Datenspuren drahtloser Kommunikationstechnologien – Strategien zum Schutz der Privatsphäre

Marc Haase, Matthias Handy, Dirk Timmermann

Einleitung

Die Einführung drahtloser Kommunikationstechnologien in Bereiche des täglichen Lebens führt zunehmend zu einer Gefährdung der Privatsphäre eines jeden Bürgers und damit auch seines Rechts auf informationelle Selbstbestimmung. Dieses Recht verlangt den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten.

Bislang konnte jeder Bürger die Preisgabe seiner persönlichen Daten gut kontrollieren, da diese meist in nicht elektronischer Form von ihm aufbewahrt und weitergegeben wurden. Mit der jedoch zunehmenden Speicherung persönlicher Daten auf mobilen Geräten, wie. z.B. Adressen auf Mobiltelefonen, Terminen und Dokumenten auf persönlichen digitalen Assistenten (PDAs) und der Integration von drahtlosen Kommunikationstechnologien auf mobilen Geräten sind diese bei unzureichendem Sicherheitsmanagement auf mobilen Geräten von Dritten unbemerkt abrufbar. Damit droht bei der spontanen Kommunikation mit Geräten in der näheren Umgebung im Sinne des „Ubiquitous Computing“ in zunehmendem Maße ein Kontrollverlust über gespeicherte persönliche Daten.

Noch viel kritischer in Bezug auf die Privatsphäre von Nutzern mobiler Geräte ist die Möglichkeit zu bewerten, mobile Geräte und damit ihre Nutzer anhand von spezifischen Merkmalen drahtloser Kommunikationstechnologien, wie z.B. Geräteadressen zu erkennen und zu verfolgen. Bislang wurde der Sicherheitsaspekt bei drahtlosen Kommunikationstechnologien nur in der Ausprägung einer abhörsicheren Kommunikation zwischen mobilen Geräten berücksichtig. Dieser gewährleistet zwar eine vertrauliche Kommunikation zwischen Kommunikationspartnern, ist jedoch für den Schutz der Privatsphäre eines Bürgers nicht ausreichend.

Dieser Artikel beschäftigt sich mit der Analyse von Datenspuren bei Bluetooth und WLAN, diskutiert Strategien zur deren Vermeidung und leitet Anforderungen an zukünftige drahtlose Kommunikationstechnologien bezüglich des Schutzes der Privatsphäre ab.

Analyse von Datenspuren

Datenspuren sind spezifische, nicht veränderliche Merkmale einer drahtlosen Kommunikationstechnologie, die bei ihrem Einsatz an die Umgebung abgegeben werden. Beispiele hierfür sind eindeutige Geräte- oder MAC-Adressen. Damit besteht für einen Nutzer die Gefahr, dass ein Beobachter vom Nutzer abgegebene Datenspuren zeitlich und räumlich verkettet und damit Bewegungsprofile von Nutzern erstellt.

Das Auftreten von Datenspuren ist technologiespezifisch bedingt. Eindeutige Geräte- und MAC-Adressen sind bei vielen Kommunikationstechnologien Voraussetzung für eine kollisionsfreie Kommunikationsabwicklung. Periodisch ausgestrahlte Statusinformationen (Beacons) gewährleisten darüber hinaus den Aufbau neuer Kommunikationsverbindungen, die Steuerung der Verbindungsqualität und das Kommunikationsmanagement. Das bedeutet, dass bei der drahtlosen Kommunikation eine Vielfalt an Datenspuren an die Umgebung abgegeben wird. Entscheidend für den Schutz der Privatsphäre von Personen ist demnach die Frage, wer diese Datenspuren empfangen und lesen kann, und wie man sich vor der unkontrollierten Aussendung von Datenspuren selber schützen kann.

Die Ansammlung und Auswertung von Datenspuren ist bei lizenzpflichtigen drahtlosen Kommunikationstechnologien (GSM, UMTS) gesetzlich geregelt (Bundesdatenschutzgesetz [1], Artikel 10 Grundgesetz [2]). Die Privatsphäre der Nutzer ist hier relativ gut geschützt, obwohl aktuelle Entwicklungen, wie z.B. die Handyortung von Kindern, auch hier Datenschutzaspekte gefährden.

Bei lizenzfreien Funktechnologien, wie z.B. bei Bluetooth [3] und IEEE 802.11 (WLAN) [4], lässt sich eine gesetzliche Kontrolle von Datenspuren nicht einfach durchsetzen, da diese Technologien am Markt frei verfügbar und damit von jeder privaten Person eingesetzt werden können. Kommerzielle Anbieter von IEEE 802.11 und Bluetooth-Zugangsnetzwerken sind zwar ebenfalls an gesetzliche Regelungen gebunden, jedoch lassen sich Bluetooth und IEEE 802.11 auch ganz ohne einen kommerziellen Anbieter betreiben. Ein Nutzer kann in diesem Fall nicht mehr davon ausgehen, dass mit den von ihm erzeugten Datenspuren gesetzeskonform umgegangen wird.

Wie schon bereits erwähnt, sind die am gebräuchlichsten eingesetzten drahtlosen Kurzstrecken-Kommunikationstechnologien für mobile Geräte Bluetooth und IEEE 802.11 (WLAN). Nach einer anfänglichen Diskussion über die Verträglichkeit beider Technologien miteinander, werden mittlerweile beide Technologien parallel in Abhängigkeit von der erforderlichen Reichweite, der Datenrate und vom Energieverbrauch in mobilen Geräten eingesetzt.

Für die Analyse von Datenspuren bei drahtlosen Kommunikationstechnologien sind folgende Kriterien von Bedeutung:

- Gibt es eindeutige, nicht veränderliche Merkmale?
- Werden Statusinformationen an die Umgebung abgestrahlt?
- Mit welchem Aufwand lassen sich Datenspuren empfangen?

Die durchgeführte Analyse [5] von Bluetooth und IEEE 802.11 zeigt, dass beide Technologien eindeutige Gerätemerkmale in Form von Geräteadressen besitzen. Bei Bluetooth sind Geräte durch eine eindeutigen 48-bit Adresse (BD_ADDR) gekennzeichnet, bei IEEE 802.11 durch eine eindeutige und nicht änderbare EAI-48 MAC

Adresse. Diese werden im Produktionsprozess vom Hersteller fest vergeben und sind nicht änderbar.

In Bezug auf ausgestrahlte Statusinformationen werden bei IEEE 802.11 Beacon Pakete vom Access-Point periodisch gesendet, um eine gemeinsame Zeitbasis innerhalb einer Zelle zu gewährleisten. Jeder Access-Point lässt sich damit anhand der Beacon-Pakete lokalisieren. Der Empfang von Beacon-Paketen ist durch keinerlei Sicherheitsmaßnahmen geschützt, da er Voraussetzung für einen erfolgreichen Kommunikationsaufbau ist.

Im Gegensatz zu IEEE 802.11 werden bei Bluetooth keine Beacon Pakete periodisch ausgesendet. Kommunikationsbereite Bluetooth-Geräte werden mit Hilfe einer Suchfunktion (Bluetooth Inquiry) gefunden. Als Ergebnis erhält das suchende Bluetooth Gerät die Geräteadressen und Zeitinformationen benachbarter Kommunikationspartner und damit verfolgbare Datenspuren.

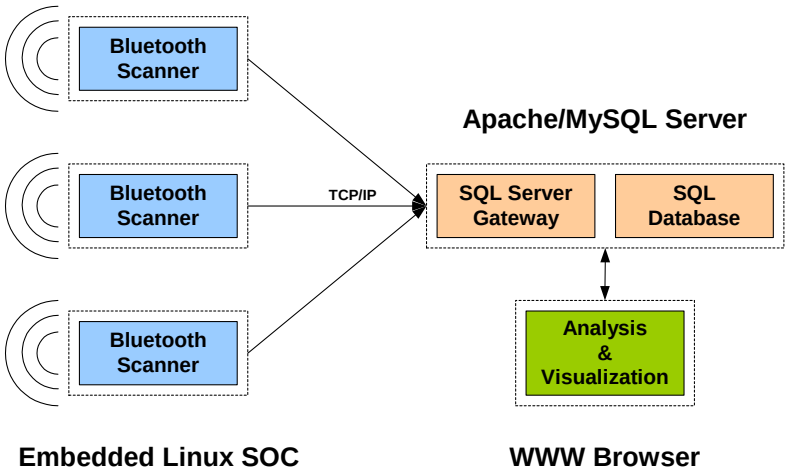

Abbildung 1 BlueTrack Systemarchitektur

BlueTrack

Neben der theoretischen Untersuchung von Datenspuren wurde auch eine praktische Analyse von Datenspuren speziell bei Bluetooth Geräten durchgeführt. Dafür wurde das BlueTrack System entwickelt. BlueTrack besteht aus verteilten, eingebetteten Sensoren zur Erkennung von Bluetooth Geräten und einer zentralen Datenbank. Der Versuchsaufbau umfasst drei Sensoren, die in den Gängen eines Gebäudes platziert wurden. Die BlueTrack Sensoren suchen mittels der Bluetooth Inquiry Funktion nach aktiven Bluetooth Geräten in der näheren Umgebung. Jedes gefundene Gerät wird mit seiner eindeutigen Bluetooth Adresse, einem Zeitstempel, dem jeweiligen Aufenthaltsort und dem Gerätenamen vom Sensor an die zentrale Datenbank übermittelt. Die gesammelten Datensätze lassen sich anschließend über einen WEB Server abrufen und auswerten. Abbildung 1 zeigt den schematischen Aufbau des BlueTrack Systems.

Erste praktische Ergebnisse zeigen, dass erstaunlich viele Benutzer von mobilen Geräten mit Bluetooth Schnittstelle, wie z.B. Mobiltelefonen und Personal Digital Assistants (PDA), mit diesem noch sehr einfach gestalteten System entdeckt werden können. Obwohl das Testgelände im Moment nur sehr begrenzt ist (Universitätsgebäude), lassen sich sehr aufschlussreiche Bewegungsprofile von Testkandidaten, wie z.B. der regelmäßige Besuch von Vorlesungen, erstellen.

Strategien zum Schutz der Privatsphäre

Eine Funktechnologie, die die Privatsphäre des Nutzers schützt, zeichnet sich durch eine Änderbarkeit identifizierender Gerätemerkmale aus. Damit ließe sich die Verkettung von Funkaktivitäten über identifizierende Gerätemerkmale wie statische MAC-Adressen ausschließen. Eine weitere Strategie ist, dass die Funktechnik nur aktiv sein darf, wenn der Nutzer es verlangt. Damit kann ein mobiles Endgerät nicht mehr aufgrund von protokollbedingten Funkaktivitäten von anderen Netzwerkteilnehmern bemerkt werden. Die dritte Strategie zum Schutz der Privatsphäre ist die Forderung nach einem unbemerkbaren Empfangs von Broadcast-Nachrichten, die es Benutzern von mobilen Endgeräten ermöglicht, Dienstbeschreibungen von angebotenen Dienstanbietern passiv zu empfangen.

Literatur

[1] Bundesdatenschutzgesetz (BDSG), http://www.bfd.bund.de/information/BDSG.pdf

[2] Grundgesetz (GG) für die Bundesrepublik Deutschland, Artikel 10, Brief-, Post- und Fernmeldegeheimnis

[3] Specification of the Bluetooth System (Specification), Version 1.1, Februar 2001.

[4] The Institute of Electrical and Electronics Engineers, Inc.: Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. New York, NY 10016-5997, USA.

[5] Haase, M.; Handy, M.; Timmermann, D.: Anonymitätsaspekte bei Bluetooth und WLAN, 4.IuK-Tage Mecklenburg-Vorpommern, Rostock, Juni 2003

Verfasser

Dipl.-Ing. Marc Haase, Dipl.-Wirtsch.-Ing. Matthias Handy, Prof. Dr. Dirk Timmermann

Universität Rostock, Fakultät für Informatik und Elektrotechnik

Institut für Angewandte Mikroelektronik und Datentechnik

Richard-Wagner-Str. 31

18119 Rostock