

RE: Dumb question abt. Wireless WEP security

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2004-01/0280.html>

From: Rosenhan, David (*David.Rosenhan_at_swiftbrands.com*)

Date: 01/20/04

Date: Tue, 20 Jan 2004 15:06:49 -0700

To: <jburzenski@americanhm.com>

There are new ways to help you make your wireless connection even more difficult to crack if you have Cisco Equipment (PCMCIA & PCI cards with 340-1200 AP's and 350-up bridges) I am not trying to sell Cisco, but if you have it already then you can use TKIP (temporal key integrity protocol) MIC (Message integrity Check) and if you have ACS you can do leap, leap is also supported in other security server software and will work with Cisco equipment.

TKIP hashes the key at an interval you choose (300 seconds usually), MIC swaps 2 bits in the packet and ACS with LEAP will basically do the same thing as TKIP except the server determines the hashed WEP key.

> *Hi all,*

>

> *There seems a general understanding that WEP is not secure*

> *enough, because theoretically WEP encryption can be broken.*

>

> *The question is about the practical usage; how easy it is for*

> *WEP to be broken?*

The rate at which WEP can be broken using traditional methods depends on the amount of traffic that is generated by the wireless network. In my experience a typical network will take at least 3 days to crack with the average looking more like 7-10 days. This is using tools such as Kismet / Aircrack / wepcrack.

To attempt to answer your first question below, I haven't run into a WEP protected network that could be cracked in less than an hour (or a day for that matter).

> *Does it suffice to sniff the wireless network for one hour,*

> *or do we need to sniff for few days? What happens if the*

> *wireless network is periodically*

> *stopped let's say every 10 hours for 15 minutes,*

Periodically stopping the wireless network (ie. Killing the power) every day for a few minutes won't make a whole lot of difference to a cracker.

SecurityFocus BASICS: RE: Dumb question abt. Wireless WEP security

Unless you change your keys or something, the cracking process will pick up right where it left off.

If you can leave your network off for hours at a time (when the business is closed or when the lights are turned off) you will be better protected from the casual war-driver because your network will be undetectable while it is powered off.

Speaking practically, turning off your network to protect your WEP keys doesn't really make a whole lot of sense. There are two types of hackers coming after your wireless network, casual and determined.

The casual hacker will most likely keep on driving because chances are there are 10-12 unsecured, clear text wireless networks with out of the box configuration settings setup with 3 miles of where you are.

The determined hacker who has patience and accessibility to your wireless signal will break your WEP and will sniff your traffic which is why it is imperative to not rely solely on WEP for protection of your data.

>
> *Regards,*
>
> *Veli I. Cigirgan*
> *Vizo Bilisim Sistemleri Ltd.*
> *Istanbul*
> *Tel:+90(212)210 2657*
> *Fax:+90(212)210 3678*
>

David Rosenhan, CCNP
Information Technology
Swift & Company
1770 Promontory Circle
Greeley, CO 80634
970-506-8045

Ethical Hacking at InfoSec Institute. Mention this ad and get \$720 off any course! All of our class sizes are guaranteed to be 10 students or less. We provide Ethical Hacking, Advanced Ethical Hacking, Intrusion Prevention, and many other technical hands on courses. Visit us at <http://www.infosecinstitute.com/securityfocus> to get \$720 off any course!
