unsicheres Bluetooth

Beitrag von „Xapathan“ vom 8. Juni 2005 um 08:10

Neue Bluetooth-Angriffsmethode

Forscher an der Ingenieurfakultät der Universität von Tel Aviv , Israel, haben eine Bluetooth-Angriffsmethode entdeckt, die auch bei Geräten mit aktivierten Sicherheitsmaßnahmen funktionieren soll. Sie zeigen, dass die Sicherheitsfunktionen von Bluetooth unzureichend sind.

In sicheren Modus von Bluetooth können zwei (oder mehr) Geräte nur kommunizieren, wenn sie einander bekannt gemacht wurden und einen Verbindungsschlüssel ausgetauscht haben. Bei diesem so genannten Pairing muss der Benutzer auf beiden Geräten eine PIN eingeben. Diese wird verwendet, um den Verbindungschlüssel zu generieren, mit dem dann die weitere Kommunikation verschlüsselt wird. Dadurch sollte das Abhören der Kommunikation nicht mehr möglich sein.

Avishai Wool und Yaniv Shaked haben nun heraus gefunden, wie ein Angreifer diesen Mechanismus aushebeln kann. Sie belauschen die Kommunikation zwischen zwei Bluetooth-Geräten, geben ihr eigenes Gerät als eines der beiden Beteiligten aus, das vorgibt, den Verbindungsschlüssel vergessen zu haben. So erzwingen sie ein erneutes Pairing - ohne Eingabe der PIN.

Der Erfolg der Methode basiert auch darauf, dass meist nur eine vierstellige PIN verwendet wird. Diese können die Forscher auch mit einem relativ alten PC in weniger als einer Sekunde knacken, indem sie alle 10.000 Kombinationen durchprobieren. Sie geben für einen Pentium-III mit 450 MHz eine Zeit von 0,3 Sekunden an, bei einem aktuellen Pentium-IV mit 3 GHz sollen es nur 0,06 Sekunden sein. Mit dem neu ausgehandelten Verbindungsschlüssel kann ein Angreifer nun etwa auf Kosten anderer telefonieren.

Die geringe Reichweite von Bluetooth sollte in der Theorie auch etwas zur Sicherheit beitragen, da ein potenzieller Angreifer recht nahe am Opfer sein müsste. Es hat sich jedoch bereits gezeigt, dass es möglich ist, die Reichweite deutlich zu erhöhen, etwa mit verbesserten Antennen. Erst eine PIN mit 19 oder mehr Stellen kann nach Angaben der israelischen Forscher als relativ sicher vor dem beschriebenen Angriff gelten. So kann die Empfehlung nur lauten,

Bluetooth zu deaktivieren.

Beitrag von „Thomas TDI“ vom 8. Juni 2005 um 09:23

Jetzt wissen wir endlich, warum es sowas in unserem Touareg nicht gibt. Und ich dachte, das hätte nur etwas mit der Anfälligkeit und der schlechteren Sprachqualität zu tun. 

Thomas

Beitrag von „jamesbond“ vom 8. Juni 2005 um 09:47

> Zitat von Xapathan
>
> Neue Bluetooth-Angriffsmethode
>
> Forscher an der Ingenieurfakultät der Universität von Tel Aviv , Israel, haben eine Bluetooth-Angriffsmethode entdeckt, die auch bei Geräten mit aktivierten Sicherheitsmaßnahmen funktionieren soll. Sie zeigen, dass die Sicherheitsfunktionen von Bluetooth unzureichend sind.

Das wird das ewige Spiel bleiben .....

..... Sicherheitsmaßnahmen werden erfunden um von anderen "gehackt" zu werden.

Damit muss man sich als User, der nicht in einem autarken System arbeitet abfinden.

LG
james

Beitrag von „Silberfuchs“ vom 8. Juni 2005 um 10:39

> Zitat von Thomas TDI
>
> Jetzt wissen wir endlich, warum es sowas in unserem Touareg nicht gibt. Und ich dachte, das hätte nur etwas mit der Anfälligkeit und der schlechteren Sprachqualität zu tun.
>
> Thomas

Ach so, wieder was dazugelernt! **Ich** dachte nämlich, es hätte was mit der bekannten Lahmarschigkeit der VW Entwickler und Ingenieure zu tun. So kann man sich irren.

Beitrag von „agroetsch“ vom 8. Juni 2005 um 10:44

Hallo,

also immer schön drauf achten, wenn jemand dicht auffährt. will er vielleicht nur über euer Handy telefonieren

Es gibt ja auch einen "Sport" unter Kiddies, das sog. "Bluejacking". Da werden aber glaube ich primär Handies die ohne aktivierte "Sicherheitsfunktionen" laufen "gejackt"...

Ich habe BT an meinem Handy nur aktiviert wenn ich 'nen Leihwagen fahre und mit dem Hörer im Ohr fühle ich mich ohnehin nicht wohl. Danach mache ich es immer aus, allein schon wegen der Akkulaufzeit!

Beitrag von „Heinz“ vom 8. Juni 2005 um 13:45

> Zitat von Xapathan
>
> Neue Bluetooth-Angriffsmethode
> (...)
> Der Erfolg der Methode basiert auch darauf, dass meist nur eine vierstellige PIN verwendet wird. Diese können die Forscher auch mit einem relativ alten PC in weniger als einer Sekunde knacken, indem sie alle 10.000 Kombinationen durchprobieren. Sie geben für einen Pentium-III mit 450 MHz eine Zeit von 0,3 Sekunden an, bei einem

> aktuellen Pentium-IV mit 3 GHz sollen es nur 0,06 Sekunden sein. Mit dem neu ausgehandelten Verbindungsschlüssel kann ein Angreifer nun etwa auf Kosten anderer telefonieren.
> (...)

´

Sollte die Bluetooth Kommunikation wirklich so dumm sein? Vieleicht?

Es gibt schon seit Jahren Methoden, welche dies leicht verhindern könnten. In unseren entwickelten Systemen wird z.B. eine Verbindung für 15 Minuten geblockt nach 3-maliger Fehleingabe eines Passwortes. Erfolgen nach den 15 Minuten 3 weitere Fehleingaben wird der Account komplett deaktiviert. Das ist eigentlich ganz banal und nichts wirklich weltbewegendes.

Wenn so etwas wirklich nicht in der Bluetooth Kommunikation vorgesehen ist, dann ist das ein Armutszeugnis. In einem stimme ich allerdings uneingeschränkt zu: 4-stellige Pins sind zu kurz. Schon eine Ziffer mehr, wie in vielen anderen Ländern bietet einen zehnfach verbesserten Schutz.

gruß
Heinz

Beitrag von „Xapathan“ vom 8. Juni 2005 um 17:24

Der Autoflüsterer

Auf dem Hacker-Treffen "What The Hack" in den Niederlanden stellte Martin Herfurt von der Trifinite Group neben neuen und bereits bekannten Bluetooth-Schwachstellen auch den "Car Whisperer" (Autoflüsterer) vor. Dabei handelt es sich um ein Programm, mit dem man vorbei fahrende Autos abhören können soll.

Wesentlicher Teil der Abhörmöglichkeit ist die Bluetooth-basierte Freisprecheinrichtung des im Auto installierten Mobiltelefons. Ausgerüstet mit einem Bluetooth-fähigen Notebook, Linux und einer Richtantenne sowie dem Autoflüsterer-Programm soll man sich mit der Freisprecheinrichtung verbinden können.

Nach Angabe von Herfurt benutzen etliche Hersteller statische Zugriffsschlüssel in ihren Produkten. Oft sind diese die einzige Hürde für den Zugriff auf das Gerät. Ist das gelungen, kann man mit den Insassen des Autos Kontakt aufnehmen oder ihre Gespräche belauschen.

Ein Script auf dem Notebook sucht nach Bluetooth-Geräten, die ihrer Kennung nach Headsets oder andere Freisprecheinrichtungen sind. Dann startet das Script die Autoflüsterer-Software, die sich mit dem gefundenen Gerät verbindet. Dabei verwendet es bekannte Standardschlüssel des aus der Gerätekennung ermittelten Herstellers.

Herfurt weist darauf hin, dass nicht alle Bluetooth-Freisprechanlagen für diesen Angriff anfällig sind. Er ruft auch zu verantwortungsvollem Umgang mit dem Car Whisperer auf. Weitere Details finden Sie auf der Website der Trifinite Group .

Beitrag von „Xapathan“ vom 6. August 2005 um 08:30

Bald eine reale Bedrohung: Viren im PKW

Unvermittelt aufplatzende Airbags, versagende Bremsen und nicht mehr anspringende Motoren. All das könnten in Zukunft Viren verursachen, die Ihren PKW infiziert haben. Bluetooth heißt das Einfallstor für die Schädlinge. Die Automobilhersteller haben das Problem erkannt und arbeiten an Schutzmaßnahmen. Und die Hersteller von Schutzsoftware wittern einen Riesenmarkt.

Moderne Zeiten - moderne Gefahren

Sieht so die automobile Zukunft aus? Dass Sie morgens nicht zur Arbeit kommen können, weil sich ihr PKW einen Virus eingefangen hat und deshalb nicht anspringt? Zumindest zerbrechen sich Sicherheitsexperten und Automobilhersteller darüber den Kopf, wie CNN Online berichtet.

Je mehr Hacker und Virenschreiber ihre Aufmerksamkeit Handys und anderen mobilen Geräten zuwenden, desto größer wird die Gefahr, dass moderne Autos zum Opfer von Malware werden. Denn immer mehr PC-Technologie hält Einzug in PKWs, gerade auch zu Komfortzwecken. Die Computer tauschen via Bluetooth Daten mit MP3-Playern und Mobiltelefonen aus - das ist bequem, wenn es darum geht, Lieder, Adressen, Termineinträge und Kartenmaterialien abzugleichen. Aber zugleich öffnet man damit Viren den Zugang zum fahrbaren Untersatz.

Yevgeni Kaspersky von Kaspersky Lab: "Wenn Smartphones und Onboard-Computer die gleichen Kanäle zum Datentransfer benutzen... werden Hacker früher oder später eine Schwachstelle im Betriebssystem des Onboard-Computers finden – und ausnutzen." Damit könnten Angreifer im schlimmsten Fall die Motorleistung und das Abgasverhalten beeinflussen oder das Navigationssystem deaktivieren. Eine kuriose Vorstellung: Ihr nagelneues Auto besteht die Abgassonderuntersuchung (ASU) nicht, weil ein Hacker das Mischungsverhältnis

ihres Motors manipuliert hat. Ganz zu schweigen von dem Horrorszenario, wenn Sie mit 160 Stundenkilometer über die Autobahn knattern, während ein Hacker die Bremsanlage ihres Fahrzeuges abschaltet. Im Vergleich dazu erscheint das mechanische Durchschneiden der Bremsleitungen geradezu altertümlich...

Selbst wenn durch eine solche Attacke auf Ihre Fahrzeugelektronik kein Unfall verursacht wird, haben Sie jede Menge Ärger und müssen die Werkstatt aufsuchen.

Ein Gewinner steht jedoch bereits fest: Die Hersteller von Antivirensoftware. Auf sie wartet ein neuer Riesenmarkt. Die Marktforscher von IDC sagen voraus, dass der Markt für Schutzsoftware für tragbare Geräte wie Handys und PDAs auf 993 Millionen Dollar im Jahr 2008 wachsen wird. 2003 betrug der Umsatz gerade einmal 70 Millionen.

Beitrag von „agroetsch“ vom 6. August 2005 um 23:17

Na da soll einer noch mal heulen wegen nicht vorhandenem Bluetooth im Dicken.

Ich vermisse es eigentlich nicht, mir sind "verdrahtete" Lösungen oft lieber, habe ich ja schon mehrfach geschrieben.

Auch wenn solche Berichte zum Teil schon Panikmache sind, ganz von der Hand zu weisen ist es sicher nicht. Kabellos ist nun mal in!

Beitrag von „collideous“ vom 7. August 2005 um 07:31

> Zitat von Xapathan
>
> Der Autoflüsterer
>
> Auf dem Hacker-Treffen "What The Hack" in den Niederlanden stellte Martin Herfurt von der Trifinite Group neben neuen und bereits bekannten Bluetooth-Schwachstellen auch den "Car Whisperer" (Autoflüsterer) vor. Dabei handelt es sich um ein Programm, mit dem man vorbei fahrende Autos abhören können soll...

Wer sich in einem Café an einen Tisch niedersetzt oder im Supermarkt Schlange steht hat Idioten vor, hinter und neben sich, die lautstark ins Handy quatschen. Wer will sich da noch zusätzlich mit einem "Car Whisperer" quälen, und das sinnlose Palaver dahindüsender

Automobilisten abzuhören? Also ich kann mir nichts langweiligeres vorstellen.

Beitrag von „Xapathan“ vom 7. August 2005 um 09:04

> Zitat von collideous
>
> Wer will sich da noch zusätzlich mit einem "Car Whisperer" quälen, und das sinnlose Palaver dahindüsender Automobilisten abzuhören? Also ich kann mir nichts langweiligeres vorstellen.

Es ging darum, die Aufmerksamkeit für ein "offenes Scheunentor" in das System zu wecken. Hoffentlich werden die Autohersteller früh genug Schutzmassnahmen ergreifen. Sonst steuert ein Virus wirklich einmal Funktionen in Deinem Auto...

Das Abhören von Telefonaten passiert anders, ist aber für uns Normalbürger nicht interessant da stimme ich 100% zu.