

Re: Intrusion possible?

Source: <http://newsgroups.derkeiler.com/Archive/Alt/alt.internet.wireless/2005-09/msg01015.html>

- *From:* Jeff Liebermann <jeffl@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Thu, 29 Sep 2005 09:34:09 -0700
-

On Thu, 29 Sep 2005 09:17:47 +0200, Sander <Big_Scary_Man@xxxxxxxxxxxxx> wrote:

>Jeff Liebermann wrote:

>

>> Useless. WEP64 can be cracked in about 15 minutes of sniffing.

>

>Before you can sniff traffic there has to be traffic.

Agreed.

>If a network is not in active use you'll have to wait until a client >associates before you can actively attack that network.

Yep. I leave my laptop running in my vehicle sniffing away merrily. I was more interested in traffic and use patterns than in cracking WEP keys, but the methodology is the same. 8 hours later, I usually have enough traffic captured to crack many networks. My client is setup like a radio scanner. It listens on a channel for traffic. When the traffic stops, it move on to the next channel.

My all time record was about 2 years ago. My car was facing a large office building, where I captured about 4 gigabytes of traffic during the workday. I was able to later crack about 30 WEP keys out of about 40 encrypted SSID's heard. A few were trivial. Just crunching the mess after doing the capture took most of the next day. I had to crunch it several times because there was one system that had 4 SSID's associated with a single MAC address. Drove me nuts until I figured out what was happening.

WPA had just been released in early 2003, so none of the networks I sniffed were using WPA. However, I'm not sure as the RC4 encrypted payloads for WEP and WPA are identical. Only the key exchange is different.

The traffic patterns showed serious problems. About 25% of all packets heard were retransmissions implying lots of reflections and interference. A full 50% of the packets heard were "malformed" which is a nice term for a collision. I discarded these. A few systems

Re: Intrusion possible?

were operating at 1 and 2 mbits/sec which also indicates substantial co-channel interference. One system had about 1/3 of their traffic wasted as ARP requests, DNS lookups, and repetitive broadcasts, which indicates a screwed up network. I found zero indication of any VPN's in use, but may have missed them some under the packets I couldn't sniff or decrypt. There was a considerable amount of UDP traffic which implies streaming content. That could be VoIP, but is more likely to be watching movies or listening to music at work. There was some worm that had just been released and there was plenty of ICMP probes flying around.

I should do this again to see how things have changed.

>If you can

>capture the date of a client associating you have the tools to do the
>rest quickly and no other traffic is necessary. You can generate it
>yourself. But you do need that traffic first so you can replay it.

Agreed.

—

Jeff Liebermann jeffl@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx
150 Felker St #D <http://www.LearnByDestroying.com>
Santa Cruz CA 95060 <http://802.11junk.com>
Skype: JeffLiebermann AE6KS 831-336-2558
.

• **References:**

- ◆ ***Intrusion possible?***
 ◇ *From:* Tardus_merula
- ◆ ***Re: Intrusion possible?***
 ◇ *From:* Jeff Liebermann
- ◆ ***Re: Intrusion possible?***
 ◇ *From:* Sander

- Prev by Date: ***Re: Looking for wireless video web server***
- Next by Date: ***Re: Intrusion possible?***
- Previous by thread: ***Re: Intrusion possible?***
- Next by thread: ***Re: Intrusion possible?***
- Index(es):
 - ◆ ***Date***
 - ◆ ***Thread***