Tracking von Personen

Michael Lux

HTWK Leipzig

michael.lux@stud.htwk-leipzig.de

Zusammenfassung

Im Folgenden werden verschiedene Methoden genauer beschrieben, mit denen sich der Standort einer Person ermitteln lässt mit dem Ziel, Möglichkeiten der Verhüllung der Position zu zeigen. Die Ortung eines Objekts, bzw. einer Person kann über GPS, RFID-Systemen oder über das Mobilfunknetzwerk geschehen. Die rudimentären Lösungsansätze, wie etwa die Anwendung von Jamming und Spoofing oder der Verzicht auf diese Technologien sind unpraktikabel. Die Verwendung dieser Systeme im Alltag ist unumgänglich. Die Lösungsansätze dienen in erster Linie zum Schutz der Privatsphäre eines Einzelnen. Diese ist in heutiger Zeit gefährdet durch die Beschaffenheit der Systeme und die Gesetzeslage, die unzureichenden Schutz der Privatsphäre bietet.

I. Einführung

Der Standort einer Person kann auf mehrere Arten ausfindig gemacht werden. Durch Sammlung dieser Daten in bestimmten zeitlichen Abständen kann ein Bewegungsprofil der Person erstellt werden. Dieses Verfahren wird als Tracking bezeichnet. Diese Daten werden meist in Datenbanken auf Servern gespeichert. Diese bieten oftmals Sicherheitslücken für Angreifer, wodurch es zum Missbrauch der Daten kommen kann.

Im Folgenden werden drei Systeme betrachtet, die das Orten ermöglichen: das Global-Positioning-System (GPS), Radio-Frequency-Identification (RFID) und das Global-System-for-Mobile-Communications (GSMC).

II. GPS

Das Global-Navigation-Satellite-System (GNSS), umgangssprachlich GPS genannt, besteht aus mehreren Satelliten und einem Empfänger. Die georteten Objekte müssen über einen GPS-Empfänger verfügen, um die von mehreren Satelliten ununterbrochen ausgesendeten Radiosignale zu empfangen. In diesen Signalen befindet sich die Information über den Standort des Satelliten und den Zeitpunkt des Sendens des Signals.[4]

Mithilfe dieser Information von mehreren Satelliten kann die Position auf wenige Meter genau bestimmt werden. Damit Position, Höhe und genaue Zeit durch den Empfänger berechnet werden können, muss dieser stets Kontakt zu vier Satelliten haben. Um dies zu gewährleisten müssen deshalb mindestens 24 Satelliten gleichmäßig verteilt im Einsatz sein. Die Bestimmung der Geschwindigkeit des Objekts ist möglich, indem die Positionsänderung innerhalb einer bestimmten Zeit ermittelt wird.

Um nicht über GPS geortet werden zu können, empfiehlt es sich, die GPS-Funktion bei mitgeführten Geräten zu deaktivieren, beziehungsweise die GPS-Empfänger auszubauen. Da letzteres oftmals nicht realisierbar ist, können die Methoden Jamming und Spoofing angewandt werden.

Bei der ersten Methode wird ein Störsignal erzeugt auf der gleichen Frequenz auf der die GPS-Signale gesendet werden. Die Empfänger können die ursprünglichen Signale nicht mehr aufnehmen, da sie von den Störsignalen überlagert werden. Bei Letzterem wird ein gefälschtes GPS-Signal gesendet. Der Empfänger bekommt die Information an der Position zu sein, die der Anwender des Spoofings durch die Fälschung vorgibt.

Da die Praxis von Störsendern in den meisten Ländern illegal ist wird hiervon abgeraten.

Personen werden in Gefahr gebracht, die im Wirkungsradius stehen, sollten sie auf die GPS-Signale angewiesen sein. Dies gilt insbesondere für Dienstleister des Flug- und Schiffsverkehrs, da die Navigation von Flugzeugen und Schiffen mithilfe von GPS geschieht.[1]

Ein Problem von GPS ist, dass oftmals innerhalb von Gebäuden oder Tunneln die Empfänger keine Signale erhalten. Wände und andere Hindernisse unterbrechen den Kontakt zwischen Satelliten und dem Empfänger. Eine Abhilfe hierfür verschafft die Ortung durch RFID.

III. RFID

Radio-Frequency-Identification-Systeme, kurz RFID-Systeme, bestehen immer aus zwei Komponenten, einem Transponder auf dem die Daten gespeichert sind und dem Lesegerät. Das Lesegerät empfängt diese Daten und leitet sie zur Datenverarbeitung weiter. (Abbildung 1). Transponder enthalten einen Prozessor, welcher die Übertragung realisiert, eine Speichereinheit zur Speicherung der Daten und eine Antenne, welche die Signale des Lesegeräts empfängt. Die meisten Transponder arbeiten passiv, sprich sie benötigen keine eigene Energieversorgung. Sie erhalten die Energie, die von dem elektromagnetischen oder magnetischen Feld des Lesegeräts erzeugt wird.[1]

Die Position eines RFID-Chips ist dadurch ermittelbar, indem erkannt wird, ob ein Transponder in diesem Feld auf die Signale des Lesegeräts antwortet. Je nachdem wie groß der Bereich ist in dem der Sender Signale ausbreitet, kann ein mit einem RFID-Chip ausgestattetes Objekt auf wenige Zentimeter genau geortet werden.

[1] https://www.heise.de/newsticker/meldung/GPS-unter-Beschuss-Jamming-und-Spoofing-nehmen-zu-4038137.html

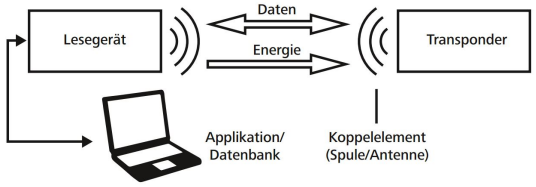

Abbildung 1: Funktionsweise eines RFID-Systems https://www.hellermanntyton.de/kompetenzen/rfid-tracking-industrie

Es gibt Realisierungen, bei denen die Kommunikation beider Komponenten über mehrere Meter hinweg stattfindet. Die exakte Positionsermittlung ist für den üblichen Einsatz nicht von Bedeutung, da ihr Zweck in der Inventur bzw. damit begründet ist, das Objekt selbst zu identifizieren, an dem der Transponder angebracht ist, über die darauf gespeicherten Daten.

Die RFID-Technologie wird in dem aktuellen Personalausweisen verwendet. Der Standort von Personen kann über diesen Weg ermittelt werden, falls das RFID-Modul auf dem Ausweis in den Sendebereich eines Lesegeräts gelangt und die Daten erfolgreich ausgelesen werden.

Es besteht eine Ausweispflicht ab einem Alter von 16 Jahren, aber keine Mitführpflicht. Zur Vermeidung über den integrierten Transponder geortet zu werden reicht es demnach, den Personalausweis nicht mit sich zu führen. Dies ist jedoch nicht praktikabel, da dieser im Alltag gebraucht werden kann.

Um den Datentransfer zu verhindern gibt es spezielle RFID-Blocker. Diese wirken in der Nähe des Transponders platziert wie ein Störsender. Es werden aktiv Signale ausgesendet die das Auslesen der Daten des Chips stören.

Eine andere Methode ist es, den Chip physikalisch zu zerstören oder einen „Kill“-Befehl zum Transponder zu schicken, welcher ihn unbrauchbar macht.[3]

Das Auslesen kann auch durch eine Art faradayschen Käfig verhindert werden, in den der Transponder platziert wird. Die elektrischen Leiter des Käfigs schirmen diesen von den außen anliegenden Feldern, etwa die eines Lesegeräts ab. Diese Praxis kann auch als Sicherheitsvorkehrung für das nächste System verwendet werden.

IV. GSM

Global-System-for-Mobile-Communications (GSM) ist ein Mobilfunkstandard zur Ermöglichung der Telekommunikation zwischen Endnutzern. Dazu wird der Protokollstack Signalisierungssystem 7 verwendet. Dieses er-

möglicht die verschiedenen Funktionen, die für die Telefonie und für Textnachrichten benötigt werden. Zum einen regelt es den Verbindungsaufbau, die Verbindungstrennung, die Funktion einen Anruf zu halten und weiterzuleiten.[5]

Ein Protokoll innerhalb des Signalisierungssystems, der Mobile-Application-Part, kurz MAP, regelt unter anderem das Verschicken von Textnachrichten (SMS). Bei diesem Prozess wird die International-Mobile-Subscriber-Identity (IMSI) der Zielperson und die Vermittlungsstelle abgefragt. Die IMSI ist jeden Netzteilnehmer eindeutig zuordenbar. Die Position der Person lässt sich auf Stadtebene eingrenzen.

Damit kann innerhalb der Location Area mit der IMSI herausgefunden werden, mit welcher Funkzelle die Zielperson verbunden ist. Die Location-Area beinhaltet alle Funkzellen in der Umgebung. Diese MAP-Abfrage können Provider und private Unternehmen, die über die Berechtigung verfügen weltweit durchführen, ohne eine SMS selbst zu verschicken.

Einige dieser Unternehmen bieten als Dienstleistung die Ortung von Personen gegen Bezahlung an. [2]

Ermittlungsbehörden können durch sogenannte Stille-SMS orten, welche Personen in einer Funkzelle eingewählt sind. Bei dieser Art von SMS werden die gleichen Anfragen gesendet, ohne dass der Empfänger der SMS eine Textnachricht erhält. Der Empfänger erfährt nicht, dass er geortet wird. Die Daten über diese Person könnten missbraucht werden, wenn sie entwendet werden. Dies ist in der Vergangenheit schon öfters vorgekommen bei Daten, die in unsicheren Datenbanken aufbewahrt wurden. Die einzige Möglichkeit nicht geortet zu werden besteht darin, sein Mobiltelefon auszuschalten, beziehungsweise den Akku oder die Simkarte herauszunehmen, damit sich das Mobiltelefon nicht mit einer Mobilfunkzelle verbindet.

Durch das Stören der im Mobilfunk verwendeten Frequenzen können Personen im Umkreis keinen Kontakt mehr zum Mobilfunknetz aufbauen. Anrufe und SMS über Mobilfunk und Notrufe sind nicht möglich.

Langfristig gesehen könnte Kritik an der Erstellung massenhafter Bewegungsprofile seitens der Behörden zu Änderungen an der Gesetzeslage führen. Beispielsweise könnte ein richterlicher Beschluss benötigt werden um diese zu erstellen. Provider könnten die Funktion einer stillen SMS abschalten. Durch eine verringerte Sammlung dieser Daten würde das Missbrauchspotential verringert werden.

V. Fazit

Es gibt mehrere Arten eine Person zu orten, falls diese die vorher beschriebenen Technologien an sich trägt, deren eigentliche Position ermittelt wird. Selbst die Telefonnummer oder der Personalausweis reichen hierfür schon aus.

Die Lösungsvorschläge sind rudimentär und zum Teil auch verboten, wie es bei dem Erzeugen von Störsendern der Fall ist. Sie bieten keine Alternative zu Gesetzesänderung zum Schutz der Privatsphäre von Personen oder zu Änderung der Systeme, die verhindern, dass entsprechende Daten ohne das Einverständnis, beziehungsweise ohne Kenntnisnahme der Person weitergegeben werden.

Literatur

[1] S. Bioly & M. Klumpp. Radio Frequency Identification (RFID) und Dokumentenlogistik. *ILD*, 1(5), 2009.

[2] P. Gewald. *Sicherheitsaspekte von Mobiltelefonen.* Oldenburg: Springer, 1. Aufl., 2016.

[3] A. Juels, R. L. Rivest & M. Szydlo. The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy. *CCS*, 1(1), 2003.

[4] W. Mansfeld. *Satellitenortung und Navigation: Grundlagen und Anwendung globaler Satellitennavigationssysteme.* Wiesbaden: Springer, 2. Aufl., 2004.

[5] M. Sauter. *Grundkurs Mobile Kommunikationssysteme.* Koeln: Springer, 6. Aufl., 2015.