Wie sicher sind Lösungen mit Bluetooth?

Zutrittskontrollen auf den (Blau-)Zahn gefühlt

Die Bluetooth-Spezifikation bietet bereits sehr komfortable Lösungen für mobile Systeme. Auch Zutrittskontrollsysteme mit dem Handy und mobile Fingerabdruckscanner sind am Markt verfügbar. Die Spezifikation der Technologie bietet ausreichende Möglichkeiten, um eine ähnliche Sicherheit zu gewährleisten wie ein Schlüssel-Schloss System – aber nur dann, wenn alle Sicherheitsmechanismen ausgeschöpft und die Umsetzungen der Technologie vertrauenswürdig sind.

Von Markus Linnemann (l.) und Prof. Dr. Norbert Pohlmann Gelsenkirchen

Die Bürotür schließt sich automatisch, das Garagentor geht auf, ohne dass man aussteigen muss und den Fingerabdruckscanner kann man in der Hosentasche bedienen.

Aktuell findet sich die Bluetooth-Technologie, die solche Vorgänge ermöglicht, in fast allen mobilen Geräten, wie Handys, Headsets, Navigationsgeräten oder auch Laptops.

Innovative Anbieter nutzen die Technologie verstärkt für Lösungen der Zutrittskontrolle oder einer anderen Art der Authentifizierung, etwa in sicherheitskritischen Geräten, wie Kartenlesern, Zeiterfassungsgeräten oder biometrischen Scannern. Die Idee ist, dadurch sowohl den Komfort als auch die Sicherheit zu erhöhen. Die Sicherheitsanforderungen an Funknetzwerke sind in diesen Einsatzfällen daher besonders hoch. Die Bluetooth-Spezifikation bietet hier alle Vorkehrungen, um Sicherheit zu gewährleisten. Sie bietet drei unterschiedliche Sicherheitsstufen, die bis hin zu einer 128bit Verschlüsselung und obligatorischer Authentifizierung reichen. Grundsätzlich bietet Bluetooth also die Möglichkeit einer sicheren Verbindung. Wie sieht es jedoch mit den Anwendungen in der Realität aus?

Das erste Treffen!

Die Rose im Knopfloch ist ein übliches Erkennungsmerkmal beim ersten Treffen. Nachdem die Rose entdeckt wurde, folgt das gegenseitige Vorstellen. Bluetooth-Geräte arbeiten nach dem selben Prinzip, genannt „Pairing“. Ein Handy zeigt seine MAC-Adresse (eindeutige Adresse) nach außen, sucht nach Bluetooth-Geräten und findet beispielsweise eine Türschließanlage, die ebenfalls ihre MAC-Adresse preisgibt. Jetzt folgt das gegenseitige Bekanntmachen. Das Handy sendet eine Zufallszahl an das Schlosssystem und unter Zuhilfenahme der MAC-Adresse des anfragenden Handys, der Zufallszahl und einer PIN wird ein Verbindungsschlüssel (Link-Key) erzeugt und innerhalb beider Geräte mit der dazugehörigen MAC-Adresse gespeichert. Der PIN ist der für die Sicherheit entscheidende Faktor. Dieser wird in beiden Geräten eingegeben, oder er ist in einem Gerät voreingestellt. Der PIN wird nicht im Klartext übertragen, sondern lediglich für die Berechnung des Schlüssels auf beiden Seiten verwendet. Grundsätzlich ist die PIN-Länge bis zu 16 Zeichen frei wählbar.

Der Pairing-Prozess ist unter Sicherheitsaspekten der Knackpunkt jeder Bluetooth-Kommunikation. Während des Pairingvorgangs sind die MAC-Adressen beider Geräte sichtbar. Ist die PIN gut gewählt, das heißt, ist sie deutlich länger als 10 Zeichen, ist eine Attacke auf den Pairing-Prozess sehr schwierig. Bei schlechter Wahl des PINs werden die Geräte angreifbar.

Ein Beispiel liefern Angriffe auf Headsets und Freisprecheinrichtungen. Diese arbeiten in der Regel mit voreingestellten kurzen PINs wie 0000, 1111 oder 1234, da sie aus Komfort- und Platzgründen am Headset nicht einstellbar sind. Wenn ein mit dem Headset verbundenes Telefon ausgeschaltet wird, sucht das Headset einen neuen „Partner“. Wer die MAC-Adresse des Headsets kennt, kann sich jetzt mit diesem verbinden und es als „Wanze“ verwenden oder auch Geräusche einspielen. Die MAC-Adresse kann bei aktuellen Geräten allerdings nur während eines Pairing-Prozesses mitgeschnitten oder durch einen aufwendigen Brute-Force-Angriff (automatisiertes Ausprobieren aller Kombinationen) erlangt werden. Ältere Autofreisprecheinrichtungen waren der Einfachheit halber so konfiguriert, dass die MAC-Adresse permanent sichtbar war, um das Verbinden zu vereinfachen. Dies ist sicherheitstechnisch natürlich unverantwortbar.

Das Wiedersehen!

Beim nächsten Kontakt der beiden Bluetooth-Geräte gibt es ein Wiedersehen, die Geräte kennen sich bereits. Es findet eine Authentifizierung statt. Durch ein Challenge-Response-Verfahren überprüfen die Geräte, ob sie den beim Pairing-Vorgang erstellten Link-Key besitzen. Bei erfolgreicher Überprüfung kann die Kommunikation beginnen. Die Authentifizierung kann im non-discoverable Modus stattfinden. Die MAC-Adresse ist beim Wiedersehen also nicht zwingend sichtbar, was das Sicherheitsniveau erhöht. [1]

[1] T. Drecker, Bluetooth Sicherheitsanalyse, Diplomarbeit if(is), 2006

Die Link-Keys können vom Benutzer gelöscht werden. In diesem Fall muss das Pairing wiederholt werden. Einzelne Systeme bieten das erneute Pairing als Sicherheitsfeature an, da eine Speicherung der Link-Keys damit entfallen kann. Auf der anderen Seite ist der Pairing-Prozess abhörbar und damit eher eine Schwachstelle.

Um einen Angriff auf bereits verbundene Geräte durchzuführen, müssten die Geräte zum erneuten Pairing aufgefordert werden. Hierfür existieren drei allerdings nicht triviale Vorgehensweisen, die von Yaniv Shaked and Avishai Wool [2] beschrieben werden. Sie haben es damit geschafft, den Pairing-Prozess mitzuschneiden und die PIN zu rekonstruieren.

Man tauscht sich aus!

Das Kennenlernen ist vorbei und man möchte Vertrauliches austauschen. Vielleicht indem man in einer eigenen Sprache spricht. Bluetooth löst diese Aufgabe durch eine bis zu 128bit Verschlüsselung. Diese nutzt beispielsweise ein Fingerabdruckscanner, der die biometrischen Daten komfortabel per Bluetooth übertragen kann. Dessen Daten dürfen nach der Authentifizierung nicht unverschlüsselt durch die Luft gesendet werden, da sie somit direkt mitlesbar wären. Bluetooth nutzt einen Algorithmus (Safer+), der unter anderem den Link-Key, die MAC-Adressen und diverse Zufallszahlen für die Verschlüsselung verwendet. Manchmal ist aber auch nur eine geringere Verschlüsselung von beispielsweise 56bit möglich. Die ist heute aber nicht mehr als sicher anzusehen.[3] Auch die 128bit Verschlüsselung des verwendeten E0-Algorithmus wird nicht als absolut sicher angesehen. Allerdings ist hier immenser Aufwand für eine Attacke notwendig.

Die Bluetooth-Technologie verspricht also grundsätzlich eine solide Sicherheit, allerdings nur dann, wenn

- ein PIN mit mehr als 10 Stellen gewählt wird,
- der Pairing-Prozess möglichst an einem vertrauenswürdigen Ort durchgeführt wird (kein Angreifer in Reichweite),
- die Datenübertragung mit voller 128bit Verschlüsselung gesichert ist,
- der non-discoverable-Modus verwendet werden kann.

Schwachstellen in der Bluetooth-Umsetzung

Für fünf Euro ist es mit einer Chipsdose möglich, eine Richtfunkantenne zu bauen, die die Reichweite von Bluetooth auf bis zu 2 km erhöht. Gezielte Angriffe auf Pairing-Prozesse sind damit auch außerhalb der Standardreichweite der BT-Spezifikation durchführbar.

Fehleranfällig sind auch die Umsetzungen der BT-Spezifikation. So gibt es ältere Handymodelle, bei denen das Auslesen des Telefonbuchs und das Schicken einer SMS über die BT-Schnittstelle kein wirkliches Problem darstellen, da in der Umsetzung eines Profils (Object Push Profile), in dem nur das Geben von Daten erlaubt sein soll, auch das „Daten holen“ erlaubt oder keine Authentifizierung implementiert wurde. Finanziell schmerzhaft wird dieser Umstand, wenn jemand jede Nummer des Telefonbuches mit einer 0900-Nummer versieht und das Telefonbuch wieder in das Telefon lädt.

Dies ist kein Fehler der BT-Spezifikation, sondern ein Fehler des Herstellers bei der Programmierung der BT-Schnittstelle. Beim Einsatz sollte also darauf geachtet werden, dass vertrauenswürdige, getestete Lösungen Verwendung finden, beispielsweise nachweisbar durch eine Zertifizierung der Soft-/Firmware.

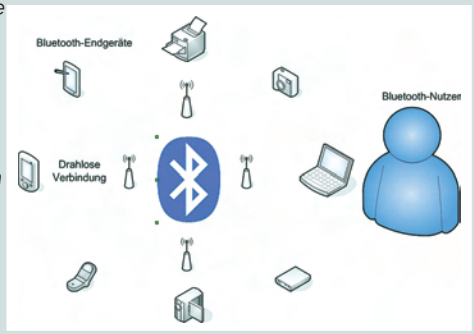
Bei Schließsystemen müssen allerdings weitere Überlegungen angestellt werden. Türen in Reichweite dürfen nicht versehentlich geöffnet werden. Zusätzliche Taster und eine gering eingestellte Reaktionsreichweite können dies verhindern. Falls eine Autorisierung nur auf der MAC-Adresse beruht, kann diese für einen Angriff kopiert und auf ein anderes Gerät übertragen werden. Da- ▶

[2] Yaniv Shaked and Avishai Wool, Cracking the Bluetooth PIN, http://www.eng.tau.ac.il/~yash/shaked-wool-mobisys05/, 2005
[3] Scott R. Fluhrer and Stefan Lucks, Analysis of the E0 Encryption System, http://th.informatik.uni-mannheim.de/people/lucks/papers/e0.5.pdf, 2001

Die Bluetooth-Spezifikation im Überblick

Für Kurzstreckenverbindungen ist seit 1999 die Funktechnologie Bluetooth (BT) spezifiziert, die das Kabelchaos, das durch die Vielzahl an Geräten entstand, minimieren sollte.

Die BT-Technologie ist in der als stabil angesehenen Version 1.1 seit 2001 auf dem Markt und verbreitet sich seitdem rasant, besonders im Mobilfunksektor. Die aktuelle Version 2.1 aus dem Jahr 2007 ist bereits wesentlich schneller und stabiler als die ursprüngliche Spezifikation. Die Reichweite der Technologie ist sehr unterschiedlich und wird in verschiedene Klassen eingeteilt. Von Class 3 Geräten mit einer Reichweite von ca. 1 m geht es bis zu Class 1 Geräten, die bei Sichtkontakt eine Distanz von bis zu 300 m überbrücken können. Standardgeräte funken zumeist ca. 10 bis 20 m weit. Mit 2,1 MBit/s erreicht Bluetooth inzwischen eine Datenrate, die selbst für multimediale Inhalte ausreichend ist. Im Anwendungsfall für Türöffner oder biometrische Lesegeräte ist diese Bandbreite weit mehr als ausreichend.



Bluetooth Piconetz

Der große Vorteil der Bluetooth-Kommunikation liegt im Aufbau eines Ad-hoc Netzwerkes. Zwei oder mehr Endgeräte können, ohne vorher konfiguriert zu werden, miteinander kommunizieren. Diese Kommunikationsumgebung wird Piconetz (siehe Abbildung) genannt und kann bis zu acht aktive Teilnehmer haben. [1] Die Grundlage für eine einfache Kommunikation ist mit Bluetooth-Technologie erreicht.

Da das ISM (Industrial, Scientific and Medical) – Band, auf dem Bluetooth funkt, zwischen 2,402 GHz und 2,480 GHz-Band ein frei verwendbares Frequenzband ist, arbeitet die Technologie mit einem Frequenzsprungverfahren, dem Frequency Hopping Spread Spectrum (FHSS), um gegenseitigen Störungen auf der Luftschnittstelle auszuweichen. Die Frequenz wird innerhalb des Frequenzbandes bis zu 1600 mal pro Sekunde gewechselt. Dadurch werden die Störungen durch WLAN und andere Funknetze auf dieser Frequenz minimiert und das Mitschneiden einer Kommunikation erschwert.

mit lässt sich ein anderes Gerät vortäuschen.

Natürlich unterliegen auch Funk-Lösungen Gefahren wie Diebstahl, andererseits bieten sie Schließmechanismen, die ausschließlich innen angebracht werden können und damit Manipulation von außen nicht ausgeliefert werden.

Letztlich bleibt je nach Anwendungsfall abzuwägen, ob die Bedrohungen für BT-Lösungen höher oder sogar geringer sind und ob der Komfort oder die Sicherheit im Vordergrund steht. Eine ausführliche Prüfung der Lösungen auf die angesprochenen Schwachstellen sollte als absolute Pflicht angesehen werden.

Über unsere Autoren:

Prof. Dr. Norbert Pohlmann ist Geschäftsführender Direktor und Dipl.-Inform. (FH) Markus Linnemann ist Geschäftsführer des Instituts für Internet-Sicherheit an der Fachhochschule Gelsenkirchen (www.internet-sicherheit.de). Kontakt: norbert.pohlmann@informatik.fh-gelsenkirchen.de; markus.linnemann@internet-sicherheit.de

Aus der Praxis: Bluetooth-Handy zur Türöffnung

Mit dem Produkt wirelessKey des österreichischen Unternehmens Sorex Wireless ist im Markt seit Juni 2008 ein System verfügbar, das ermöglicht, bluetoothfähige Mobiltelefone für die Zutrittskontrolle zu nutzen (vorgestellt in WIK 4/2008). WIK fragte Sorex-Geschäftsführer Christian Csank zu den Sicherheitsaspekten der Lösung.

Herr Csank, nutzen Sie Sorex wirelessKey bei sich zu Hause?
C. Csank: Ja, ich nutze wirelessKey zum Öffnen meiner Wohnungstür und bin sehr zufrieden damit.

Durch welche Maßnahmen haben Sie bei sich sichergestellt, dass Ihre Haustür nicht unberechtigt geöffnet werden kann?
C. Csank: Die Sicherheit des Systems wird durch mehrere Faktoren gewährleistet. Das industrielle Bluetooth der Klasse I wechselt 1.600 Mal pro Sekunde die Frequenz, sodass befürchtete Frequenzstörungen ausgeschlossen sind. Auch ist der Code zur Autorisierung mit einer 128-Bit-Verschlüsselung ausgestattet. Dieser wird nur einmal ausgetauscht, nämlich bei der erstmaligen Anmeldung. Dabei ist ein Abfangen des Codes praktisch unmöglich, wenn man darauf achtet, dass man bei der Anmeldung alleine ist. Danach ist der Code im Modul gespeichert und wird jeweils bei Annäherung eines Bluetooth-Handys an die Tür überprüft. Dabei werden keine Daten übertragen. Bei Verlust des Handys kann das System deaktiviert werden. Das Steuerungsmodul an der Tür befindet sich von außen unerreichbar im Innenraum, anders als etwa NFC-Sensoren, Fingerprintsysteme oder Tastaturen von Codeschlössern, die an der Außenseite platziert werden und damit nicht vor Sabotage sicher sind.

Wie wird bei Anwesenheit verhindert, dass sich die Eingangstür aus Versehen unbemerkt öffnet? Schalten Sie Bluetooth am Handy zu Hause aus?
C.Csank: Es gibt zwei Möglichkeiten, dies zu verhindern: Entweder die Montage eines Tasters an der Außenseite der Tür, der gedrückt werden muss, um das Schloss zu öffnen. Oder eine Benachrichtigung am Handy, die zur Öffnung bestätigt werden muss.

Kontakt:Christian Csank, Geschäftsführer der SOREX – Wireless Solutions GmbH, Wiener Neustadt, christian.csank@sorex-austria.com