

Re: bluetooth pin-cracker

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2003-11/0066.html>

From: Jimi Thompson (jimit_at_myrealbox.com)

Date: 11/15/03

Date: Sat, 15 Nov 2003 12:44:38 -0600

To: <pen-test@securityfocus.com>

All,

Bluetooth is not my area of specialty, but I have a question regarding this. Rather than crack the key to try to either hijack the session or intercept the data, why not try to just get the data that you want by other means? How difficult would it be to get your "malicious" device to authenticate to another user's equipment? I'm referring to the possibility of walking up to someone on a commuter train and using Bluetooth to steal their electronic address book, say from their cell phone.

Thanks,

Jimi

At 10:18 PM +0000 11/10/03, Chris McNab wrote:

>Hi,

>

>> *does anybody know a tool, which can brute force cracking the pin (4-6*

>*digests), which*

>> *is needed for a connection to bluetooth device?*

>

>*The PIN is used when pairing two Bluetooth devices, and is combined on both*
>*devices along with a 128-bit pseudo-random number, and the 48-bit Bluetooth*
>*address of one of the devices, to generate the initialization key which is*
>*used to authenticate, and protect link keys used for encryption and*
>*decryption traffic on both devices.*

>

>*The PIN is the effectively shared secret which protects the initialization*
>*key in the pairing process, and is only used once during that pairing*
>*process.*

>

>*With this in mind, you can't perform an active brute force attack to*
>*compromise a pair of Bluetooth devices. The only easy way to remotely*
>*compromise the traffic between two Bluetooth devices, is to sniff the*
>*pairing between two devices, and attack the PIN number to compromise the*
>*link key - then you can decrypt all that traffic easily.*

SecurityFocus Penetration: Re: bluetooth pin-cracker

>
>*Two direct attacks against the Bluetooth E0 cipher are known, but of*
>*significant complexity (2^{66} and 2^{100}), and published by Jakobsson and*
>*Wetzel at <http://citeseer.nj.nec.com/jakobsson01security.html>.*
>
>*My point is, if you haven't sniffed the pairing process, you will have a*
>*very hard time compromising the initialization key.*
>
>*Regards,*
>
>*Chris*
>
>*Chris McNab*
>*Technical Director*
>
>*Matta*
>*18 Noel Street*
>*London W1F 8GN*
>
>*<http://www.trustmatta.com>*
>
>
>
>-----
>*Network with over 10,000 of the brightest minds in information security*
>*at the largest, most highly-anticipated industry event of the year.*
>*Don't miss RSA Conference 2004! Choose from over 200 class sessions and*
>*see demos from more than 250 industry vendors. If your job touches*
>*security, you need to be here. Learn more or register at*
>*http://www.securityfocus.com/sponsor/RSA_pen-test_031023*
>*and use priority code SF4.*
>-----

Network with over 10,000 of the brightest minds in information security
at the largest, most highly-anticipated industry event of the year.
Don't miss RSA Conference 2004! Choose from over 200 class sessions and
see demos from more than 250 industry vendors. If your job touches
security, you need to be here. Learn more or register at
http://www.securityfocus.com/sponsor/RSA_pen-test_031023
and use priority code SF4.
