsident Nikolas Sarkozy als eine seiner ersten Amtshandlungen die Nutzung von Blackberry für Regierungsmitglieder verboten. Grund dafür ist die Befürchtung des für die innere Sicherheit in Frankreich zuständige Secrétariat Général de la Défense Nationale (SGDN), geheime Sitzungen könnten allzu leicht von fremden Geheimdiensten abgehört werden, da die Blackberry-NOCs in Kanada und in Großbritannien angesiedelt sind und diese Länder über z.T. sehr großzügige Datenschutzregelungen verfügen, sobald Geheimdienste sich dafür interessieren. Die Befürchtungen sind nach Bekanntwerden der UKUSA-Verträge nicht ganz unbegründet. UKUSA bezeichnet die zwischen Großbritannien (United Kingdom) und den USA 1949 geschlossenen Verträge zur Zusammenarbeit der US-amerikanischen National Security Agency (NSA) und dem britischen GCHQ sowie dem kanadischen CSE, dem australischen DSD und dem neuseeländischen GCSB. Ganz aktuell sind Bestrebungen der britischen Regierung, mit einem Milliardenaufwand jegliche Kommunikation, d.h. auch mobile Email-Kommunikation, zu überwachen und zentral zu speichern. (siehe Abbildung 6)

Auch das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) hat sich zunächst kritisch zu Blackberry geäußert, ist dann aber wieder zurückgerudert und hält sich seitdem auffällig mit Stellungnahmen zu diesem Thema zu-

rück. Es wird lediglich darauf verwiesen, dass es bisher keine Möglichkeit gegeben habe, die von RIM verwendeten Algorithmen zu prüfen, so dass keinerlei Erkenntnisse über die verwendeten Sicherheitsmechanismen vorliegen, die fundierte Aussagen ermöglichen.

RIM seinerseits hat 2005 das Fraunhofer Institut für sichere Informationstechnologie (SIT) beauftragt, eine detaillierte Sicherheits-Analyse der Blackberry-Lösung zu erarbeiten. Auf der IDC Security Conference 2006 in Frankfurt hat Fraunhofer SIT bekanntgegeben, dass die erste von drei Testphasen zur Sicherheit von E-Mail-Push-Diensten mit der BlackBerry-Lösung abgeschlossen ist. Dabei sind keine Hinweise auf verborgene Hintertüren, einen bei RIM liegenden Master-Key oder andere Möglichkeiten gefunden worden, wie die E-Mail-Kommunikation mittels der BlackBerry-Enterprise-Lösung von Dritten gelesen oder manipuliert werden könnte. Einige von Fraunhofer empfohlene Sicherheitsoptimierungen sind bereits umgesetzt worden, so dass mit einem endgültigen Abschluss der Untersuchungen noch in diesem Jahr gerechnet wird.

Geht man davon aus, dass bei Blackberry wirklich eine korrekte Implementierung des AES-256 vorliegt, bleibt also vor allem die Frage, ob der im eigenen Unternehmen stehende Synchronisierungsserver ein nicht zu kontrollierendes Einfallstor in die gesamte Unternehmenskommunikation darstellt. Zumal dieser Server beispielsweise bei MS-Exchange vollumfänglichen Zugriff auf die gesamte E-Mail-Kommunikation haben muss. Würde also der Server über eine Hintertüre

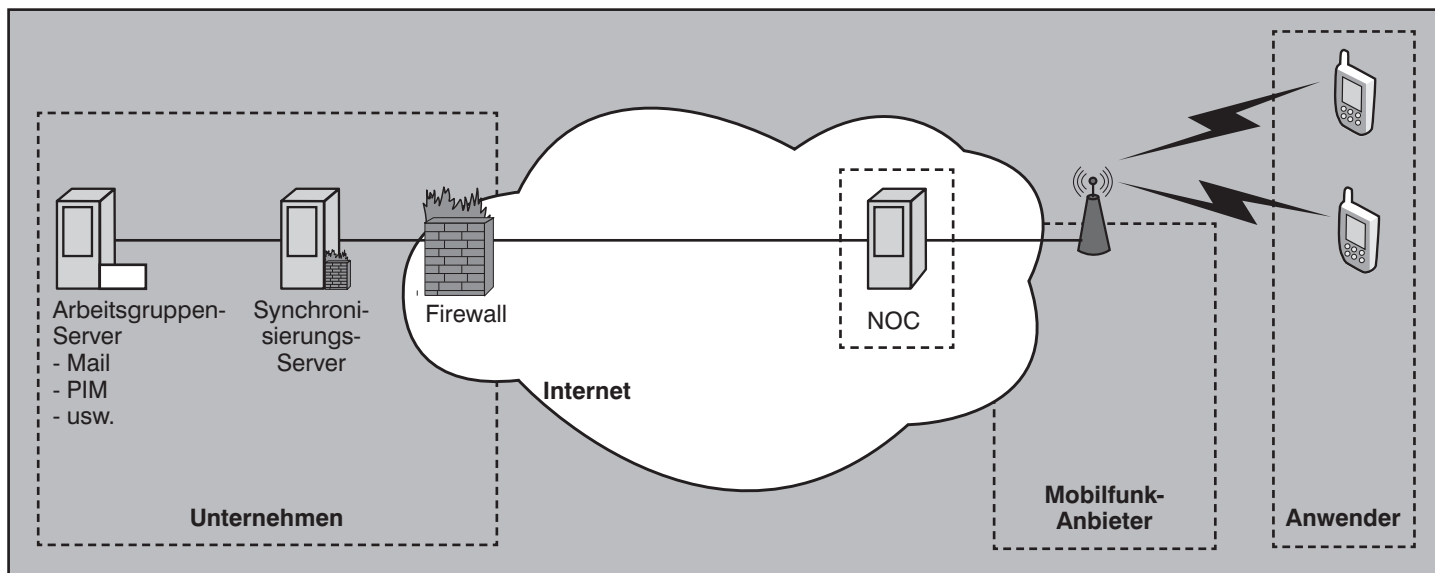


Abbildung 6: Push Mail Synchronisation unter Einsatz eines Network Operation Centers

Sicherheitsaspekte öffentlicher Mobilfunknetze - Teil 1

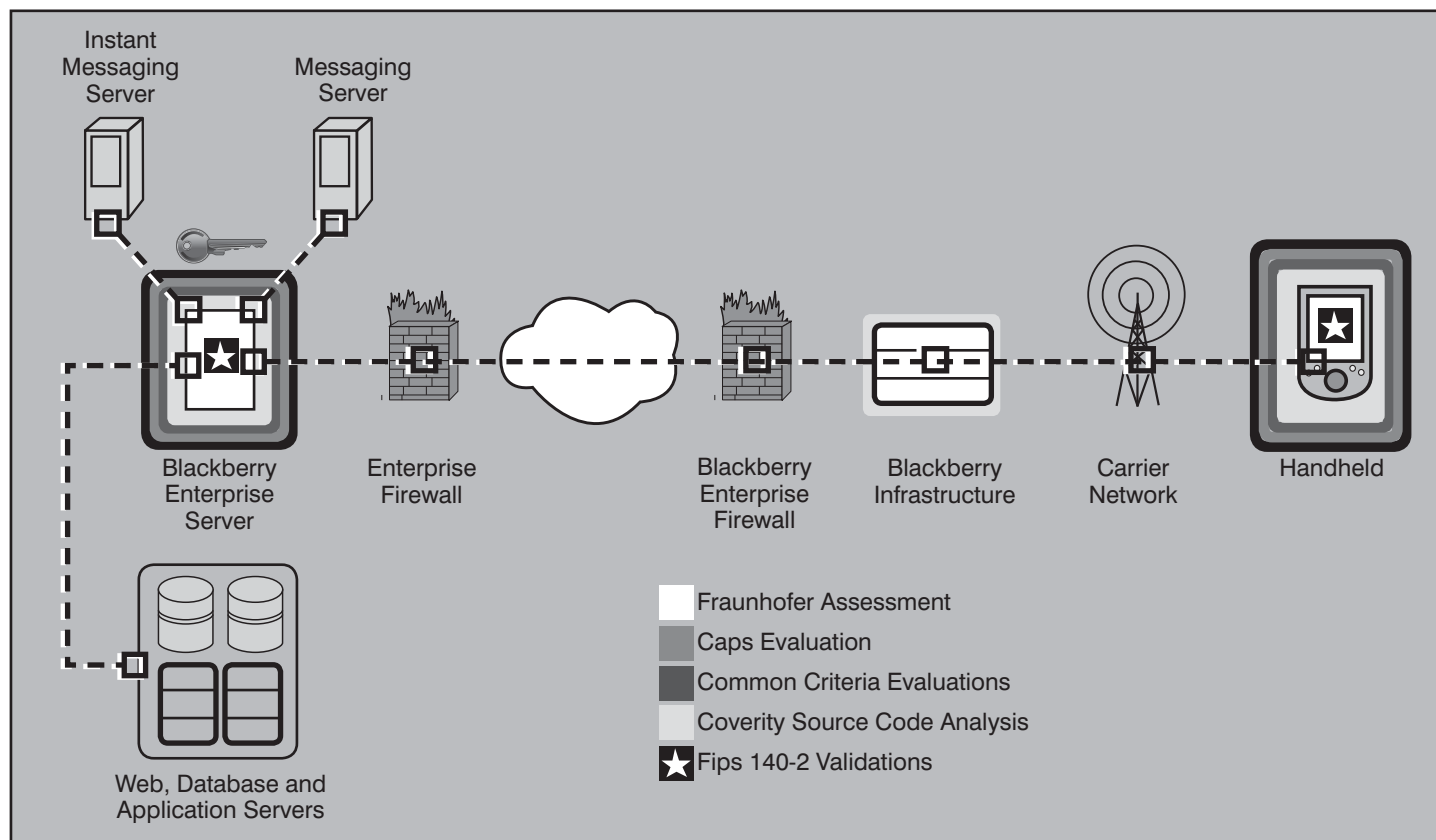


Abbildung 7: Bereiche unterschiedlicher Sicherheitsevaluierungen bei Blackberry

verfügen, wäre die gesamte E-Mail-Kommunikation und nicht nur die Kommunikation von und zu den mobilen Endgeräten dem Zugriff von außen ausgesetzt.

Zwar soll Fraunhofer SIT auch diese Fragestellung klären (siehe Abbildung 7), und RIM hat dazu nicht nur Fraunhofer die entsprechenden Quellcodes zur Verfügung gestellt, aber diese Untersuchungen sind natürlich nur begrenzt aussagekräftig. Denn niemand außer dem Betreiber kann sicherstellen, dass die zur Verfügung gestellte Software wirklich zum Einsatz kommt oder evtl. beim nächsten Update nicht doch wieder eine Hintertür eingebaut worden ist. Zudem stellt sich die Frage, warum RIM nicht auf die Bedenken und Sorgen der Skeptiker eingeht und beispielsweise eine weiter verteilte NOC-Struktur aufbaut. So könnte beispielsweise auch ein NOC in Deutschland bereitgestellt werden, das dann natürlich auch deutschen Datenschutzvorschriften unterliegt. Die Kosten und der Image-Gewinn sollten dafür kaum höher zu bewerten sein, als die ständige Sicherheitsdebatte.

Die Bedenken sind zweifelsohne spitzfindig, treffen teilweise auch auf andere Anbieter als RIM zu und klingen ein wenig paranoid, aber auch hier zeigt die Erfah-

rung, dass man bei solchen Dingen selten positiv überrascht wird. Bei erhöhtem Schutzbedarf ist also das NOC bzw. der Synchronisierungsserver ein zusätzlicher Risikofaktor. Realisiert man eine Push-Mail-Lösung gänzlich im eigenen Haus, erkaufte man sich jedoch die volle Kontrolle über die Datensicherheit mit einem höheren administrativen Aufwand. Angebote für solche eigenen Lösungen sind jedoch schon länger verfügbar und weisen einen ähnlichen Komfort auf wie NOC-basierte Lösungen.

Eventuell sicher surfen

Neben Push Mail und anderen Nachrichten-Übertragungsmöglichkeiten werden mobile Endgeräte zunehmend mehr auch für den mobilen Internet-Zugang genutzt. Auch hier muss daher die Frage gestellt werden, wie sicher dieser Zugang z.B. im Vergleich zu ansonsten intensiv geschützten Unternehmensnetzen aus. Bleibt wenigstens das private Online-Banking oder der Zugriff auf Dokumente im Unternehmensnetz vor unbefugten Augen verborgen? Vielleicht! Unabhängig von der zugrundeliegenden Übertragungstechnologie – GPRS, EDGE oder UMTS-Derivat – erfolgt der Zugriff auf Websites aller Art mithilfe des Wire-

less Access Protocol (WAP). Ausschließliches Ziel der ersten Versionen dieser Protokollfamilie war die effiziente Übertragung von Websites über schmalbandige Datenverbindungen und deren, für mobile Endgeräte optimierte, Darstellung. Hierzu wurde eine Reihe von Protokollen definiert. Die Inhalte werden in einer für mobile Endgeräte optimierten Version auf Seiten des Webservers bereitgestellt und nach dem Transport per Internet und WAP entsprechend auf dem Endgerät dargestellt. Diese Anwendungsschicht wird in Abbildung 8 mit Wireless Application Environment (WAE) bezeichnet.

Während der Transport durch das Internet mittels der herkömmlichen Protokolle TCP, TLS und HTTP stattfindet, wird der Transport zum Endgerät mithilfe der WAP Protokoll Suite sichergestellt. Hierzu wird ein WAP-Gateway benötigt, welches die Protokolle übersetzt. Problem dabei: sowohl TLS als auch HTTP Protokoll werden in ihre WAP-Äquivalente umgesetzt. Die durch TLS gesicherten Inhalte müssen also entschlüsselt und für die Übertragung zum Endgerät per Wireless TLS (WTLS) erneut verschlüsselt werden. Das bedeutet, dass die Ende-zu-Ende Sicherheit von Inhalten am Gateway durchbrochen wird. Das WAP-Gateway stellt hier

Sicherheitsaspekte öffentlicher Mobilfunknetze - Teil 1

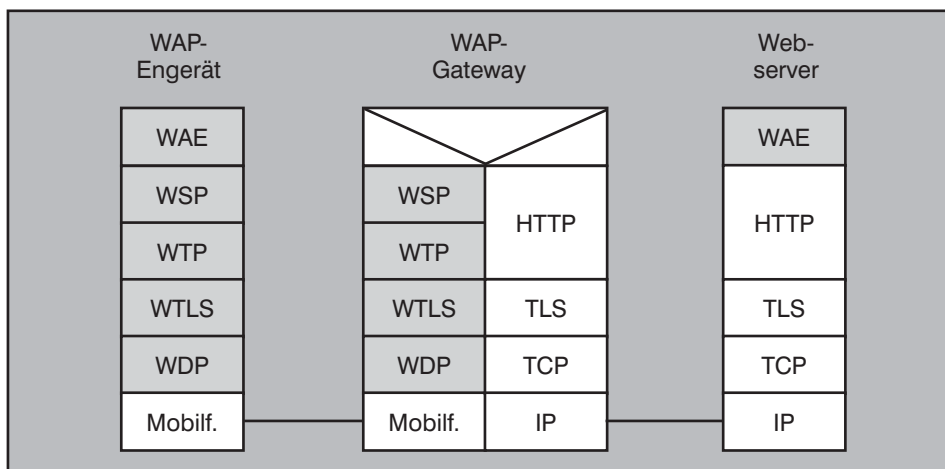


Abbildung 8: Protokoll-Stack der WAP 1.x - Familie

also die Schwachstelle aller WAP Versionen 1.x dar.

Dieser Umstand wurde mit der aktuellen Version des Standards WAP 2.0 aufgelöst. WAP 2.0 definiert unter anderem eine Variante der Extensible Hypertext Markup Language (XHTML) als neues Format für WAE-Inhalte. Diese Beschreibungssprache erweitert die geläufige Hypertext Markup Language (HTML) um Sprachelemente der für WAP 1.x verwendeten Wireless Markup Language (WML). Die neue Version trägt aber auch der Tatsache Rechnung, dass das primäre Ziel nicht mehr die Optimierung der Übertragungsgeschwindigkeit sein kann. Vielmehr wird davon ausgegangen, dass der genutzte Datendienst IP als Basisprotokoll zur Verfügung stellt. Die Architektur beinhaltet zwar weiterhin ein WAP-Gateway. Das ist aber zum Transport der WAE-optimierten Inhalte nicht mehr zwingend erforderlich. Es kann auch - dann allerdings ohne Protokolloptimierung -

direkt auf Inhalte eines WAE zugegriffen werden. Andernfalls übernimmt das WAP-Gateway die optionale Optimierung der Protokolle TCP und HTTP, so dass im Falle einer TLS-gesicherten Verbindung zwar TCP optimiert wird, die darüber liegenden Schichten aber unangetastet bleiben. Die Ende-zu-Ende-Sicherheit bleibt somit gewahrt. (siehe Abbildung 9)

Um beim Surfen und dem Zugriff auf eventuell vertrauliche Inhalte also sicherzugehen zu können, dass die Daten vor Zugriff durch Angreifer oder Innetäter geschützt bleiben, ist die Verwendung von WAP 2.0 unerlässlich. Die Tauglichkeit eines Endgerätes für WAP 2.0 und der Verzicht auf den Einsatz von WAP 1.x für den Anwender allerdings nicht leicht zu überprüfen. Oft klaffen Produktbeschreibung des Herstellers und Realität auseinander. Zudem gibt es diverse Mischformen, z.B. Geräte, die zwar WAP 1.x verwenden, aber sowohl WML als auch XHTML im Browser darstellen können.

Der einzige Weg, sich der WAP 2.0 Fähigkeit eines Endgeräts zu versichern, liegt darin, ohne den Umweg über ein WAP-Gateway auf eine WAE zuzugreifen.

Allerdings lässt sich das Zurückgreifen auf WAP-Proxys nicht immer vermeiden. Ein Derivat dieser Protokollfamilie kommt für den Versand von Multimediamanrichten mittels Multimedia Message Service (MMS) zum Einsatz. Die multimedialen Inhalte werden dabei auf Servern zwischengespeichert, während die eigentliche MMS nur die notwendigen Links zu diesen enthält. Dem Empfänger wird die Nachricht mithilfe von WAP Push – einer Push-Technologie ähnlich dem Push Mail Verfahren, die auf WAP basiert – zugestellt. Die eigentlichen Inhalte lädt das Endgerät dann über einen MMS-Proxy von den Servern der Anbieter. Problematisch ist hierbei, dass der MMS Proxy sich gegenüber dem Endgerät nicht authentifizieren muss. So können Inhalte gefälscht oder mit Schadsoftware versetzt und die Identität des Urhebers verschleiert werden, falls die MMS über einen kompromittierten MMS-Proxy ausgeliefert wird. Briant ist auch das MMS-Phishing, bei dem - analog zu dem von Emails bekannten Vorgehen - dem Anwender eine vertrauenswürdige Quelle vorgegaukelt wird, um ihn zur Eingabe persönlicher Daten oder Passwörter zu bewegen. Gegen solche Attacken kann man sich nur durch gesunden Menschenverstand beim Umgang mit MMS schützen.

Umsichtig handeln

Gesunder Menschenverstand ist auch bei der Nutzung von elektronischen Handels- und Bezahlplattformen notwendig. Ob das bequeme Shopping während der U-Bahn-Fahrt nach Feierabend oder

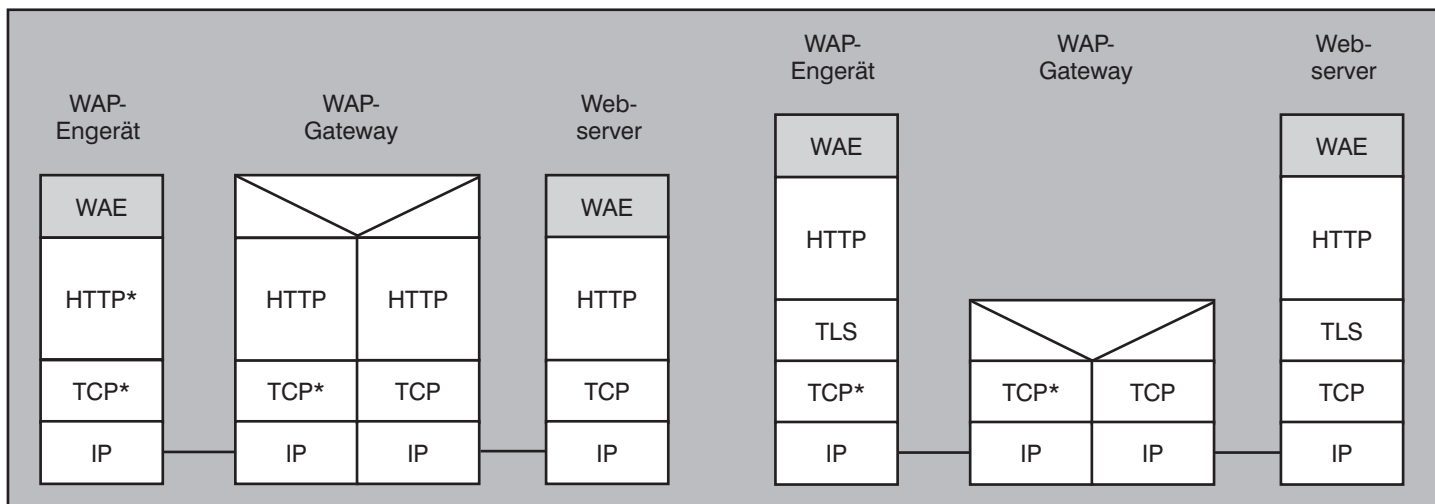


Abbildung 9: WAP 2.0 mit (l.) und ohne (r.) Optimierung höherer Protokollschichten

Sicherheitsaspekte öffentlicher Mobilfunknetze - Teil 1

das Lösen eines Tickets für selbige per SMS. M-Commerce und M-Payment sind das mobile Gegenstück zu den mittlerweile etablierten E-Commerce und E-Payment Angeboten des Internets. Dementsprechend sind auch die Gefährdungen ähnlich. Die durch das bereits angesprochene Email- oder MMS-Phishing erlangten Zugangsdaten geben dem Angreifer nicht nur Einblick in die Gewohnheiten des Nutzers. Sie können vielmehr ganz konkrete, wirtschaftliche Folgen für den Einzelnen haben. Doch es braucht noch nicht einmal einen gewaltigen technischen Aufwand, um in Besitz der Zugangsdaten zu gelangen. Ein simpler Blick über die Schulter eines ahnungslos Einkaufenden genügt, und schon können Zahlungen von seinem Account aus vorgenommen werden. Ein umsichtiger Umgang mit solchen Angeboten sollte also selbstverständlich sein (gilt übrigens auch für Notebook-Nutzer, denn mit den auf einer einzigen Bahnreise in der 1. Klasse mühelos gewinnbaren Informationen lassen sich ganze Wirtschaftsteile einer Zeitung füllen).

Darüber hinaus ist die Auswahl der genutzten Plattformen ausschlaggebend. Prinzipiell dürfen nur Angebote genutzt werden, bei denen persönliche Daten und Zahlungsinformationen verschlüsselt übertragen werden. Bei für den mobilen Einsatz zugeschnittenen Webplattformen geschieht das meist per Secure Sockets Layer (SSL), das in Kombination mit HTTP in Form von HTTPS Verwendung findet (erkennbar am „https://“ zu Beginn der Adresse). So gesicherte Verbindungen sind prinzipiell unbedenklich. Allerdings muss dennoch auf die Vertrauenswürdigkeit des Anbieters geachtet werden. Denn was nutzt eine sichere Verbindung, wenn die Gegenseite kompromittiert ist. Brauchbare Kriterien sind hier eventuelle Zertifizierungen und die Beständigkeit des Anbieters am Markt. Plattformen für die mobile Nutzung sind durch ihren Komfort sehr attraktiv für den Kunden. Damit können sie für viele Unternehmen eine gewinnbringende Ergänzung der Vertriebswege sein, insbesondere wenn diese mit ihren Produkten den privaten Endverbraucher adressieren. Ein Nachweis der Sicherheit eines solchen Angebots, z.B. durch Security Audits, sollte daher im ureigensten Interesse der Anbieter liegen.

Fazit

Der öffentliche Mobilfunk birgt eine Reihe von Tücken in puncto Sicherheit. Ein bewusster und umsichtiger Umgang mit diesem Medium ist dringend geboten, und das nicht nur, wenn es um den

Schutz von Geschäftsgeheimnissen geht. Auf die Sicherheit der verwendeten Netztechnologie hat der Kunde keinen oder nur indirekten Einfluss. Hier ist auf Kundenseite viel Vertrauen in die Gewissenhaftigkeit der Netzbetreiber notwendig. Bleibt zu hoffen, dass diese das Vertrauen auf Vorschuss zu würdigen wissen und dem Kunden in Zukunft ein höheres Maß an Sicherheit und Transparenz gewähren.

Doch die Sicherheit der Netztechnologie alleine hilft nicht, wenn die zur Verfügung gestellten Dienste selbst Teil des Problems sind. Ob Ende-zu-Ende-Sicherheit bei Datendiensten oder Deaktivierung nicht genutzter oder potentiell unsicherer Leistungsmerkmale - der Anwender kann einiges zum Schutz seiner Privatsphäre und seiner Daten beitragen. Mit dem Wissen um die Gefährdungen und ein wenig gesundem Menschenverstand lassen sich viele Fallen der mobilen Datenwelt vermeiden. Eine umsichtige Planung der Nutzung von mobilen Endgeräten und Diensten ist für Unternehmen dennoch unerlässlich. Die Sicherheitsstandards, die auf viele Unternehmensnetze bereits heute angewendet werden, müssen auch die mobilen Teilnehmer erfassen, um die Wirksamkeit des Gesamtkonzepts sicherzustellen.

In der täglichen Praxis fällt jedoch immer wieder auf, dass Unternehmen zwar intensiv den Schutz ihrer eigenen Netze betreiben, den mobilen Zugriffsmöglichkeiten ihrer Mitarbeiter aber vergleichsweise unkritisch gegenüberstehen. Wenn man berücksichtigt, dass die mobilen Endgeräte und öffentlich Mobilfunknetze immer leistungsfähiger werden, ist das aber eine äußerst bedenkliche Herangehensweise. Denn eines ist klar: Gelangt ein ungeschütztes mobiles Endgerät in falsche Hände, bestehen fast alle Möglichkeiten, auf unternehmenskritische Daten zuzugreifen. Dazu gehören nicht nur die Daten auf dem Endgerät selbst, sondern auch die Unternehmensdaten, auf die vom Endgerät aus zugegriffen werden kann.

Es muss demnach als höchst fahrlässig betrachtet werden, wenn sich die IT-Verantwortlichen eines Unternehmens auf die Betreiber von Mobilfunknetzen oder die Anbieter von mobilen Diensten verlassen. Zu groß ist die Gefahr, dass sensible und geschäftskritische Daten aufgrund von inhomogenen Sicherheitskonzepten und arglosem Endanwenderverhalten das Unternehmen verlassen. Ein solches Risiko kann sich kein Unternehmen auf lange Sicht leisten, Unternehmen in

einem verschärften Wettbewerbsumfeld nicht mal kurzzeitig. Was der einzelne Anwender und Unternehmen tun können, um sensible Daten vor dem Zugriff Dritter zu schützen, wird das Thema des zweiten Teils dieses Artikels sein.

Literatur

Pressemitteilung „Fast jeder zweite Mensch telefoniert mobil“ vom 05.06.2007, Branchenverband BITKOM, http://www.bitkom.de/de/presse/30739_46282.aspx, (zuletzt überprüft: 22.09.2008)

Technische Referenzen und Mobilfunkstandards der dritten Generation von Mobilfunknetzen, The 3rd Generation Partnership Project, <http://www.3gpp.org/specs/specs.htm>, (zuletzt überprüft: 22.09.2008)

Pressemitteilung des Bundesministerium der Justiz zum Thema Vorratsdatenspeicherung vom 09. November 2007, http://www.bmj.bund.de/enid/cf71891a0cf2593af66c730,46bdaa706d635f6964092d0934383133093a095f7472636964092d0933303334/Pressestelle/Pressemitteilungen_58.html, (zuletzt überprüft: 22.09.2008)

Deutscher Bundestag Drucksache 16/5846, 27. Juni 2007, „Entwurf eines Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“ - <http://dip.bundestag.de/btd/16/058/1605846.pdf>, (zuletzt überprüft: 22.09.2008)

Broschüre „Öffentliche Mobilfunknetze und ihre Sicherheitsaspekte“, Bundesamt für Sicherheit in der Informationstechnik, <http://www.bsi.de/literat/doc/oefms/index.htm>, (zuletzt überprüft: 22.09.2008)

Artikel „Telekom bespitzelte mehrere Journalisten“ vom 10.09.2008, Onlineangebot des Handelsblattes, <http://www.handelsblatt.com/unternehmen/it-medien/telekom-bespitzelte-mehrere-journalisten;2035251>, (zuletzt überprüft: 22.09.2008)

Pressemitteilung „Über 10 Millionen UMTS-Nutzer in Deutschland“ vom 10.02.2008, Branchenverband BITKOM, http://www.bitkom.de/de/presse/30739_50446.aspx, (zuletzt überprüft: 22.09.2008)