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.