14 Sicherheitsaspekte der Mobilkommunikation

Der dritte Teil dieses Buches ist spezifischen Sicherheitsaspekten der Mobilkommunikation gewidmet. In diesem Kapitel werden zunächst generelle Aspekte hierzu betrachtet, bevor in den folgenden Kapiteln konkrete Systembeispiele diskutiert werden. Kapitel 15 beschreibt die Sicherheitsmechanismen in drahtlosen lokalen Netzen nach dem Standard IEEE 802.11 und geht intensiv auf die Sicherheitsdefizite dieses Standards und mögliche Lösungsalternativen hierfür ein. Das sich anschließende Kapitel 16 behandelt Sicherheitsaspekte in funkbasierten Weitverkehrsnetzen. In diesem Zusammenhang werden die Sicherheitsmechanismen von GSM-Netzen und die auf ähnlichen Prinzipien beruhenden Verfahren für UMTS/LTE-Netze behandelt.

14.1 Bedrohungen in Mobilkommunikationsnetzen

Ergeben sich in Mobilkommunikationsnetzen neue Sicherheitsaspekte?

Im Rahmen einer umfassenden Betrachtung der ingenieurwissenschaftlichen Disziplin Netzsicherheit ist in Bezug auf Mobilkommunikationsnetze zunächst die Frage legitim, inwieweit sich aus den Umständen und technischen Eigenschaften der Mobilkommunikation neue Sicherheitsaspekte und Lösungsansätze ergeben. Hierzu ist zunächst festzuhalten, dass die Mobilkommunikation natürlich all den Bedrohungen ausgesetzt ist, die auch bereits bei der Festnetzkommunikation zu beachten sind, das heißt Vortäuschen einer Identität (Maskerade), Autorisierungsverletzung, Abhören, Verlust, Modifikation oder Fälschung übertragener Dateneinheiten, Abstreiten von Kommunikationsvorgängen sowie Sabotage. Demzufolge müssen auch in Mobilkommunikationsnetzen ähnliche Maßnahmen wie in Festnetzen ergriffen werden.

Spezifische Aspekte

Darüber hinaus ergeben sich aus der Mobilität der Benutzer beziehungsweise ihrer Geräte und dem Vorhandensein drahtloser

Kommunikationsabschnitte jedoch auch noch eine Reihe spezifischer Aspekte, die in dieser Form nicht in Festnetzen auftreten:

Verstärkung des Risikopotenzials

- Einige bereits in Festnetzen bestehende Bedrohungen weisen ein größeres Risikopotenzial auf: So können beispielsweise drahtlose Übertragungsstrecken erheblich leichter abgehört werden als leitungsgeführte Übertragungsmedien, da der direkte physikalische Zugang in der Regel sehr einfach zu erhalten ist. Aus dem gleichen Grund können die Dienste eines drahtlosen Netzes auch einfacher von unbefugten Instanzen genutzt werden, sofern keine adäquaten Sicherungsmechanismen vorgesehen werden.

Neue Schwierigkeiten bei der Realisierung von Sicherheitsdiensten

- Es treten einige neue Schwierigkeiten bei der Realisierung von Sicherheitsdiensten auf: So muss beispielsweise die Authentizität mobiler Geräte von den jeweiligen Netzzugangspunkten immer neu verifiziert werden, wenn ein Gerät den Netzzugangspunkt wechselt, also einen sogenannten *Handover* ausführt. Die Schlüsselverwaltung stellt sich in diesem Zusammenhang auch deutlich schwieriger dar, weil die jeweiligen Partnerinstanzen im Allgemeinen nicht vorherbestimmt werden können, da sie ja von den Bewegungen des Benutzers abhängen.

Vertrauen in globalen Netzen

- Bei global verfügbaren Mobilfunknetzen, wie dem GSM-Netz, muss eine Authentifizierung der Nutzer sicher möglich sein, selbst wenn Nutzern und Providern von Fremdnetzen nicht vollständig vertraut wird.

Erstellung von Bewegungsprofilen

- Schließlich ergibt sich auch eine komplett neue Bedrohung: Der momentane Aufenthaltsort eines Gerätes und damit seines Benutzers stellt eine erheblich interessantere Information dar als in Festnetzen und sollte daher vor Ausspähen geschützt werden.

Während die ersten drei Aspekte in den folgenden Kapiteln bei der Betrachtung konkreter Systembeispiele ausführlich behandelt werden, können hingegen in Bezug auf die Vertraulichkeit des momentanen Aufenthaltsortes bei den bisher implementierten Architekturen lediglich Schwachstellen und bestenfalls Ansätze zu ihrer Lösung identifiziert werden. Ansätze zur Wahrung der Vertraulichkeit des Aufenthaltsortes sind bisher hauptsächlich in der Forschung untersucht worden und haben kaum Eingang in praktisch eingesetzte Architekturen der Mobilkommunikation gefunden. Aus diesem Grund werden sie im folgenden Abschnitt im Rahmen

einer allgemeinen Betrachtung unabhängig von konkreten Systembeispielen behandelt.

14.2 Wahrung der Vertraulichkeit des Aufenthaltsortes

Wie sich in den folgenden Kapiteln noch zeigen wird, verfügen heutige Mobilkommunikationsnetze über keine ausreichenden Maßnahmen für einen adäquaten Schutz der Information über den aktuellen Aufenthaltsort eines mobilen Gerätes, im Englischen auch kurz mit *Location Privacy* bezeichnet. Im Vorgriff auf die ausführlichere Untersuchung dieses Aspektes in den folgenden Kapiteln sind hierzu insgesamt die folgenden Defizite festzustellen:

- *Wireless LANs*
  In drahtlosen lokalen Netzen wird die Identität mobiler Geräte nicht vor lokalem Abhören auf der Funkschnittstelle geschützt, da jeder Übertragungsrahmen die im Prinzip weltweit eindeutige MAC-Adresse des Netzwerkadapters im Klartext enthält. Sofern sie nicht zu einer ohnehin unsicheren Authentisierung verwendet wird, kann die MAC-Adresse zwar theoretisch mit jedem Anmelden an einem WLAN geändert werden, praktisch wird eine solche Maßnahme jedoch nicht im größeren Maßstab vorgenommen. Besitzt ein Gerät mehrere Funkschnittstellen, etwa das in diesem Buch nicht näher betrachtete Bluetooth, oder ein Nutzer mehrere Geräte mit Funkschnittstellen, müssten zudem die Adressen aller Schnittstellen gleichzeitig gewechselt werden, andernfalls ist eine einfache Verknüpfung der Adressinformationen möglich.
- *GSM, UMTS & LTE*
  In GSM-, UMTS- und LTE-Netzen können aktive Angreifer die weltweit eindeutigen Identifikationen (sogenannte IMSI) mobiler Geräte abfragen, sofern sie gefälschte Signalisierungsnachrichten über die Funkschnittstelle an die Geräte senden und von diesen empfangen können. Weiterhin kann der Betreiber eines »besuchten« Zugangsnetzes die Bewegungen der bei ihm aktuell registrierten Geräte überwachen und ihrer eindeutigen Identifikation zuordnen. Der vertragliche Netzbetreiber eines mobilen Gerätes, der sogenannte Heimatnetzbetreiber, kann die Bewegungen des Gerätes sogar weitgehend vollständig überwachen, da er auch von den »besuchten« Netzen Signalisierungs- beziehungsweise Abrechnungsdatensätze für die vertraglich an ihn gebundenen Geräte erhält. Den Kommunikationspartnern eines mobilen Gerätes gegenüber

wird der momentane Aufenthaltsort des Gerätes wenigstens verborgen, sodass diese Information eigentlich nur Netzbetreibern (und gegebenenfalls Strafverfolgungsbehörden) zugänglich ist.

Mobile Internetnutzung

- Bei der mobilen Nutzung von Internetdiensten ist ein weiterer Aspekte in Bezug auf die Wahrung der Vertraulichkeit des Aufenthaltsortes des Benutzers zu bedenken: Es stellt sich die Frage, ob Instanzen, mit denen der mobile Rechner kommuniziert, ein Bewegungsprofil des entsprechenden Nutzers erstellen können. In dieser Hinsicht bietet ein Zugang über WLAN in der Regel gute Möglichkeiten für die korrespondierenden Rechner, Rückschlüsse auf den momentanen Aufenthaltsort zu ziehen, da die extern sichtbaren IP-Adressen in solchen Netzen oft recht scharf auf einige wenige geografische Bereiche, etwa große Städte, abgebildet werden können. Bei Mobilfunknetzen hingegen lassen die einem mobilen Gerät zugeordneten IP-Adressen in der Regel nur relativ unscharfe Rückschlüsse auf den aktuellen Aufenthaltsort des mobilen Gerätes zu (zum Beispiel auf den Betreiber des besuchten Netzes und damit auf das aktuell besuchte Land).

Zielkonflikt zwischen Erreichbarkeit und Unbeobachtbarkeit

Das grundsätzliche Problem beim Entwurf von Mobilkommunikationssystemen in Bezug auf die Vertraulichkeit des Aufenthaltsortes mobiler Geräte besteht in dem Zielkonflikt, dass einerseits mobile Geräte erreichbar für ankommende Kommunikationsanfragen sein sollen, andererseits ihr momentaner Aufenthaltsort nicht durch (einzelne) Instanzen im Netz permanent überwacht werden können soll.

In den vergangenen Jahren ist eine Reihe grundsätzlicher Ansätze für dieses Problem vorgeschlagen worden [MR99]:

Broadcast

- *Rundrufübermittlung von Nachrichten (Broadcast):* Hierbei werden alle Nachrichten an alle potenziellen Empfänger gesendet, sodass der Aufenthaltsort der Empfänger nicht bekannt sein muss. Soll zusätzlich die Vertraulichkeit der übermittelten Nachrichten gewährleistet werden, so werden alle Nachrichten noch mit dem öffentlichen Schlüssel des jeweiligen Empfängers chiffriert. Konsequenterweise müssen in diesem Fall alle potenziellen Empfänger jeweils alle Nachrichten dechiffrieren, um die für sie bestimmten Nachrichten herauszufiltern. Es liegt auf der Hand, dass dieser Ansatz nicht für große Netzwerke oder große Nachrichtenaufkommen skaliert.

- *Temporäre Pseudonyme:* Bei diesem Ansatz verwenden alle mobilen Geräte nicht ihre tatsächliche Identität, sondern werden über regelmäßig wechselnde Pseudonyme adressiert. Damit ein mobiles Gerät erreichbar sein kann, wird eine Instanz für die Abbildung auf das aktuelle temporäre Pseudonym des Gerätes benötigt. Diese Instanz kann jedoch prinzipbedingt die Abfolge der temporären Pseudonyme eines spezifischen Gerätes nachvollziehen und aufzeichnen.

Temporäre Pseudonyme

- *Mix-Netzwerke:* Nachrichten werden im Netz über Instanzen geleitet, die jeweils nur einen Teil des Weges einer Nachricht in Erfahrung bringen können und die als *Kommunikations-Mixe* bezeichnet werden (zur Funktionsweise dieses Ansatzes siehe unten).

Mix-Netzwerke

In den folgenden Abschnitten wird eine Reihe von Details dieser Ansätze vertieft betrachtet.

14.2.1 Broadcast-Kommunikation

Explizite vs. implizite Adressen

In Bezug auf die Adressierung mobiler Geräte bei Broadcast-Kommunikation kann weiterhin zwischen *expliziten* und *impliziten Adressen* unterschieden werden. Bei Verwendung expliziter Adressen (zum Beispiel IP-Adressen) ist jede Instanz, die eine bestimmte Nachricht »sieht«, in der Lage, die adressierte Instanz zu bestimmen. Implizite Adressen zeichnen sich hingegen dadurch aus, dass sie kein bestimmtes Gerät oder keinen bestimmten Ort identifizieren, sondern lediglich eine Instanz benennen, ohne dass mit dem Namen eine weitere Bedeutung verknüpft ist. Implizite Adressen werden in der Regel zufällig aus einem ausreichend großen Adressraum gewählt, um die Wahrscheinlichkeit zufälliger Kollisionen gering zu halten.

Offene und verdeckte implizite Adressen

Bei impliziten Adressen wird weiterhin zwischen *offenen (sichtbaren)* und *verdeckten (unsichtbaren) impliziten Adressen* unterschieden. Der Unterschied zwischen den beiden Varianten besteht darin, dass bei mehrfachem Auftreten der gleichen sichtbaren Adresse jede Instanz die Gleichheit der sichtbaren Adresse erfahren kann, wogegen unsichtbare implizite Adressen nur von der adressierten Instanz auf Gleichheit überprüft werden können.

Realisierung verdeckter impliziter Adressen

Die Realisierung verdeckter impliziter Adressen stützt sich auf Public-Key-Operationen. Die zu adressierende Instanz A wählt hierfür eine Zufallszahl r_A und gibt sie zusammen mit ihrem öffentlichen Schlüssel $+K_A$ an potenzielle Kommunikationspartner bekannt. Will zu einem späteren Zeitpunkt die Instanz B eine

Nachricht an A senden, so wählt sie eine Zufallszahl r_B und erstellt die folgende verdeckte implizite Adresse für A: $ImplAddr_A = \{r_B, r_A\}_{+K_A}$. Wird diese Adresse in einer Broadcast-Nachricht versendet, so kann lediglich A feststellen, dass sie darin adressiert wurde, da sie die einzige Instanz ist, welche die Adresse korrekt entschlüsseln kann.

14.2.2 Temporäre Pseudonyme

Grundidee temporärer Pseudonyme

Die Grundidee beim Einsatz temporärer Pseudonyme zur Wahrung der Vertraulichkeit des aktuellen Aufenthaltsortes mobiler Geräte ist, dass der momentane Aufenthaltsort eines Gerätes nicht mehr gemeinsam mit seiner Identifikation ID_A, sondern mit einem zeitlich wechselnden Pseudonym $P_A(t)$ gespeichert wird. Die Abbildung der Identität ID_A auf das aktuelle temporäre Pseudonym $P_A(t)$ wird durch eine vertrauenswürdige Instanz durchgeführt, die ihrerseits nicht wissen muss, wo sich das Gerät zu einem bestimmten Zeitpunkt aufhält.

Weiterleitung von Nachrichten

Wenn eine eingehende Nachricht zu dem aktuellen Aufenthaltsort des Gerätes A geleitet werden muss, so erfolgt diese Operation in zwei Schritten:

1. Zunächst wird die Identität ID_A auf das aktuelle temporäre Pseudonym $P_A(t)$ abgebildet und in der Nachricht die Adressierungsinformation entsprechend angepasst.
2. Im zweiten Schritt wird die Nachricht zu dem aktuellen Aufenthaltsort des Gerätes weitergeleitet (zum Beispiel durch Auswerten einer Datenbank mit den aktuellen Aufenthaltsorten aller temporären Pseudonyme).

Erbringung durch unabhängige Instanzen

Falls diese beiden Funktionalitäten durch unabhängige Instanzen erbracht werden, kann gewährleistet werden, dass keine einzelne Instanz Bewegungsprofile mobiler Geräte erstellen kann.

Hierfür ist es selbstverständlich von zentraler Bedeutung, dass die Instanzen, welche die Nachricht nach der Eintragung des temporären Pseudonyms weiterleiten, der Nachricht keine Information über die tatsächliche Identität ID_A des Empfängers entnehmen können.

Durch den Einsatz der im folgenden Abschnitt erklärten Kommunikations-Mixe kann ein zusätzlicher Schutz realisiert werden, der verhindert, dass mehrere Instanzen im Netz unrechtmäßig Informationen austauschen, um die Information über das Bewegungsprofil eines mobilen Gerätes dennoch aufzudecken.

14.2.3 Kommunikations-Mixe

Grundidee von Kommunikations-Mixen

Das Konzept der Kommunikations-Mixe wurde 1981 von D. Chaum für unbeobachtbare E-Mail-Kommunikation erfunden. Ein Kommunikations-Mix verschleiert die Kommunikationsbeziehungen zwischen Sender und Empfänger mit den folgenden Maßnahmen:

Funktion von Kommunikations-Mixen

- Er nimmt eine temporäre Speicherung eingehender Nachrichten vor, die mit seinem öffentlichen Schlüssel chiffriert sind,
- er ändert die Gestalt der Nachrichten, indem er sie mit seinem privaten Schlüssel dechiffriert, und
- er ändert die Reihenfolge der Nachrichten und leitet sie jeweils in Bündeln weiter (engl. *batch processing*).

Auf diese Weise wird – bei Vorliegen eines ausreichenden Verkehrsaufkommens – erreicht, dass ein Angreifer, der alle eingehenden und ausgehenden Nachrichten eines Kommunikations-Mixes lesen kann, dennoch keine Zuordnung der eingehenden zu den ausgehenden Nachrichten vornehmen kann und somit keine Schlüsse über die Beziehungen zwischen Sendern und Empfängern ziehen kann.

Kaskadierung von Kommunikations-Mixen

Gelingt einem Angreifer jedoch die Kompromittierung des Kommunikations-Mixes, so kann dieser prinzipbedingt keinen Schutz mehr bieten. Dieser Gefahr kann durch eine zusätzliche Kaskadierung von Kommunikations-Mixen begegnet werden. Ein Sender A kann beispielsweise eine Nachricht m im Prinzip wie folgt unter Einbeziehung der beiden Kommunikations-Mixe $M1$ und $M2$ unbeobachtbar an den Empfänger B schicken:

$$\begin{aligned} A \rightarrow M_1\colon &\quad \left\{r_1, M2, \{r_2, B, \{r_3, m\}_{+K_B}\}_{+K_{M2}}\right\}_{+K_{M1}} \\ M_1 \rightarrow M_2\colon &\quad \left\{r_2, B, \{r_3, m\}_{+K_B}\right\}_{+K_{M2}} \\ M_2 \rightarrow \ \ B\colon &\quad \left\{r_3, m\right\}_{+K_B} \end{aligned}$$

Erforderliches Nachrichtenaufkommen

Es ist jedoch von grundsätzlicher Bedeutung für die Sicherheit dieses Schemas, dass alle Kommunikations-Mixe eine ausreichende Anzahl von Nachrichten verarbeiten. Für das Verstehen dieser Anforderung stelle man sich beispielsweise ein Netz von Kommunikations-Mixen vor, durch welches im Extremfall nur eine einzige Nachricht geleitet wird. Obwohl in jedem Mix eine Umcodierung vorgenommen wird, kann ein Angreifer, der alle Kommunikationsverbindungen abhören kann, den Weg der Nachricht durch die kaskadierten Mixe verfolgen. Aus dem gleichen Grund sollten alle Nachrichten eine ähnliche Länge haben. Die Idee der kaskadierten

Netze wurde bereits konzeptionell auf Mobilkommunikationssysteme übertragen [MR99].

14.3 Zusammenfassung

Verstärkung bestehender Risikopotenziale

In Mobilkommunikationsnetzen und drahtlosen lokalen Netzen existieren die gleichen Bedrohungen wie auch in Festnetzen. Darüber hinaus verstärkt sich durch das Vorhandensein einer drahtlosen Übertragungsstrecke das Bedrohungspotenzial erheblich und es kommt eine Reihe von Schwierigkeiten bei der Realisierung von Sicherheitsdiensten (zum Beispiel Schlüsselmanagement für die Authentisierung im Zugangsnetzbereich) hinzu.

Neue Bedrohung »Erstellung von Bewegungsprofilen«

Weiterhin ergibt sich aus der Mobilität der Geräte und ihrer Benutzer die neue Bedrohung, dass Bewegungsprofile einzelner Geräte erstellt werden können. Es sind in der Vergangenheit eine Reihe theoretischer Konzepte vorgeschlagen worden, um dieser Bedrohung zu begegnen: die Nachrichtenübermittlung per Rundruf (Broadcast), die Verwendung temporärer Pseudonyme und der Einsatz kaskadierter Kommunikations-Mixe, welche die Verbindung zwischen eingehenden und ausgehenden Nachrichten verschleiern. Eine Übertragung dieser Ideen auf in der Praxis eingesetzte Mobilkommunikationsnetze wurde bisher lediglich auf konzeptioneller Ebene geleistet. Die folgenden Kapitel dieses Buchteiles sind konkreten Systembeispielen gewidmet.

14.4 Weiterführende Literatur

[MR99] MÜLLER, G.; RANNENBERG, K. (Hrsg.): *Multilateral Security in Communications*. Addison-Wesley-Longman, 1999

[Sch03] SCHILLER, J.: *Mobilkommunikation*. Addison-Wesley, 2003
Dieses Buch bietet eine umfassende Einführung in die Grundprinzipien der in den folgenden Kapiteln betrachteten Systembeispiele. Es wird ergänzend empfohlen, da in diesem Buch ausschließlich sicherheitsrelevante Aspekte diskutiert werden.

14.5 Übungen

1. Welche neuen Bedrohungen und Schwierigkeiten in Bezug auf die Kommunikations- und Netzsicherheit ergeben sich bei Mobilkommunikationssystemen im Vergleich zur Festnetzkommunikation?
2. Warum sollte bei einem Handover eines mobilen Endgerätes von einer Basisstation zu einer anderen die Authentizität des Endgerätes erneut überprüft werden?
3. Wie gut skaliert das Verfahren der verdeckten (unsichtbaren) impliziten Adressen mit einer steigenden Anzahl versendeter Nachrichten?
4. Erörtern Sie die Einsatzmöglichkeiten kaskadierter Kommunikations-Mixe für interaktive Anwendungen wie Internettelefonie oder Videokonferenzdienste.