Datenübertragung im Automobil –

mit Bluetooth und sicher?

Bei der Diskussion im Zusammenhang mit drahtloser Kommunikation geht es mittlerweile um eine Vielzahl von Techniken, Netzwerkstrukturen, Reichweiten und unterschiedlichen Übertragungsraten. Längst sind neben Wireless Local Area Networks (WLANs) auch die Wireless Personal Area Networks (WPANs) hier ein wichtiger Aspekt. Die WPANs werden zunehmend interessant für eine Vielzahl von Anwendungsbereichen und haben durch Bluetooth einen starken und leistungsfähigen Kommunikationsmittler.

Auch im Bereich der Automobilindustrie hat Bluetooth das Potential sich als eine der Kommunikationstechniken der Zukunft zu etablieren: Freisprecheinrichtungen, Navigationsgeräte, Mobiltelefone, DVD-Player und weitere Car-Infotainment-Komponenten könnten so zukünftig kabellos ohne großen Konfigurationsaufwand im Auto betrieben werden. Ob der Schein trügt oder ob es wirklich Gold ist, was da so blau glänzt, ist nur mittels Anwendungsszenarien und mit Hilfe umfassender Sicherheitsanalysen im Car-Infotainment-Bereich zu klären.

Abbildung 1: Bluetooth Logo

Bluetooth im Automobil

Kennt nicht jeder die lästigen Halterungen für Freisprecheinrichtungen im Automobil und das notwendige Übel, das diese bei einem Wechsel des Mobiltelefons ausgetauscht werden müssen?

Wie einfach ist es dagegen, wenn jeder sein Mobiltelefon in der Jackentasche lassen und trotzdem den Komfort der Freisprecheinrichtung nutzen kann. Das ist nur ein Vorteil der Bluetooth-Übertragung; die Einsatzszenarien sind weitaus vielfältiger: Externe Ein- und Ausgabegeräte können ohne großen Aufwand drahtlos miteinander verbunden, Textnachrichten über Tastaturen geschrieben und Navigationssysteme mit Mobiltelefonen synchronisiert werden. Mit der Einführung der Enhanced Data Rate, dem Übergang zu größeren Datenraten in der Bluetooth-Technik, lassen sich auch größere Multimediadaten transportieren. In naher Zukunft könnte Bluetooth alle lästigen Kabel ersetzen und die perfekte drahtlose Umgebung im Automobil schaffen.

Zukünftige Anwendungen

Neben der drahtlosen Kommunikation für die Freisprecheinrichtung denken viele Automobilhersteller aber schon heute über weitere Dienste nach, die in naher Zukunft über Bluetooth ansprechbar sein sollen. Eine Ausbreitung der drahtlosen Kommunikation zieht jedoch auch die weitere Kopplung schon bestehender Bussysteme mit sich. Bussysteme wie der CAN-Bus realisieren seit Jahren die Datenübertragung in der Automobilelektronik und sind aus dem Betrieb im Kfz nicht mehr wegzudenken. Über diese Systeme kommunizieren nicht nur Multimediakomponenten – auch Motor- und Getriebesteuerung tauschen ihre Daten darüber aus. Etabliert sich in diesem Bereich die drahtlose Übertragung als Standard, könnten Sicherheitslücken, wie sie in der Bluetooth-Technik gefunden wurden, mehr als nur einen Eingriff in die Privatsphäre bedeuten. Momentan wird noch eine physikalische Ankopplung an die Steuergeräte der Automobilelektronik benötigt, um Software-Updates aufzuspielen; in Zukunft sind hierfür Techniken wie Bluetooth einsetzbar, wodurch eine Manipulation an wichtigen Steuerelementen leichter realisierbar sein könnte.

Bluetooth Sicherheitsmechanismen im Überblick

Bei den Sicherheitsmechanismen der Bluetooth-Technologie kann man von einer Sicherheit auf Raten sprechen. Dem Benutzer werden einige Funktionen angeboten, doch liegt es allein im Ermessen der Kommunikationspartner, ob sie diese Sicherheit auch nutzen wollen.

Ganz allgemein gibt es bei Bluetooth drei Sicherheitsmodi:

Der Sicherheitsmodus 1 (Non-Secure Mode) bietet neben dem Pairing-Prozess und dem Frequenzsprungverfahren keinerlei Sicherheitsmechanismen. Das Frequenzsprungverfahren dient allerdings eher dazu Störern im Funkraum auszuweichen, anstatt eine gezielte Attacke zu verhindern.

Der Sicherheitsmodus 2 (Service-Level Enforced Security) bietet zusätzlich optionale Sicherheitsmechanismen auf Dienstebene. Nutzen die höheren Dienste nach dem Verbindungsaufbau keine expliziten Sicherheitsfunktionen, sind Sicherheitsmodus 1 und 2 identisch.

Der Sicherheitsmodus 3 (Link-Level Enforced Security) nutzt eine Authentifikation und eine Verschlüsselung schon beim Verbindungsaufbau. Beide Sicherheitsmechanismen sind ein fester Bestandteil der Bluetooth-Spezifikation und schützen in diesem Modus die Daten der Kommunikationspartner.

Konkret bietet Bluetooth drei Sicherheitsfunktionen, die eine vertrauenswürdige und geschützte Kommunikation ermöglichen sollen. Das Pairing zweier Endgeräte ist ein notwendiges Sicherheitsprotokoll,

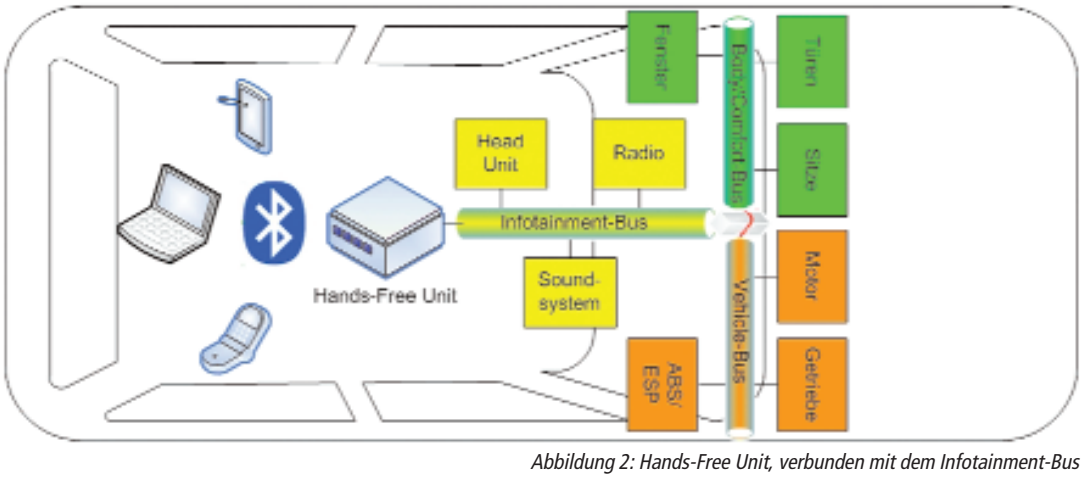

Abbildung 2: Hands-Free Unit, verbunden mit dem Infotainment-Bus

das bei einem ersten Verbindungswunsch durchlaufen werden muss. Nehmen zwei Bluetooth-Einheiten zum ersten Mal Kontakt miteinander auf, erstellen sie einen Verbindungsschlüssel. Der Verbindungsschlüssel wird für jede weitere Kommunikation mit diesem Endgerät gespeichert oder jedes Mal neu erstellt. In diesen Schlüssel fließt ein PIN (Personal Identification Number) – auch Preshared Secret genannt – ein, der maßgeblich den Sicherheitsstandard der Verbindung beeinflusst. Viele Bluetooth-Schwachstellen beruhen auf einem zu schwachen Preshared Secret.

Wurde das Pairing erfolgreich durchlaufen, bilden eine Authentifikation und eine Verschlüsselung weitere Sicherheitsfunktionen. Wie bei den Sicherheitsmodi erwähnt, ist die Verschlüsselung nicht zwingend vorgeschrieben, sondern kann optional genutzt werden. Sowohl die Authentifikation, als auch die Verschlüsselung nutzen den Verbindungsschlüssel als Eingangsparameter. Die Authentifikation verifiziert den Kommunikationspartner durch ein Challange-Response-Verfahren. Beide Seiten berechnen ein Ergebnis und vergleichen dieses. Nur bei gleichen Verbindungsschlüsseln, gleichen sich auch die Ergebnisse und beweisen damit die Identität der Gegenstelle. Die Verschlüsselung beruht auf dem E0-Algorithmus (Safer+), welcher bei Bluetooth Schlüssellängen von bis zu 128 Bit nutzt. Die konkrete Schlüssellänge wird von dem Gerät bestimmt, welches den kürzesten Schlüssel nutzt. In die Verschlüsselung gehen Parameter wie der Verbindungsschlüssel und eine Zufallszahl ein.
Da die Sicherheit des Verbindungsschlüssels ausschließlich auf dem Preshared Secret beruht, alle anderen Parameter aber auf der Luftschnittstelle im Klartext mitlesbar sind, ist das Preshared Secret mit der notwendigen Sensibilität zu behandeln und sollte von allen Kommunikationspartner dementsprechend gewählt werden.

Bedrohungen

Gerade zum Anfang des letzten Jahres kamen immer häufiger Berichte über Schwachstellen in der Bluetooth-Technik auf. Schlagzeilen vom Auslesen privater Kontaktdaten und Angriffe auf Freisprecheinrichtungen haben die IT-Medien beschäftigt. Einer Gruppe Computerexperten um Martin Herfurt ist es gelungen über eine Freisprecheinrichtung Gespräche im Automobil zu belauschen und Audiodaten auszugeben [2]. Dabei nimmt das Mikrophon im Auto die Rolle einer Wanze ein und der Lautsprecher kann für jede Audioausgabe missbraucht werden. Wird das Mikrophon im Auto als Abhörgerät missbraucht, kann die Kommunikation der Insassen belauscht werden. Dieses Szenario mag zwar nicht bei jedem Gespräch interessant erscheinen, doch könnte man so gezielt hochrangige Personen belauschen. Diese und viele weitere Angriffe beruhen auf einer Schwachstelle in den meisten Freisprecheinrichtungen. Durch zu kurze und triviale Passwörter ist es Unbefugten möglich solche Bluetooth-Einheiten zu missbrauchen und Einfluss auf private Datenbestände zu nehmen.
Die Diskussion um die Schuldfrage für mögliche Angriffe geht grundsätzlich in zwei Richtungen. So werden auf der einen Seite die zu losen Empfehlungen bezüglich der Nutzung der Sicherheitsmechanismen in der Bluetooth-Spezifikation kritisiert und als Hauptgrund für die mangelnde Sicherheitsvorsorge gesehen; auf der anderen Seite herrscht die Meinung vor, dass auch eine zu schwache Implementierung der Sicherheitsmechanismen seitens der Automobil- und Hardwareindustrie für die Schwachstellen verantwortlich ist. Die Bluetooth Spezifikation fordert bei der Wahl des Preshared Secrets eine Mindestlänge von vier Ziffern, gibt aber jedem Hersteller die Möglichkeit Secrets mit einer Länge von bis zu 16 Stellen zu implementieren. Viele Automobilhersteller verwenden in ihren Freisprecheinrichtungen vierstellige, triviale Preshared Secrets und öffnen so Unbefugten den Zugriff auf private Daten und die unberechtigte Nutzung von Diensten. Kombinationen wie „0000" oder „1234" sind keine Seltenheit. Dabei spielt es keine Rolle, ob die Kombination so trivial ist oder etwas raffinierter gewählt, in der heutigen Zeit stellen vierstellige Passwörter, PINs oder Preshared Secrets keinen angemessenen Schutz gegen Angriffe dar.

Schlussbetrachtung und Ausblick

Im Moment ist noch die Bequemlichkeit für den Anwender wichtiger als die notwendigen Sicherheitsvorkehrungen für Daten und Dienste. Sowohl die Elektronikkonzerne als auch die Automobilindustrie müssen dazu angehalten werden eine sicherere Bluetooth-Umgebung zu schaffen. Sind es momentan nur Angriffe auf Freisprecheinrichtungen, können es in naher Zukunft enorme Beeinträchtigungen des Fahrzeugbetriebs sein. Die drahtlose Kommunikation wird früher oder später auch in der Automobilindustrie zum Standard und muss bis dahin ein sicheres Konzept und eine einfache Umsetzung zum Schutz der Daten vor Manipulation bieten.

T. Drecker: „Sicherheitsanalyse der Bluetooth-Schnittstelle mit Blick auf Car-Infotainment-Systeme", Diplomarbeit, Institut für Internet-Sicherheit, FH-Gelsenkirchen 2006

Thomas Drecker, thomas.drecker@internet-sicherheit.de und Prof. Dr. Norbert Pohlmann, norbert.pohlmann@informatik.fh-gelsenkirchen.de, Institut für Internet-Sicherheit
Fachhochschule Gelsenkirchen, www.internet-sicherheit.de

Links

[1]Bundesamt für Sicherheit in der Informationstechnik (BSI) „Bluetooth Gefährdungen und Sicherheitsmaßnahmen (www.bsi.de).
[2] www.trifinite.org
[3] www.bluetooth.com
[4] www.bluetooth.org/specWeitere Informationen über Bluetooth-Sicherheitsmechanismen: Institut für Internet-Sicherheit, http://www.internet-sicherheit.de