Ein Überblick über Ansätze zur Vermeidung der Manipulation von Ortungsverfahren

Michael Decker
Institut AIFB, Universität Karlsruhe (TH)
76128 Karlsruhe
decker@aifb.uni-karlsruhe.de

Abstract: Die Verfügbarkeit von Ortungsverfahren zur Positionsbestimmung von mobilen Endgeräten wie Mobilfunktelefonen oder PDAs ermöglicht eine eigene Klasse von neuartigen Anwendungen, die sog. Location Based Services (LBS). In den einschlägigen Arbeiten wird jedoch fast nie betrachtet, inwiefern die Ortungsverfahren robust gegenüber Manipulationsversuchen („Location-Spoofing") durch Dritte oder die (möglicherweise illegitimen) Besitzer des Endgerätes selbst sind. Es werden deshalb zur Motivation zunächst einige Anwendungsszenarien genannt, für die spezielle manipulationsresistente Ortungsverfahren benötigt werden. Darauf aufbauend werden dann verschiedene grundlegende Ansätze zur Vermeidung von Location-Spoofing klassifiziert und beschrieben. Es wird auch darauf eingegangen, welche besonderen Anforderungen die einzelnen Verfahren an die Endgeräte stellen und für welche Anwendungsszenarien sie geeignet sind.

1 Einleitung und Motivation

Unter Ortung versteht man die Ermittlung des Aufenthaltsortes eines mobilen Gerätes. Meistens handelt es sich bei diesem Gerät um ein von einem Nutzer ständig mitgeführtes persönliches Kommunikationsgerät wie z.B. Mobilfunktelefon, Notebooks oder PDA mit der Möglichkeit zur drahtlosen Datenkommunikation über Technologien wie GPRS, UMTS oder WiFi. Mittlerweile stehen zahlreiche technische Verfahren zur Realisierung von Ortung zur Verfügung (z.B. [TuPo04, 74ff] oder [Küpp05, 155ff]):

- Das wohl bekannteste Ortungssystem ist das satellitengestützte „Global Positioning System" (NAVSTAR GPS) der USA, mit dem eine Genauigkeit bis auf ca. 15 m Meter erzielt werden kann. Mit zusätzlichen Korrektursignalen von terrestrischen Referenzstationen (sog. Differential GPS, D-GPS) kann eine Genauigkeit bis auf wenige cm erreicht werden.

- In zellular aufgebauten Funknetzen (z.B. Mobilfunknetze) kann anhand der Kenntnis der verwendeten Basisstation eine Positionsbestimmung vorgenommen werden (Zellortung). Je nach Größe der von einer Basisstation bedienten Funkzelle beträgt die Ortungsgenauigkeit zwischen 100 Metern (in Ballungszentren) oder 35 Kilometern (im ländlichen Raum). Durch Hinzunahme weiterer Basisstationen (Triangulation) oder Berücksichtigung der Laufzeiten kann die so erzielte Genauigkeit weiter verbessert werden.

- Die genannten Verfahren sind für Anwendungen in Gebäuden leider wenig geeignet, so dass auch spezielle Indoor-Verfahren entwickelt wurden, z.B. WLAN-Fingerprinting oder RFID-basierte Systeme. Mit diesen Systemen sind Genauigkeiten von 1-2 m erreichbar.

Mobile Anwendungen, die den über ein oder mehrere Ortungsverfahren ermittelten Aufenthaltsort eines mobilen Endgerätes auswerten, werden als „Location-based Services" (LBS) bezeichnet [TuPo04, 73ff]. Hierbei muss das geortete Endgerät nicht notwendigerweise das Gerät des Dienstaufrufers sein: bei sog. Tracking-Diensten (z.B. http://www.track-your-kid.de) initiiert der Nutzer mit seinem Endgerät die Ortung eines anderen Endgerätes. Ein weiteres klassisches Beispiel für LBS sind sog. POI-Finder-Dienste: ein POI (Point-of-Interest) ist hierbei eine bestimmte stationäre Einrichtung, die typischerweise für einen Reisenden oder Ortsunkundigen von Interesse ist, z.B. eine Sehenswürdigkeit, ein Restaurant, Hotel oder Tankstelle. Mit einem POI-Finder-Dienst kann sich der Nutzer ohne mühsame Eingabe seines aktuellen Aufenthaltsortes — den er vielleicht auch gar nicht genau genug kennt — den nächstgelegenen POI einer bestimmten Kategorie (z.B. Apotheke) anzeigen lassen, ggf. ist auch eine Navigation an diesen Ort hin möglich.

Bei der Entwicklung von Ortungsverfahren steht meist die räumliche Präzision der erzielten Ortung im Vordergrund; die Absicherung eines Ortungsverfahrens gegen bewusste Manipulationsversuche durch den mobilen Nutzer selbst (interner Angriff) oder einen Dritten (externer Angriff) wird meist nicht behandelt, wohl weil sich aus den üblicherweise herangezogenen Anwendungsszenarien keine Motivation für einen Beteiligten oder potenzielle Angreifer ergibt, erheblichen technischen Aufwand zu betreiben, um die Ortung zu manipulieren. Es lassen sich aber durchaus Anwendungen finden, bei denen dies nicht der Fall ist, so dass bei der Entwicklung die Absicherung gegen interne und/oder externe Manipulationen von Bedeutung ist:

- Unter Zugriffskontrolle (Access Control) werden Maßnahmen und Techniken verstanden, um zu entscheiden, ob einem bestimmten Nutzer eines Informationssystems gestattet werden soll, eine bestimmte Operation (z.B. lesen, schreiben, löschen, ausführen) auf einer bestimmten Ressource (z.B. Datei, Datenbankobjekt, Dienst) auszuführen. Die hierfür zuständige Komponente (Soft- und/oder Hardware) wird als Referenz-Monitor bezeichnet. Bei der sog. ortsabhängigen Zugriffs wird für diese Entscheidung nicht nur die Identität oder Gruppen-/Rollenzugehörigkeit des jeweiligen Nutzers ausgewertet, sondern auch dessen aktueller Aufenthaltsort (z.B. [DaBP07]). So lassen sich Sicherheitspolitiken umsetzen, die etwa den Zugriff auf vertrauliche Dateien außerhalb des Betriebsgeländes oder aus Ländern mit Spionagegefahr verbieten. Dieser Anwendungsfall stellt übrigens die ursprüngliche Motivation für den vorliegenden Artikel dar. Bemerkenswerterweise wird in den einschlägigen Veröffentlichungen mit ortsbewussten Zugriffskontrollmodellen die Manipulationsresistenz von Ortungsverfahren nicht thematisiert.

- Anstelle die Ortung als zusätzliche Information neben der Identität eines Nutzers für eine Zugriffsentscheidung auszuwerten, kann es auch sinnvoll sein, *nur* die Ortsinformation auszuwerten, wenn nämlich der Aufenthalt an einem bestimmten Ort

schon als Berechtigungsnachweis gewertet werden kann. Dies wäre etwa der Fall für eine Unternehmensabteilung oder ein Gelände, deren/dessen Zugang mit herkömmlichen Mitteln (etwa Wachpersonal, Zäune, verschließbare Türen, Mauern) gesichert ist. Eine rein ortsbasierte Zugriffskontrolle hat den Vorteil, dass nicht automatisch mit dem Zugriff auf gesicherte Ressourcen ein Nutzungsprofil der jeweiligen Nutzer erstellt wird (z.B. Nutzer X erscheint immer erst um 10 Uhr am Arbeitsplatz).

- Bestimmte mobile Dienste sollen nur dann verfügbar sein, wenn sich der Nutzer in unmittelbarer Nähe zu einem bestimmten physischen Objekt befindet, z.B. bei Diensten zur Fernsteuerung von (beweglichen) Maschinen/Fahrzeugen, Entriegelung von Türen oder Zugriff auf Drucker.

- Werden Navigationsdienste für militärische Fahrzeuge oder Werttransporte genutzt, so könnte eine externe Manipulation der Ortung genutzt werden, das Fahrzeug in einen Hinterhalt zu locken[1].

- Ortungstechnologien werden auch zur Nachverfolgung des Aufenthaltsortes von verurteilten Straftätern („elektronische Fußfessel“[2]) und Werttransporten verwendet, so dass hier interne Manipulationen zu befürchten sind. Weiter gibt es die Anwendung, dass ein Alarm ausgelöst werden soll, wenn hochwertige bewegliche Güter (z.B. Baumaschinen) einen bestimmten definierten Bereich (z.B. Baustelle, Firmengelände) verlassen („Geofencing“).

- Im Rahmen von Digital Rights Management (DRM) sind Fälle denkbar, in denen digitaler Content mit mobilen Endgeräten nur an bestimmten Orten (z.B. Ländern) wiedergegeben werden kann [GaWo98, Mund05], da z.B. ein Spielfilm vom entsprechenden Anbieter nur für ein bestimmtes Land lizenziert wurde (vgl. auch DVD-Region-Codes). Denkbar wäre auch eine Beschränkung der Lizenz auf ein Firmengeländer (z.B. Campus- oder Site-Lizenz). Unter der Berücksichtigung der Ortszeit könnte so auch den einschlägigen jugendschutzrechtlichen Bestimmungen bei der Ausstrahlung digitaler Inhalte ohne zusätzliche Authentifizierungsmaßnahmen entsprochen werden, z.B. Streaming von Filmen mit Altersfreigabe ab 16 Jahren erst ab 22 Uhr Ortszeit gem. Jugendmedienschutz-Staatsvertrag (JMStV) §5.

Die bewusste Manipulation von Ortungsverfahren wird in der Literatur mit „Location Spoofing“ (engl. to spoof: täuschen, reinlegen) bezeichnet, wobei dieser Begriff sowohl für externe (z.B. [WaJo03]) als auch interne Manipulationen (z.B. [Mund05]) Verwendung findet. Der Begriff wurde wohl in Anlehnung an Angriffe gewählt, bei denen in drahtgebundenen Netzwerken eine Adressangabe gefälscht wird (z.B. DNS-, IP- oder ARP-Spoofing). Eine reine Verhinderung der Ortung (Denial-of-Service, DoS) etwa durch Störsender („Jamming“) ist meist nicht so gefährlich wie ein Spoofing-Angriff, da dieser vom Angegriffenen erkannt werden kann. Ein interner Angriff liegt auch vor, wenn ein mobiles Endgerät durch Verlust oder Diebstahl in den Besitz einer unbefugten

[1] Z.B. http://www.jamesbondfilms.co.uk/tomorrow-never-dies.htm (letzter Abruf: 17.11.2008)
[2] http://www.justiz.baden-wuerttemberg.de/servlet/PB/menu/1229914/index.html (letzter Abruf: 20.11.2008)

Partei gelangt ist, die dann z.B. unter Laborbedingungen Ortungssignale erzeugen oder Manipulationen an Soft- und/oder Hardware durchführen kann.

Ziel des vorliegenden Artikels ist es, einen Überblick über verschiedene in der Literatur beschriebene grundlegende Anti-Spoofing-Verfahren zugeben. Hierzu wurde auch ein Klassifikationsschema entworfen.

Der verbleibende Teil des vorliegenden Artikels ist wie folgt gegliedert: in Kapitel 2 werden zunächst eine Klassifikation verschiedener Ansätze zur Vermeidung von Spoofing sowie einige für das weitere Verständnis notwendige Konzepte eingeführt. Diese Ansätze werden in den darauf folgenden Kapiteln 3 bis 7 im Einzelnen behandelt. In Kapitel 8 wird kurz auf GPS und Galileo eingegangen, bevor im letzten Kapitel eine Zusammenfassung gegeben wird.

2 Überblick und Grundlagen

Die in der Literatur gefundenen Verfahren zur Vermeidung von Spoofing lassen sich wie folgt klassifizieren (siehe Abbildung 1):

- Plausibilitätskontrollen
- Tamperproof Hardware: Spezielle gegen physische Manipulationen geschützte Hardware
- Location-Keys
- Request-Response-Protokolle
- Funktechnische Maßnahmen

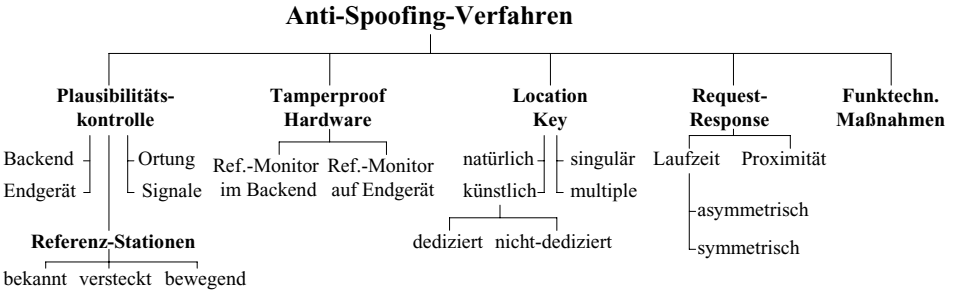

Abbildung 1: Überblick Anti-Spoofing-Verfahren („Anti-Spoofing-Baum“)

Die einzelnen Klassen von Verfahren werden in dieser Reihenfolge in je einem eigenen Kapitel behandelt, wobei dabei noch die einzelnen Unterklassen beschrieben werden. Falls eine entsprechende Aussage möglich ist, wird auch erörtert, ob ein Verfahren nur für Eigenortung (das mobile Endgerät kann selbst die Ortung errechnen) oder Fremdortung (die Ortung wird im stationären Backend des Ortungsnetzwerkes errechnet) ein-

setzbar ist. Weiter wird auch erwähnt, ob die mobilen Endgeräte über bestimmte Ausstattungsmerkmale wie hochpräzise Uhren oder einen drahtlosen Kommunikationskanal mit geringer Latenzzeit verfügen müssen.

Eine Form des Angriffs, die für mehrere Verfahren relevant ist, sind sog. Rerouting-Angriffe (auch „Wormhole-Attack" genannt): hierbei wird ein Funksignal an einer Stelle empfangen und über ein anderes Medium („out-of-Band") an einen Sender weitergeleitet (getunnelt). Ein mobiles Endgerät könnte sich hiermit also Signale weiterleitet lassen, die nur an einem anderen Ort empfangbar sind. Rerouting-Angriffe sind generell nur durch die mit ihnen einhergehende Verzögerung bedingt durch die Out-of-Band-Weiterleitung erkennbar. Durch ein Aufspreizen des Signals auf ein möglich breites Spektrum (siehe Kapitel 7) können sie aber technisch erheblich erschwert werden. Für GPS stehen mit sog. GPS-Repeatern oder Reradiatoren schon kommerzielle Produkte zur Verfügung, die die von einer Antenne empfangenen GPS-Signale an einem über Kabel verbundenen Sender wiedergeben („rerouten"), um damit GPS-Empfang in Verkaufs- oder Laborräumen zu ermöglichen[3]. Beim Replay-Angriff wird ein Signal aufgezeichnet und bewusst zeitverzögert — ggf. an einem anderen Ort — wiedergegeben.

3 Plausibilitätskontrollen

Bei Plausibilitätskontrollen kann unterschieden werden, ob sie auf der errechneten Ortung oder schon den empfangenen „Rohsignale" ansetzt. Ein weiteres Unterscheidungskriterium ist die Komponente des Ortungssystems, die die Kontrolle vornimmt: hier sind das mobile Endgerät selbst, das stationäre Backend des Ortungsnetzwerkes oder dedizierte Referenzstationen möglich.

3.1 Ebene der Plausibilitätskontrolle

Bei Plausibilitätskontrollen auf Signalebene kann die absolute oder relative Stärke der vom Ortungsnetz empfangenen Funksignale überprüft werden [WaJo03]. Dies ist etwa bei GPS eine gute Möglichkeit, von künstlichen Sendern („Pseudoliten") ausgestrahlte Signale zu erkennen, da diese meist vielfach stärker als die aus dem All mit einer Stärke von nur noch -160 dBW empfangbaren Signale sind. Aber auch nur ein mäßiger Pegelanstieg der von mehreren Satelliten empfangenen Signale kann ein Hinweis sein, dass ein Spoofing-Angriff gerade eingesetzt hat. Speziell bei GPS sind die Almanachdaten (groben Laufbahnen der Satelliten für etwa drei Monate im Voraus) über das Internet verfügbar, so dass anhand dieser überprüft werden kann, ob die am vermeintlichen Ort sichtbare Satellitenkonstellation plausibel ist.

Eine Plausibilitätskontrolle kann auch erst dann durchgeführt werden, wenn die Ortung bereits errechnet wurde: hier kann etwa anhand mehrerer aufeinander folgender Ortungen betrachtet werden, ob sich der Nutzer mit einer realistischen Geschwindigkeit fortbewegt oder ob plötzlich „Sprünge" des vermeintlichen Aufenthaltsortes oder Bewegun-

[3] Siehe etwa http://www.gps-world.biz/products/reradproducts.php oder
http://www.navilock.de/produkte/gruppen/22/GPS_Repeater (letzter Abruf jeweils am 12.11.2008)

gen „durch die Wand“ auftreten. Stehen zusätzliche Sensoren am mobilen Endgerät zur Verfügung (Entfernungsmesser, (Kreisel-)Kompass, Beschleunigungs- und Geschwindigkeitsmesser), so kann anhand der von diesen gelieferten Informationen eine Fortschreibung der Ortung vorgenommen werden (Koppelnavigation oder „Dead Reckoning“), so dass spätere Ortsberechnungen des zu überwachenden Ortungssystems auf Plausibilität hin untersucht werden können.

Die erste Form der Plausibilitätskontrolle auf Ebene der „Rohsignale“ eignet sich hauptsächlich für Szenarien mit Eigenortung, die zweite Form kann auch für Fremdortung eingesetzt werden.

3.2 Ort der Plausibilitätskontrolle

Die Plausibilitätskontrolle kann nicht nur vom mobilen Endgerät oder dem Ortungsnetzwerk vorgenommen werden, sondern auch von speziellen Referenzstationen: diese sind eine optionale Erweiterung des Ortungsnetzwerkes mit bekanntem Standort. Für das GPS-System werden weltweit mehrere solcher Stationen betrieben (z.B. in Colorado Springs oder auf den Ascension Islands), um Fehlfunktionen einzelner Satelliten rechtzeitig zu erkennen. Referenzstationen können aber auch eingesetzt werden, um externe Spoofing-Angriffe zu erkennen: hierbei errechnet die Station ihre Position und vergleicht sie mit der bekannten Position; gibt es Abweichungen über einen bestimmten Schwellwert hinaus, so werden die mobilen Endgeräte und/oder Backendsysteme gewarnt. Ein externer Angreifer könnte daher seine Signale zur Überlagerung des eigentlichen Ortungssystems so ausstrahlen, dass die Referenzstation hiervon nicht betroffen ist, sehr wohl aber das anvisierte mobile Endgerät. Es gibt deshalb den Ansatz, verstecke Referenzstationen zu verwenden [CaCS06]. Da solch ein Versteck mit der Zeit aufgedeckt werden kann oder je nach Situation Referenzstationen an unterschiedlichen Orten benötigt werden, können auch mobile Referenzstationen (z.B. in KFZ installiert) eingesetzt werden.

4 Tamperproof Hardware

In der Literatur werden Systeme für den Anwendungsfall beschrieben, dass ein Endgerät nur an bestimmten Orten verschlüsselte Inhalte wie Spielfilme wiedergeben darf [Mund05, GaWo98]. Für das Anwendungsgebiet von Set-Top-Boxen wird sogar gefordert, dass eine Entschlüsselung von ausgestrahlten Inhalten nicht in Gaststätten oder öffentlichen Plätzen möglich sein soll, sondern nur in Privatwohnungen. Da das Endgerät sich hier im Zugriffsbereich des potentiellen Angreifers befindet, ist dies nur unter Verwendung spezieller Hardwarebausteine möglich, die insbesondere auch gegen direkte physische Manipulation resistent sind („Tamperproof Hardware“). Diese Module müssen hierbei die Funktionalitäten für die (Eigen-)Ortung sowie die Entschlüsselung beinhalten.

Das von Mundt in [Mund05] beschriebene System sieht zusätzlich ein Uhrenmodul vor: er geht davon aus, dass die von einem Satellitennavigationssystem ausgestrahlten Systeme einen Zeitstempel beinhalten und digital signiert sind. So soll ein Empfänger Re-

routing-Angriffe erkennen können, da Rerouting zu einer Zeitverzögerung führt, die mit diesen Zeitstempeln erkannt werden können. Um aber die entsprechenden Zeitabweichungen erkennen zu können, ist eine hochpräzise Uhr nötig (wird ein Signal mit Lichtgeschwindigkeit weitergeleitet benötigt es für eine Strecke von z.B. 100 km weniger als 3,4 Millisekunden). Eine hinreichende zeitliche Ganggenauigkeit kann nur mit Atomuhren erreicht werden, die aber für mobile Endgeräte im Konsumerbereich aufgrund der Kosten und des Gewichts nicht in Frage kommen. Im System von Mundt muss deshalb die Uhr im Abstand von ca. drei Stunden neu mit einer externen Zeitquelle unter Verwendung eines speziellen kryptografischen Protokolls synchronisiert werden. Es wird also nicht ständig eine Kommunikationsverbindung benötigt.

Aber auch wenn die Ortung nicht auf dem mobilen Endgerät lokal benötigt wird, sondern auf einem Backendsystem für eine Zugriffsentscheidung durch einen sog. Referenz-Monitor, kann es sinnvoll sein, ein gegen Manipulation geschütztes Hardwaremodul auf dem Endgerät für die Ortung zu haben: in diesem wird nicht nur die Funktionalität zur Errechnung der Eigenortung untergebracht, sondern auch noch ein privater Schlüssel, um die Ortung digital zu signieren, bevor sie an das Backend übertragen wird. Das Backend kann mit dem zugehörigen öffentlichen Schlüssel dann die Authentizität der Ortung überprüfen.

5 Location-Keys

Bei Location-Keys muss das mobile Endgerät eine Information, die nur an bestimmten Orten empfangbar ist, an das stationäre Backend weiterleiten. Dieses Prinzip eignet sich insbesondere, wenn Eigenortung für eine verteilte mobile Anwendung eingesetzt wird, bei der auf dem Backend eine vertrauenswürdige Ortung für Zugriffsentscheidungen benötigt wird.

Wir unterscheiden zunächst, ob es sich um Location-Keys natürlichen oder nicht-natürlichen Ursprungs handelt. Bei den künstlichen Location-Keys kann weiter unterschieden werden, ob sie speziell für die Vermeidung von Spoofing ausgestrahlt wurden (dedizierte Location-Keys); nicht-dedizierte Location-Keys sind also Signale, die primär für einen anderen Zweck ausgestrahlt werden, etwa die eigentliche Ortung oder zur drahtlosen Kommunikation.

Ein Anti-Spoofing-Verfahren, das auf nicht-dedizierten Location-Keys basiert, ist der CyberLocator [DeMa96], bei dem es sich um eine Erweiterung für GPS handelt. Die mobilen Endgeräte müssen hierbei an das stationäre Backend nicht nur die errechnete Ortung weiterleiten, sondern auch noch die von den Satelliten empfangenen „Rohsignale“ (Radio Fingerprint). Diese sind auch unter Kenntnis der aktuellen Satellitenlaufbahnen (Ephemeride) nicht vorhersagbar, da sie durch komplexe atmosphärische Effekte (z.B. Änderung Wetter, Einfluss Ionosphäre) ständig beeinflusst werden. Am Backend werden die vom mobilen Endgerät gemeldeten Signale mit Messungen von vertrauenswürdigen Referenzstationen verglichen. Diese Referenzstationen müssen sich in einer Entfernung von 2.000-3.000 km Entfernung zu dem mobilen Endgeräten befinden. Es sind aber Rerouting-Angriffe denkbar, bei denen das mobile Endgerät von einem am

vorgeblichen Ort befindlichen Empfänger die relevanten Signale weitergeleitet bekommt. Um dies zu verhindern wird gefordert, dass das Endgerät die Location-Keys innerhalb von 5 ms an das Backend liefert (zum Vergleich: für UMTS-HSDPA beträgt die Latenzzeit etwa 150 ms, für drahtgebundenes DSL etwa 20 bis 60 ms). Leider bieten die Autoren des CyberLocators keine Herleitung der max. möglichen Entfernung zwischen Endgerät und Referenzstation, das System ist anscheinend auch nie implementiert worden.

Ein weiterer Ansatz, mit dem Endgeräte ihren Aufenthaltsort in von WLAN abgedeckten Gebieten nachweisen können, wird „Location Aware Access Control“ (LAAC) genannt und ist in [CBGo06] beschrieben. Hierbei werden von Funkbaken spezielle Signale mit begrenzter Reichweite ausgestrahlt, es handelt sich also um dedizierte Location-Keys. Diese Keys bestehen einfach aus langen zufällig erzeugten Bit-Strings, die periodisch erneuert werden. Das Endgerät verknüpft alle empfangen Schlüssel mittels der XOR-Funktion und wendet auf das Ergebnis eine Hash-Funktion an. Das Ergebnis dieser Berechnung wird an das Backend weitergeleitet. Da das Backend über einen gesicherten Kanal die Location-Keys der einzelnen Basis-Stationen erhält, kann es die gleiche Berechnung wie das Endgerät durchführen und somit die Location-Keys verifizieren. Zusätzlich kann über spezielle Sektor-Antennen der Abstrahlungswinkel dieser Signale eingeschränkt werden. Zwei Baken mit einem Abstrahlungswinkel von jeweils 90 Grad können so angeordnet werden, dass das von beiden überdeckte Gebiet die Form eines Rechtecks hat. Es können also gezielt Flächen wie Ladenlokale oder Firmengelände abgedeckt werden. Die Möglichkeit eines Rerouting-Angriffs wird von den Autoren von LAAC als zu aufwändig erachtet, als dass sie dafür Gegenmaßnahmen vorsehen würden. Lediglich ein Replay-Angriff wird durch das regelmäßige wechseln des Location-Keys verhindert (ein Location-Key sollte eine Lebensdauer in der Größenordnung von höchstens einigen wenigen Sekunden haben). Dies ist aber vor dem Hintergrund zu sehen, dass LAAC speziell dafür entwickelt wurde, eine Zugriffskontrolle für drahtlosen Internetzugriff über WLAN-Hotspots (die gleichzeitig auch die Baken sind) auf Ladenlokale zu beschränken, so dass ein Angreifer, der über eine schnelle drahtlose Kommunikationsverbindung verfügt, die für einen Rerouting-Angriff notwendig wäre, kaum einen Nutzen davon hat, wenn er das LAAC-System überlistet.

Ein ähnlicher Ansatz wird in [Mich02] mit „Pervasive Access Control“ (PAC) beschrieben: hierbei verwendet das mobile Endgerät den von einer Bake empfangenen Location-Key als Schlüssel für eine Hashfunktion, mit der eine Signatur für einen Dienstrequest an einen zentralen Server erzeugt wird. Der Server liefert dann ein sog. „Ticket“ an das Endgerät zurück, das damit gegenüber einem lokalen Gerät (z.B. Drucker) seine Zugriffsberechtigung nachweisen kann.

In [Mala07] ist ein weiterer Ansatz für WLANs beschrieben, mit dem Endgeräte ihren Aufenthaltsort gegenüber einem Backend nachweisen, wenn davon ausgegangen wird, dass nicht autorisierte Nutzer keinen Zutritt zu dem Gelände haben, das mit dem WLAN versorgt werden soll. Hierzu übermittelt das Endgerät seine Position (die z.B. mit GPS oder einem infrarotbasierten Ortungsverfahren berechnet wird) sowie die Signalstärken, mit denen es mehrere Accesspoints (AP) des Netzwerkes empfangen kann, an das Backend. Die gemessenen Signalstärken stellen einen künstlichen und nicht dedizierten

Location-Key dar: dem Backend sind an einzelnen Referenzpositionen innerhalb des Geländes die tatsächlichen Messwerte bekannt, der Angreifer kann diese aber nur abschätzen. Es gibt zwar spezielle Modelle, mit denen die Empfangsstärke eines APs an einem bestimmten Ort vorhergesagt werden kann, hierfür ist es aber notwendig, die Bebauung (Wände) und Möblierung sowie die spezifischen Dämpfungsfaktoren der verwendeten Materialien zu kennen.

Wird ein digitales Signal von einem geostationären Satelliten ausgestrahlt, so unterscheiden sich die in einem bestimmten Zeitintervall an verschiedenen Punkten der Erdoberfläche empfangenen Nachrichten aufgrund der Phasenverschiebung, die aus den unterschiedlichen Entfernungen zum Satelliten resultieren. In [GaWo98] wird ein Verfahren beschrieben, in dem dieser Effekt ausgenutzt wird, um einen Location-Key zu erhalten. Hierzu ist es aber notwendig, dass das Endgerät mit hoher zeitlicher Präzision die Aufzeichnung des Satellitensignals startet und beendet; es werden deshalb von den Autoren verschiedene Wege vorgeschlagen, wie dieser „Aufzeichnungsbefehl“ an die Endgeräte übermittelt werden kann, z.B. über ein Broadcastsignal, das von einem terrestrischen Netzwerk ausgestrahlt wird. Da es sich bei dem aufgezeichneten Signal um ein digitales TV-Programm handelt, liegt hier wieder ein nicht-dedizierter Location-Key vor.

In der Literatur wird noch kein Anti-Spoofing-Verfahren beschrieben, das mit natürlichen Location-Keys arbeitet, jedoch wäre hier prinzipiell die kosmische Hintergrundstrahlung als Key geeignet, da diese — bedingt u.a. durch atmosphärische Effekte — an jedem Ort der Erde zu einem bestimmten Zeitpunkt ein spezifisches Empfangsmuster ergibt.

Neben der Unterscheidung der Herkunft des Location-Keys kann noch weiter unterschieden werden, ob ein Location-Key immer für einen Ort steht (singulärer Location-Key, wie beim CyberLocator), oder ob ein Key durch Überlagerung mit anderen Keys für mehrere Orte stehen kann (multiple Location-Keys, wie bei LAAC).

Der prinzipielle Nachteil von Location-Key-Ansätzen ist, dass das Endgerät hierbei über einen Kommunikationskanal mit geringer Latenzzeit verfügen muss.

6 Request-Response-Protokolle

Request-Response-Protokolle basieren darauf, dass das mobile Endgerät („Prover“) von dem vertrauenswürdigen und stationären „Verifier“ eine Nachricht (Request) mit nicht vorhersehbarem Inhalt erhält, die er sofort beantworten muss (Response). Im einfachsten Fall handelt es sich bei dieser Nachricht um einen zufällig erzeugten Bitstring hinreichender Länge („Nonce“), der einfach reflektiert werden muss. Die Grundidee ist, dass der Prover hierzu nur in der Lage ist, wenn er sich tatsächlich an dem von ihm vorgegebenen Ort aufhält. Ist er nämlich weiter entfernt, so können die Funksignale diese Strecke nicht überbrücken oder die Signallaufzeit ist zu lange. Die Grundannahme bei Auswertung der Signallaufzeiten ist es, dass selbst bei einem Rerouting-Angriff die Nachricht nicht schneller als mit Lichtgeschwindigkeit übertragen werden kann. In der Klassi-

fikation der Anti-Spoofing-Verfahren wird deshalb für „Request-Response“ zwischen „Proximität“ und „Laufzeit“ unterschieden.

Ein schönes Beispiel für solch ein auf Laufzeitmessung beruhendes System wird von Sastry et al. beschrieben [SaSW03]: Der Prover sendet zunächst per Funk eine Nachricht mit seinem angeblichen Aufenthaltsort an den Verifier. Wenn der Verifier sich für diesen Aufenthaltsort für zuständig hält, schickt er ebenfalls per Funk den Request mit dem Nonce und startet die Zeitmessung. Sobald der Prover diesen Request erhält, sendet er ihn zurück an den Verifier, allerdings über Ultraschall. Der Verifier stoppt die Zeitmessung, sobald er die Response erhalten hat und überprüft anschließend, ob die Laufzeit unter Berücksichtigung der Signalgeschwindigkeiten von Funk und Ultraschall hinreichend klein ist.

Die Besonderheit dieses Verfahren ist, dass die drahtlose Datenkommunikation über zwei unterschiedliche Medien — nämlich Funk und Ultraschall — geschieht. Dies ist dadurch motiviert, dass bestimmte Messungenauigkeiten der Laufzeit berücksichtigt werden sollen, insbesondere die Verarbeitungszeit, die der Prover u.U. benötigt, um die Antwort zu erzeugen. Die sich aus der Lichtgeschwindigkeit ergebenden Entfernungsungenauigkeiten sind aber so groß, dass diese das Verfahren unbrauchbar machen würden. Es wird deshalb auf Ultraschallwellen zurückgegriffen, die sich mit einer um sechs Größenordnungen geringeren Geschwindigkeit ausbreiten (331 m/sec gegenüber etwa $3x10^8$ m/sec). Eine zeitliche Messungenauigkeit von 0,1 Sekunden (z.B. Reaktionszeit auf Prover) resultiert damit nur in einer räumlichen Ungenauigkeit von ca. 33 m statt ca. 30.0000 km, womit das Verfahren sogar für die meisten Indoor-Anwendungen noch brauchbar wäre. Die langsame Ultraschallkommunikation ist aber prinzipiell mit Rerouting angreiferbar: die Autoren wählen deshalb bewusst Ultraschall für den „Rückweg“, da hier ihrer Ansicht nach der technische Aufwand für Rerouting zu groß wäre.

In [WaFe03] findet sich die Beschreibung eines weiteren Verfahrens Request-Response-Verfahrens, es werden jedoch sowohl der Request als auch die Response über Funk übertragen, somit handelt es sich also um ein symmetrisches Verfahren.

Die Kommunikation eines Mobilfunktelefons mit einer Basisstation kann auch als Request-Response-Protokoll aufgefasst werden. Je nach Mobilfunkstandard bietet hierbei auch die Verschlüsselung der Daten auf der Luftschnittstelle gegen externe Angreifer eine gewisse Sicherheit, wobei aber etwa der für GSM verwendete Algorithmus A5/1 gebrochen wurde; der Verschlüsselungsalgorithmus A5/3 für UMTS gilt bisher als sicher. Mobilfunkzellen können aber bis zu 35 km Durchmesser haben, was für viele Anwendungsszenarien zu ungenau ist. Es kann aber zusätzlich die Laufzeit der Signale zwischen Endgerät und Basisstation berücksichtigt werden; diese muss lt. GSM-Protokoll ohnehin ständig bekannt sein, da ein Endgerät mit zunehmender Entfernung von der Basisstation die Übertragung seiner Datenpakete („Bursts“) vorziehen muss, um dem ihm gemäß dem TDMA-Verfahren (Zeitmultiplexing) zugeteilten Zeitschlitz der Basisstation zu treffen. Ohne diesen „Time Advance“ (TA) genannten Mechanismus könnte es zu Kollisionen von Bursts zweier Endgerät kommen, wenn das Endgerät mit dem direkt folgenden Zeitschlitz wesentlich näher an der Basisstation ist, da der Burst des weiter entfernten Endgeräts aufgrund der großen Laufzeit verspätet eintrifft und

nicht beendet ist, wenn der Burst des zweiten Gerätes die Basisstation erreicht. Über die TA-Messungen kann die Distanz zwischen Endgerät und Basisstation mit einer Genauigkeit von 550 m bestimmt werden. Aus dem Maximalwert der zugehörigen TA-Variablen im GSM-Protokoll ergibt sich auch die Höchstentfernung von ca. 35 km zwischen Basisstation und Endgerät. In [WuLC03] wird dieses System daraufhin untersucht, inwieweit es als Mechanismus gegen Location-Spoofing verwendet werden kann. Sie kommen zu dem Ergebnis, dass kein Spoofing-Schutz vorliegt, wenn die Entfernung zwischen Endgerät und Basisstation geringer als 4.600 m ist. Hierbei wird davon ausgegangen, dass eine Manipulation von clientseitiger GSM-Hardware für die meisten Fälle nicht realistisch ist.

Eine Variation der Proximität-Erkennung (ohne Laufzeitberechnung) findet sich in [VoNe06]: im zu überwachenden Gebiet sind hierbei mehrere Verifier installiert. Gibt ein Endgerät vor, sich in diesem Gebiet zu befinden, muss ein Signal auch von den entsprechenden Verifiern zu empfangen sein. Die Autoren leiten dabei Aussagen her, wie viele Verifier für Gebiete bestimmte Größe und Form benötigt werden. Zusätzlich gibt es aber auch „Rejection Verifier" außerhalb des Schutzgebietes: empfängt ein solcher Rejector das Signal des Provers, so wird der Zugriff verweigert.

7 Funktechnische Maßnahmen

Es gibt spezielle funktechnische Maßnahmen, die das Überlagern oder Auslöschen der Ortungssignale durch Angreifer erschweren. Die entsprechenden Arbeiten sind dem Bereich der Nachrichtentechnik zuzuschreiben und sollen deshalb nur kurz angerissen werden:

- Frequenzspreizung (Spread-Spectrum-Verfahren): Hierbei wird ein schmalbandiges Signal in ein Signal mit einer größeren Bandbreite umgewandelt. Durch die erhöhte Bandbreite ist es dann für einen Angreifer wesentlich aufwändiger, das Signal zu stören [PiSM82]. Konkrete Frequenzspreizungsverfahren sind etwa *Frequence Hopping Spread Spectrum* (FHSS) oder *Direct Sequence Spread Sprectrum* (DSSS). Frequenzspreizung kann aber auch eingesetzt werden, um das Signal robuster gegenüber natürlichen Störungen (z.B. Inferenzen) zu machen.

- Manchester-Coding: Für einen Angreifer ist es schwieriger, ein gesendetes Bit (1) „auszulöschen" als ein nicht gesetztes Bit (0) zu setzen. Beim sog. Manchester-Coding wird deshalb jedes Bit der Originalnachricht auf zwei Bits abgebildet ($0 \rightarrow 01$, $1 \rightarrow 10$), so dass ein Angreifer, der keine gesendeten Bits auslöschen kann, nicht Nachrichten derart manipulieren kann, so dass dies der Empfänger nicht entdeckt. [CaRC07]

- Erkannte Störsender können unter Verwendung einer speziellen Antenne mit Nullsteuerung (sog. „Phased Array Antenna") unterdrückt werden. [DoHä04, 172]

- Ähnlich der Frequenzspreizung ist der Ansatz, für die Signale verschiedener Sender in Ortungsnetzwerken unterschiedliche Frequenzen zu verwenden. Beim russischen GLONASS-System etwa sendet jeder Satellit auf einer eigenen Frequenz [DoHä04,

172]. Beim US-amerikanischen GPS hingegen senden alle Satelliten auf den gleichen Frequenzen, da die Navigationsnachrichten aber mit dem CDMA-Verfahren codiert sind ist es für den Empfänger trotzdem möglich, einzelne Satelliten „herauszuhören“.

8 Absicherung von GPS und Galileo

GPS ist das wohl bekannteste Ortungssystem, das inzwischen auch von vielen Privatnutzern tagtäglich für Navigation eingesetzt wird. Alle nominal 24 Satelliten des Systems strahlen auf denselben Frequenzen L1 und L2 Navigationsnachrichten aus, die u.a. die Nummer des jeweiligen Satellits oder die Bahnlaufdaten (Ephemeride) enthalten. Um diese Nachrichten mit CDMA zu modulieren, stehen zwei Codes zur Verfügung: der Coarse Acquistion Code (C/A) für den auf zivile Nutzung ausgelegten Standard Positioning Service (SPS) und der Precise Code (P-Code), der militärischen Nutzern für den sog. Precise Positioning Service (PPS) vorbehalten sein sollte und durch die Verwendung des geheimen Y-Schlüssels zum P(Y)-Code wird [DoHä04, 173f; Küpp05, 165ff]. Während der C/A-Code nur auf der L1-Frequenz ausgestrahlt wird, wird der P(Y)-Code sowohl auf der L1- als auch der L2-Frequenz ausgestrahlt. Der P(Y)-Code kann als symmetrische Chiffre aufgefasst werden, da zur Ver- als auch Entschlüsselung der gleiche Schlüssel Y verwendet wird. Weil er eine um den Faktor 10 höhere Frequenz als der C/A-Code hat, lässt sich mit ihm auch eine deutlich bessere Ortungsgenauigkeit erzielen. Dieser Schlüssel muss auf allen autorisierten GPS-Empfängern vorhanden sein; wird nur eines dieser Geräte kompromittiert, so könnte der Angreifer eigene mit dem P(Y)-Code verschlüsselte Navigationsnachrichten ausstrahlen, um eine Spoofing-Attacke durchzuführen. Da dieselbe Navigationsnachricht mit dem öffentlichen C/A-Code als auch dem P(Y)-Code verschlüsselt wird, kann auch ein Known-Plaintext-Angriff durchgeführt werden. Der Y-Schlüssel wird deshalb alle 24h Stunden ausgetauscht (Rekeying). Jenseits von Spoofing-Angriffen sind Angriffe auf den P(Y)-Code aber mittlerweile uninteressant, weil es mit sog. Codeless Receivern/Kinematic Receivern auch ohne dessen Kenntnis möglich ist, die höhere Ortungsgenauigkeit des PPS zu erreichen [DoHä04, 229f]. Weiter sind für GPS mit „RAIM“ (Receiver Autonomous Integrity Monitoring) verschiedene Formen der Plausibilitätskontrolle der empfangenen Signale auf dem Endgerät verfügbar, für die aber redundante Messungen (z.B. Sichtbarkeit von mehr als den vier systembedingt notwendigen Satelliten) verfügbar sein müssen [Lang99].

Das von der EU geplante Galileo-System soll vergleichbar den beiden GPS-Diensten verschiedene — teilweise kostenlose — Dienste anbieten, die sich in Genauigkeit oder Integritätsgarantien unterscheiden. Um Spoofing zu vermeiden ist geplant, die von einigen Diensten ausgestrahlten Navigationsnachrichten mit einem Public-Key-Verfahren digital zu signieren: hierbei wird die Nachricht vom Satelliten unter Verwendung des geheimen Schlüssels signiert, der Empfänger kann dann mit dem zugehörigen öffentlichem Schlüssel verifizieren, dass das Signal tatsächlich von einem Galileo-Satelliten ausgestrahlt wurde. Ein Angreifer müsste an den nur in der Kontrollstation oder auf den Satelliten gespeicherten geheimen Schlüssel gelangen, um selbst erzeugte Navigationsnachrichten digital zu signieren. Um ein Rerouting anhand des ebenfalls signierten Zeitstempels zu erkennen, müsste der Empfänger aber über eine hochpräzise Uhr verfügen.

9 Zusammenfassung und Ausblick

Anhand eines Klassifikationsschemas wurden verschiedene Prinzipien vorgestellt, mit denen bewusste Manipulationen von Ortungsverfahren verhindert werden können. Nicht behandelt wurden Ansätze, die speziell für infrastrukturlose Netzwerke (Sensornetzwerke, MANETs) entwickelt wurden, z.B. [CaCS06]. Neben verschiedenen Formen der Plausibilitätskontrolle, Location Keys und Request- und Response-Protokollen wurden auch manipulationssichere Hardware und spezielle funktechnische Maßnahmen betrachtet.

Plausibilitätskontrollen können sowohl bei Eigen- als auch Fremdortung durchgeführt werden, wobei eine Auswertung auf Signalebenen vor allem für ersteres geeignet ist. Manipulationssichere Hardware ist immer dann unabdingbar, wenn die Zugriffsentscheidung selbst lokal auf dem mobilen Endgerät durchgeführt werden soll, wie dies etwa bei DRM-Szenarien der Fall ist. Location-Key-Verfahren können durch Rerouting angegriffen werden; wenn durch die Ortung aber nur der Zugriff auf Internetzugriff (z.B. über WLAN-Hotspot) gesteuert werden soll ist dieses Verfahren ausreichend. Bei Request-Response-Protokollen mit Laufzeitmessungen werden hochpräzise Uhren benötigen, bei proximitätsbasierenden Ansätzen sind komplexe und teilweise auch dynamische Abschattungen zu berücksichtigen (z.B. durch Gebäude, Passanten oder Fahrzeuge). Auch eine Kombination mehrerer Ortungsverfahren ist denkbar, da es für den Angreifer dann aufwändiger wird, mehrere Verfahren gleichzeitig so zu manipulieren, dass keine Inkonsistenzen auftreten.

Eine generelle Empfehlung für ein Anti-Spoofing-Verfahren kann nicht gegeben werden, es müssen immer die für den jeweiligen Anwendungsfall gegebenen Anforderungen und Möglichkeiten berücksichtigt werden.

Literatur

[CaRC07] Capkun, S.; Rasmussen, K.B.; Cagalj, M.: SecNav: Secure Broadcast Localization and Time Synchronization in Wireless Networks. International Conference on Mobile Computing and Networking (MobiCom), 2007, 310-313.

[CaCS06] Capkun, S.; Cagalj, M.; Srivastava, M.: Secure Localization with Hidden and Mobile Base Stations. IEEE International Conference on Computer Communications (INFOCOM), 2006, 1-10.

[CBGo06] Cho, Y.; Bao, L.; Goodrich, M.: LAAC: A Location-Aware Access Control Protocol. Third Annual International Conference on Mobile and Ubiquitous Systems: Networking & Services, 2006, 1-7.

[DaBP07] Damiani, M.L.; Bertino, E.; Perlasca, P.: Data security in location-aware applications. An approach based on RBAC. International Journal on Information and Computer Security, 1(1/2), 2007, 5-38.

[DeMa96] Denning, D.; MacDoran, P.: Location-Based Authentication: Grounding Cyberspace for Better Security. Computer Fraud & Security, Elsevier, February 1996, 12-16.

[DoHä04] Dodel, H.; Häupler, D.: Satellitennavigation. Hüthig-Verlag, Bonn, 2004.

[GaWo98] Gabber, E.; Wool, A.: How to Prove Where You Are: Tracking the Location of Customer Equipment. Proceedings of the 5th ACM Conference on Computer and Communications Security, 1998, 142-147.

[Küpp05] Küpper, A.: Location-based Services. Fundamentals and Operations. Wiley & Sons, Chichester, U.K., 2005.

[Lang99] Langley, R. B.: The Integrity of GPS. GPS World, March, 1999, 60-63.

[Mala07] Malaney, R.A.: Securing Wi-Fi Networks with Position Verification (Extended Version). International Journal of Security Networks, 2(1-2), 2007, 27-36.

[Mich02] Michalakis, N.: PAC: Location Aware Access Control for Pervasive Computing Environments. Proceedings of the Second Student Oxygen Workshop, Gloucester, MA, USA, 2002.

[Mund05] Mundt, T.: Location Dependent Digital Rights Management. Proceedings of the 10th IEEE Symposium on Computers and Communications (ISCC 2005), 2005.

[PiSM82] Pickholtz, R. L.; Schilling, D. L.; Milstein, L. B.: Theory of Spread-Spectrum Communications — A Tutorial. IEEE Transactions on Communications, 80(5), 1982, 855-884.

[SaSW03] Sastry, N.; Shankar, U.; Wagner, D.: Secure Verification of Location Claims. Proceedings of the Conference on Wireless Security (WiSe), 2003, 1-10.

[TuPo04] Turowski, K.; Pousttchi, K.: Mobile Commerce — Grundlagen und Technik. Springer-Verlag, Berlin et al., 2004.

[VoNe06] Vora, A.; Nesterenko, M.: Secure Location Verification Using Radio Broadcast. IEEE Transactions on Dependable and Secure Computing, 3(4), 2006, 377-385.

[WaFe03] Waters, B. R.; Felten, E. W.: Secure, Private Proofs of Location. Technical Report TR-665-03, Dep. of Computer Science, Princeton University, 2003.

[WaJo03] Warner, S. W.; Johnston, R.G.: GPS Spoofing Countermeasures. Technical Report LAUR-03-6163, Los Alamos National Laboratory, U.S.A., 2003.

[WuLC03] Wullems, C.; Looi, M.; Clark, A.: Enhancing the Security of Internet Applications using Location: A New Model for Tamper-resistant GSM Location. Proceedings of the 8th IEEE International Symposium on Computers and Communications (ISCC' 03), 2003, 1251-1258.