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

Band: 82 (2004)

Heft: 2

Artikel: Sicherheitslücken bei Bluetooth-Handys

Autor: Sellin, Rüdiger

DOI: https://doi.org/10.5169/seals-876831

Fähigkeit, Informationen über Stube und Büro hinweg direkt dorthin zu liefern, wo sie in diesem Moment benötigt und konsumiert werden, als bezahlungswürdig wahrgenommen.

Im Fall der MeteoSchweiz-Applikationen werden zwei Zahlungsarten umgesetzt: Mit einem Sunrise-Abonnement kann direkt via Mobiltelefonrechnung bezahlt werden, für alle anderen Provider kommt das MeteoSchweiz-E-Wallet zum Zug. Für E-Wallet ist eine Anmeldung per Internet nötig, dafür ist die Bezahlung unabhängig vom Mobilfunkanbieter, und es können auch grössere Beträge abgewickelt werden.

Fazit

Viele Handy-Besitzer wissen nicht von den Fähigkeiten ihres Mobiltelefons. Sie reagieren mit Überraschung und Begeisterung, wenn sie die interaktiven MeteoSchweiz-Applikationen auf ihrem eigenen Gerät sehen. Java wird im Bereich Mobilkommunikation vorwiegend mit Spielen (Java Games) assoziiert. Dank Java ist es möglich, interaktive Dienste auf die Mobiltelefone zu bringen. ■

Rolf Sigg, Senior Software Engineer, Ergon Informatik AG,
rolf.sigg@ergon.ch, www.ergon.ch

Sicherheitslücken bei Bluetooth-Handys

RÜDIGER SELLIN **Einem Bericht zufolge weisen diverse Bluetooth-Handys gefährliche Sicherheitslücken auf. Angreifern sei es möglich, Daten aus Adressverzeichnissen und Kalendern abzuziehen, ohne dass dies auf dem Handy des Opfers angezeigt würde. Adam Laurie, Sicherheitschef des britischen Unternehmens A. L. Digital, veröffentlichte diese Informationen in einem Advisory (http://bluestumbler.org).**

Der Angriff, den Adam Laurie «Snarf-Attack» nennt, soll über Bluetooth-Verbindungen zu anderen Handys aufbauen, ohne dass das Gerät des Opfers etwas anzeigt. Adam Laurie testete nach eigenen Angaben Snarf-Angriffe erfolgreich auf den Modellen T68, T68i und T610 von Sony Ericsson sowie auf Nokias 6310i und 7650 und damit auf den meist verbreiteten Bluetooth-Handys. Zum Schutz vor Snarf-Attacken muss man laut Adam Laurie Bluetooth ganz abschalten. Bei den genannten Nokia-Modellen sieht Adam Laurie ein weiteres Sicherheitsproblem: Der Pairing-Mechanismus ermöglicht das Autorisieren bestimmter Bluetooth-Devices auf Dauer.

Implementierungsfehler

Offenbar gibt es bei Nokia-Geräten einen Implementierungsfehler, der zur Folge haben kann, dass bestimmte Geräte in dieser Liste nicht mehr auftauchen. Trotzdem können sie eine Verbindung herstellen und sogar weitere Verbindungen zu Gegenstellen aufnehmen, die im Handy des Opfers als autorisierte Pairing-Partner eingetragen sind. Dadurch ist es nicht nur möglich, Dateien zu übertragen, sondern auch Internet-, WAP- oder GPRS-Verbindungen auf Kosten des Opfers aufzubauen. Besonders gefährlich findet Adam Laurie die versteckten Einträge in Kombination mit so genanntem «Bluejacking». Bei diesem seit einiger Zeit beliebten Trick kann man auf fremden Bluetooth-Handys direkt eine Nachricht anzeigen lassen. 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 könnte man Nutzer dazu verleiten, mit der erforderlichen Passwortbestätigung die Verbindung zu autorisieren. Damit wären dann alle Daten des Zielgeräts lesbar. Ein Backup des gesamten Datenspeichers wäre möglich. Erscheint das Gerät dann nicht einmal in der Liste der autorisierten Gegenstellen, so kann der fast beliebige Zugriff praktisch unbemerkt erfolgen. Nokia und Sony Ericsson haben diese Sicherheitslücken mittlerweile offiziell bestätigt. Eine Lösung müsse jedoch in der Bluetooth-Standardisierung erarbeitet werden, was mindestens bis Ende 2004 dauern wird. ■

Rüdiger Sellin, Dipl.-Ing., PR-Manager,
Marketing Communications, Swisscom Mobile

Nokias 6310i

Nokias 7650

Sonny Ericsson T68

Sonny Ericsson T610