unsicheres Bluetooth

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