Zeitschrift: Comtec : Informations- und Telekommunikationstechnologie = information and telecommunication technology

Herausgeber: Swisscom

Band: 82 (2004)

Heft: 4

Artikel: Sicherheitsrisiken durch Bluetooth?

Autor: Sellin, Rüdiger

DOI: https://doi.org/10.5169/seals-876854

Sicherheitsrisiken durch Bluetooth?

RÜDIGER SELLIN **Viren und Würmer befallen nun auch das Handy – kaum ist eine neue Variante aufgetaucht, bietet auch schon irgendein IT-Security-Dienstleister eine dafür passende Lösung an. Alle bekannten unberechtigten Zugriffe auf das Handy erfolgen über eine fehlerhafte lokale Bluetooth-Schnittstelle. Die Einschätzungen der effektiven Bedrohung gehen aber weit auseinander.**

Die Fachwelt und viele Anwender mobiler Services werden immer wieder mit der Frage konfrontiert, ob das Handy eine Angriffsfläche für Attacken biete. Jedes technische System wird mit zunehmender Funktionalität komplexer, was etwa von den PCs hinlänglich bekannt ist. Dort wurden den Angriffen von aussen (z. B. über Disketten, die von Viren befallen sind) mit der zunehmenden Internet-Vernetzung völlig neue Dimensionen eröffnet. Bei den Handys liegt der Fall anders, weil die Kommunikation über GSM- oder UMTS-Netze in hohem Masse abhör- und angriffssicher ist. Darum kann ein potenzieller Angreifer auch nicht ungehindert über diese mobilen Kommunikationsnetze auf das Handy gelangen, sondern nutzt dazu dessen lokale Bluetooth-Schnittstelle. Allen bisher Szenarien ist nämlich gemeinsam, dass die Angriffsversuche auf bekannten Sicherheitslücken des aktuellen Bluetooth-Standards basieren. Die Ausnutzung dieser Lücken bedarf allerdings eines detaillierten Fachwissens und entsprechender Angriffswerkzeuge. Darunter ist unter anderem eine situationsgerechte, das heisst, eine für das anzugreifende Objekt passende Hard- und Software-Ausrüstung zu verstehen.

Neben einem entsprechend aufgerüsteten Laptop mit Bluetooth-Schnittstelle ist die genaue Kenntnis des anzugreifenden Objekts und dessen Sicherheitslücken eine wichtige Grundvoraussetzung für eine erfolgreiche Attacke. Ohne Insider-Wissen und hoch stehende Infrastruktur läuft per se also wenig. Auffallend ist auch, dass die Meldungen zu erfolgreichen Attacken überproportional häufig von Firmen veröffentlicht werden, die auch gleich eine Lösung des Problems anbieten. Daher stellt sich die Frage nach dem effektiven Umfang der Bedrohung.

Bluetooth-Mängel

Einem bereits Ende 2003 unter www.thebunker.net veröffentlichten Bericht zufolge weisen die Bluetooth-Schnittstellen diverser Handys Implementationsfehler auf. Mit einem als «Snarf-Attack» bezeichneten Angriff ist es möglich, über Bluetooth Verbindungen zu anderen Handys aufzubauen, ohne dass das Gerät des Opfers etwas anzeigt – dies sogar im Hidden- oder Invisible-Modus. Mit der «Snarf-Attack» erhält der Angreifer Zugriff auf Adressbuch, Kalender, Uhr und weitere Daten wie der IMEI (International Mobile Equipment Identity). Dieser Angriff beruht auf Schwächen in den Zugriffskontrollen verschiedener Handy-Typen. Adam Laurie, Sicherheitschef des britischen Secure-Hosting-Unternehmens A. L. Digital und Betreiber obiger Homepage, testete nach eigenen Angaben erfolgreiche Snarf-Angriffe unter anderem auf den älteren Modellen von Sony Ericsson (T68, T68i und T610) und Nokia (6310i und 7650). Diese stehen immer noch im Einsatz.

Für gewisse Nokia-Modelle bestehe nach Angaben von Adam Laurie ein weiteres Sicherheitsproblem. Der so genannte Pairing-Mechanismus ermögliche das Autorisieren bestimmter Bluetooth Devices auf Dauer. Normalerweise zeige das Gerät alle derart autorisierten Gegenstellen an. Doch wegen eines Implementierungsfehlers könnten bestimmte Geräte in dieser Liste nicht mehr auftauchen. Trotzdem könnten sie eine Verbindung herstellen und sogar weitere Verbindungen zu Gegenstellen aufnehmen, die im Handy des Opfers als autorisierte Pairing-Partner eingetragen seien. Dadurch sei es nicht nur möglich, Dateien zu übertragen, sondern auch Internet-, WAP- oder GPRS-Verbindungen auf dessen Kosten aufzubauen. Beim Pairing mit anderen Bluetooth-Geräten sollte man deshalb niemals Geräte autorisieren, deren Besitzer man nicht kenne – selbst dann nicht, wenn der vermeintliche Name des Geräts vertrauenswürdig erscheine. Die praktische Gefahr eines solchen Angriffs könne als sehr gering eingestuft werden, weil sich die Laborbedingungen nur unter unrealistischen Annahmen in der Praxis realisieren liessen. Für einen erfolgreichen Angriff müsse zum Beispiel im Voraus bekannt sein, welches Handy das Opfer wann und an welchem Ort einsetze, um dann mit einer entsprechenden IT-Infrastruktur möglichst unauffällig am Aufenthaltsort des Opfers anzurücken. Solche Szenarien taugten daher wohl eher für Krimis und Spionagegeschichten.

Ein weiterer Trick ist das «Bluejacking», mit dem man auf fremden Bluetooth-Handys direkt eine Nachricht anzeigen lassen kann. Normalerweise erscheint auf einem Bluetooth-Gerät der «Name» der Gegenstelle, die versucht, eine Verbindung herzustellen. Dieser Name ist jedoch frei definierbar und kann bis zu 248 Zeichen lang sein. Mit verwirrenden Anweisungen kann man Nutzer dazu verleiten, mit der erforderlichen Passwortbestätigung die Verbindung zu autorisieren, womit dann alle Daten des Zielgeräts lesbar werden. Erscheint das Gerät dann nicht einmal in der Liste der autorisierten Gegenstellen, kann das Opfer den unberechtigten Zugriff auf das Handy kaum noch bemerken. Die betroffenen Hersteller schreiben die Sicherheitslücken dem

Standard bzw. dessen Implementation zu. Daher kann man davon ausgehen, dass neben Handsets auch PCs und PDAs mit Bluetooth-Schnittstelle von der Thematik betroffen sind. Zum Schutz vor solchen Attacken sollte der Handy-Benutzer Bluetooth einfach deaktivieren. Zudem ist international bisher kein Fall bekannt, in dem ein Virus das mobile Endgerät eines Benutzers infiziert hätte. Bisherige Pressemeldungen basieren auf Herstellerinformationen von Anti-Virus-Tools.

Bedrohung des öffentlichen WLAN-Zugangs?

Anfang Mai 2004 wurde die Fachwelt durch eine Meldung unter www.heise.de nochmals auf die Sicherheitslücken der Bluetooth-Schnittstelle aufmerksam gemacht. Dort wird auf gross angelegte Laborversuche des Sicherheitsdienstleisters Integralis (www.integralis.de) hingewiesen, bei denen mithilfe eines mit spezieller Software ausgerüsteten Laptops und unter detaillierter Kenntnis des anzugreifenden Handys Daten vom Handy, wie das persönliche Telefonbuch, kopiert werden konnten. Dieser Umstand war bereits seit Ende 2003 bekannt, wurde aber nicht so breit ausgeschlachtet. Am 14. Juni 2004 wurde aus den gleichen Quellen unter den Titeln «Bluetooth-Handys ermöglichen WLAN-Surfen auf fremde Kosten» (Heise) bzw. «Warnung vor Hotspot-Vampiren» (Integralis) bekannt, dass der Missbrauch des PWLAN-Zugangs über die Bluetooth-Schnittstelle in den Hotspots von T-Mobile und Vodafone grundsätzlich möglich sei. Dabei werden wiederum die bereits vorgängig erwähnten Implementationsmängel von bestimmten Bluetooth-Handy-Modellen ausgenutzt. Eine Liste der unter Laborbedingungen getesteten Handys findet sich unter www.integralis.de/media/press_releases/ index.html

Im Normalfall melden sich T-Mobile- und Vodafone-Kunden mit ihrem WLAN-Notebook – ähnlich wie in den kostenpflichtigen Hotspots von Swisscom Mobile – durch Anforderung eines Passworts via SMS und dessen an schliessende Eingabe auf dem Laptop im Hotspot an. Diese Zugangsdaten werden auf dem Laptop in den Browser bei der Verbindungsaufnahme zum Hotspot übertragen. Anders als in den Hotspots von Swisscom Mobile verfallen diese Zugangsdaten bei T-Mobile aber nicht. Sie gelten zudem an sämtlichen T-Mobile-Hotspots in Europa und in den USA. Bei Vodafone Deutschland kann ein authentifizierter Account weltweit an allen Vodafone-Hotspots wahlweise während dreissig Minuten, drei oder 24 Stunden genutzt werden.

Swisscom Mobile stuft das Risiko für einen solchen Angriff aus folgenden Gründen insgesamt als gering ein:

- In den Hotspots von Swisscom Mobile wird jede PWLAN-Session neu authentisiert; das heisst, nach einer Unterbrechung oder am Ende der Session muss der Nutzer ein neues Passwort anfordern. Auch mehrere parallele Sessions sind nicht möglich (z. B. eine des regulären Nutzers und eine des Angreifers).
- Der Angreifer muss das Handy des Opfers sehr genau kennen und über die passende Software zur Durchführung eines Angriffs auf einem speziell dafür ausgerüsteten Laptop mit Bluetooth-Schnittstelle verfügen.
- Der Angreifer muss sich im gleichen Raum wie sein Opfer befinden und sein Opfer entweder kennen, um einen gezielten Angriff schnell durchführen zu können, oder obige Voraussetzungen rein zufällig erfüllen, was eher unwahrscheinlich sein dürfte.

Bei sensitiven Anwendungen empfiehlt Swisscom Mobile, die Bluetooth-Schnittstelle bei Nichtgebrauch generell auszuschalten und vor deren Aktivierung abzuwägen, ob der Ort der Anwendung als sicher bezeichnet werden kann. Bei unbekannten PC- oder Laptop-Anwendern innerhalb von rund 15 m Radius – etwa in fremden Büroumgebungen oder an einem PWLAN-Hotspot mit unbekannten Benutzern – sollte die Bluetooth-Schnittstelle wiederum deakti-

Was ist Bluetooth?

Bluetooth ist eine drahtlose Funkschnittstelle für die Daten-, Sprach- und Multimediaübertragung und soll primär dazu beitragen, den Kabelsalat im Büro oder unterwegs zu vermindern. Bluetooth wurde aber für weitaus mehr als nur für den «Kabelersatz» entwickelt. Die Spezifikationen von Bluetooth beinhalten eine Reihe von Anwendungsprofilen und -protokollen:

- Service Discovery: automatisches Auffinden anderer Bluetooth-User, -Geräte und -Dienste
- Headsets: drahtlose Freisprecheinrichtungen
- Telephony: lokale, drahtlose Kommunikation oder drahtloser Zugang zu öffentlichen Sprachnetzen
- Synchronisation: Synchronisieren von Terminen oder anderen Einträgen zwischen Handy, PDA und PC
- File Transfer: Transfer von umfangreichen Dateien unabhängig vom Betriebssystem
- Data Transfer: funktional vollständiger Zugang zu Inhouse-Datendiensten
- WAP: Zugang zu internen WAP-Servern über Bluetooth statt über das öffentliche Mobilfunknetz

Bluetooth sendet im so genannten ISM-Band (Industrial Scientific and Medical) auf der 2,4-GHz-Frequenz. Dieses Frequenzband ist weltweit lizenzfrei verfügbar, wird allerdings auch von anderen Anwendungen wie den Wireless Local Area Networks (WLANs) verwendet. Bluetooth wurde wegen der potenziellen Gefahr von Störungen robust ausgelegt, so zum Beispiel mit einer speziellen Prozedur für den Frequenzwechsel («Frequency Hopping»). Die Datenübertragung erfolgt bei Bluetooth mit Datenpaketen, wobei nach jedem empfangenen oder gesendeten Paket die Frequenz gewechselt wird, um die Wahrscheinlichkeit von Interferenzen zu minimieren. Im Vergleich zu anderen Anwendungen benutzt Bluetooth zudem kleinere Datenpakete und wechselt häufiger die Frequenz, was eine sehr schnelle Acknowledgement-Prozedur zwischen Sender und Empfänger bedingt. Im Standard ist auch für die Sicherheit der Bluetooth-Verbindung gesorgt, da alle Bluetooth-Pakete verschlüsselt übertragen werden. Darüber hinaus sorgt eine spezielle Fehlerkorrektur mit verschiedenen Korrekturstufen für eine Kompensation wechselnder Bedingungen im Funkfeld. Problematisch scheint aber die schnelle Acknowledgement-Prozedur zu sein, weil sie den Berichten zufolge keine effektive Zugriffssicherheit bereitstellt.

viert werden. Handy-Besitzer sollten sich zudem beim jeweiligen Hersteller nach neuen Firmware-Versionen für ihre mobilen Endgeräte erkundigen, um die Sicherheit der Bluetooth-Schnittstelle am mobilen Endgerät zu verbessern. Nokia und Sony Ericsson haben übrigens eine verbesserte Software für ihre Handys mit Bluetooth-Schnittstelle angekündigt, allerdings ohne konkrete Zeitangaben.

Weitere Entwicklungen

Seit Mitte Juli sind auch Viren auf Handys mit Microsoft-Betriebssystem und ARM-Prozessor bekannt. Diese verfügen jedoch noch nicht über einen automatisierten Verbreitungsmechanismus und müssen durch die Benutzer manuell weiterverbreitet werden. Diese Verbreitung nutzt auch nicht Sicherheitslücken von Bluetooth aus, sondern läuft ähnlich wie beim PC über den ganz normalen Kommunikations-Link des mobilen Endgeräts, beispielsweise über E-Mail, Bluetooth oder USB. Aber auch hier wird die effektive Gefahr als gering angesehen. Gleichwohl verfolgen Swisscom Mobile und andere Anbieter die Entwicklung aufmerksam und treffen bei Bedarf entsprechende Massnahmen.

Eine gute Nachricht zum Schluss

Durch die Einführung der technisch bereits implementierten Neuentwicklung mit dem Namen EAP-SIM (Extensible Authentication Protocol, Subscriber Identification Modul) wird Bluetooth beim Knacken des WLAN-Zugangs künftig keine Rolle mehr spielen. Dieser neue PWLAN-Zugang erfolgt unabhängig von der SIM-Karte im Handy über eine Data-SIM. Die Data-SIM muss aber in jedem Fall für den EAP-SIM-Client erreichbar sein (das heisst auf dem Laptop in der WLAN-PCMCIA-Karte oder im USB-Dongle). Durch die Gesamtheit dieser neuen Massnahmen wird der Missbrauch praktisch unmöglich. Dieses neue Angebot wird voraussichtlich ab Herbst 2004 nur in Kombination mit Natel Data Basic zur Anwendung kommen. EAP-SIM wird im September 2004 auch beim neuen Angebot «Mobile Unlimited» als Technologie für PWLAN eingesetzt. ■

Rüdiger Sellin, Dipl.-Ing., PR-Manager und freier Autor,
Marketing Communications, Swisscom Mobile, Bern

Referenzen

- Sicherheit in Wireless LANs, Rüdiger Sellin, Beitrag in comtec 3/2004
- IEEE-Standard 802.11i, WLAN Security, www.ieee.org
- Infos zu PWLAN: www.swisscom-mobile.ch/pwlan