Trustwave®

SpiderLabs℠

THOTCON 0x1: War Driving 4 Warehouses

Rob Havelt – Director, Penetration testing

Trustwave SpiderLabs

Greetings THOTCON 0x1

Introductions

Rob Havelt

rhavelt@trustwave.com

- I'm from Trustwave SpiderLabs – I manage the Penetration Testing Practice
- I like to take things apart
- Also Scotch, Godzilla, and the whole Danish vampire movie genre
- If pressed I could probably name at least 5 zombie moves shot in Portugal in the 70's

Trustwave®

SpiderLabs℠

FHSS in 300 seconds – a Quick Overview

802.11 FHSS Overview

- Defined in the 1997 and 1999 ANSI/IEEE standard for 802.11
- Speeds of 1 or 2 Mbit/s utilizing 2 Level or 4 Level Gaussian Frequency Shift Keying (GFSK) modulation respectively.
- Higher layer functions are pretty much the same as other 802.11 standards (b/a/n/g)
- Believed to be more secure than b/a/n/g because of a general misunderstanding of the PHY (which is the only thing different). Once we understand that, these are just super unsecured WiFi networks.

So Why Do We Care?

- A good point – this is old tech. About 11 years old now.
- Still pretty widely used in warehouse applications, and other applications. Large manufacturers, retailers, and others still use this tech. (and I can prove it!)
- Moreover, many times, and in many places where this is implemented it is implemented in a very fun way (for an attacker).

Bad Advice…

Security professionals make horrible decisions and give bad advice about this technology!

IT MAY BE OUTRIGHT FALSE:

Using technology alone … it is not possible to obtain the ESSID of the Frequency Hopping Spread Spectrum network.

-A Prominent Pen Test Firm in a Wireless Pen Test Report

IT MAY BE UTTERLY MEANINGLESS:

Unlike the CCK modulation mode of the more common 802.11b which offers a promiscuous, residual engineering, "monitor" mode, where raw wireless traffic can be sniffed, FHSS uses binary GFSK, which has no such mode available for promiscuously sniffing traffic from specific channels or hop sequences

-More "Great" Advice

802.11 FHSS Security and Architecture

- When talking about these networks – security is nearly nonexistent – what little there is is truly a blast from the past.
  - IEEE/ANSI Standard 802.11 1999 Edition defines
    - MAC Address Filtering
    - 40 Bit WEP
- However most implementations rely on "the perception of invisibility" for security. That is to say the fact that an attacker cannot find the SSID of their otherwise open network.
- Architecture can be problematic – most FHSS AP's are implemented as simple Wireless to wired bridges. There is little if any access control between the wireless and wired side, most of the time – no firewall, no built-in firewall on the AP.

Trustwave®

SpiderLabs℠

Taking Advantage – LET'S GO WARDRIVE

What Do We need?

I'm glad you asked – I have most of the parts right here.

- USRP / GNU Radio / Tunnel Interface / Packet Sniffer / WiFi Tool

Then maybe one of these

- Symbol LA-3020-500

What are we hunting?

- Symbol AP-3020-500(or 100)
- Here's some Symbol IP phones!

War Drive 4 Warehouses?

SHOW AND TELL

Trustwave®

SpiderLabs℠

Now the Fun Stuff

What's Out There?

My admittedly unscientific study was a bit telling for me at least:

- To test this theory I picked about 15 locations in WI and IL, Zoned for Heavy Industrial/ Office/ Warehouse (i.e. industrial/office parks)
- Out of 15 areas chosen I found these networks in 12 of them
- In 2 Industrial parks in Milwaukee I found these networks in over 5 different businesses in the same park!
- The top business using these were RETAILERS, next were MANUFACTURING.