Yes it is Too WiFi, and No It's Not Inherently Secure

Rob Havelt
Black Hat Europe, 2009

Greetings Black Hat

Rob Havelt
rhavelt@trustwave.com

I’m from Trustwave’s SpiderLabs – I manage the Pen Test Practice in the US.

I like to take things apart.

Also, Scotch and Godzilla

What is This All About?

- A discussion of legacy Frequency Hopping Spread Spectrum 802.11 Networks

- In “802.11 Wireless Networks: The Definitive Guide” by Mathew Gast it is said: “*At this point the FH PHY is largely a footnote in the history of 802.11, so you may want to skip this chapter…*”

- However, we can still find some relevance in the topic since there are still a great many legacy deployments.

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.

Why Do We Even Care?

- A good point – this is old tech.

- Still pretty widely used in warehouse applications, and other applications. Large manufacturers, retailers, and others still use this tech.

- Moreover, many times, and in many places where this is implemented it is implemented in a very fun way (for an attacker).

Why Do We Even Care?

Why Do We Even Care?

Bad Advice

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

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

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

Bad Implementation

- Typical Warehouse Scenario:

  Most AP's just implemented as a Wireless Bridge

  Wireless Clients have unrestricted access to wire side

  WAN connection back to corporate location

WHY?

Because legacy implementations have been there since the 90's or very early 2000's before many best practices were defined. The equipment itself supports a very limited feature set and can't be upgraded.

A Brief FHSS Interlude

- Historically FHSS was in fact designed as a security protocol… of course, this was *during World War II*

- Typically (as useable channels are regulated by country) these networks use one of 78 different hop sequences (defined in the ANSI/IEEE 802.11 standard) to hop to a new 1MHz channel (out of a total of 79 channels) approx. every 400 milliseconds.

- Due to the nature of the FHSS PHY it is greatly resistant to any narrow band interference and narrow band jamming. On the downside, one of the limitations for FHSS was transmission speed.

What's The Difference?

- Those not so well versed with technology history may wonder what the difference is between 802.11 FHSS and more modern stuff like 802.11 b/a/n/g

- Only the PHY and some of how the PHY supports MAC. The rest of layer 2 is the same – transport independent.

- That means we still have the exact same type of management frames such as Beacon, Associate, Probe, Probe Response

802.11 FHSS Security

- Security 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.

Start at the Top

To describe an attack - Let's start at the top and work our way down…

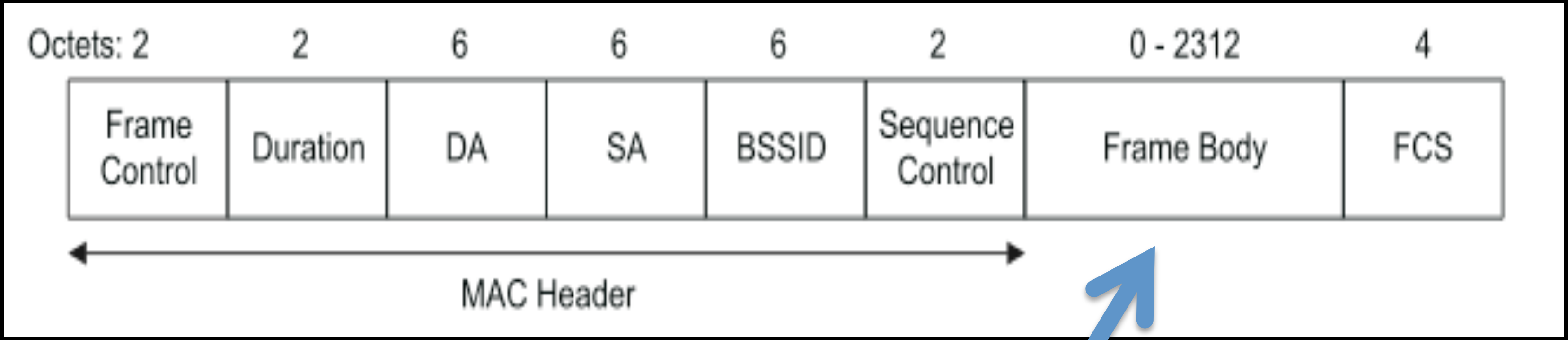
- What is the one thing we need to know to join an FHSS network and where might we find that?

- There are only 3 possible things:
    - SSID
    - Maybe a MAC address of an authorized client
    - Maybe a 40 bit WEP key

However, most time all you need is an SSID

Where is the SSID?

- Management Frames!



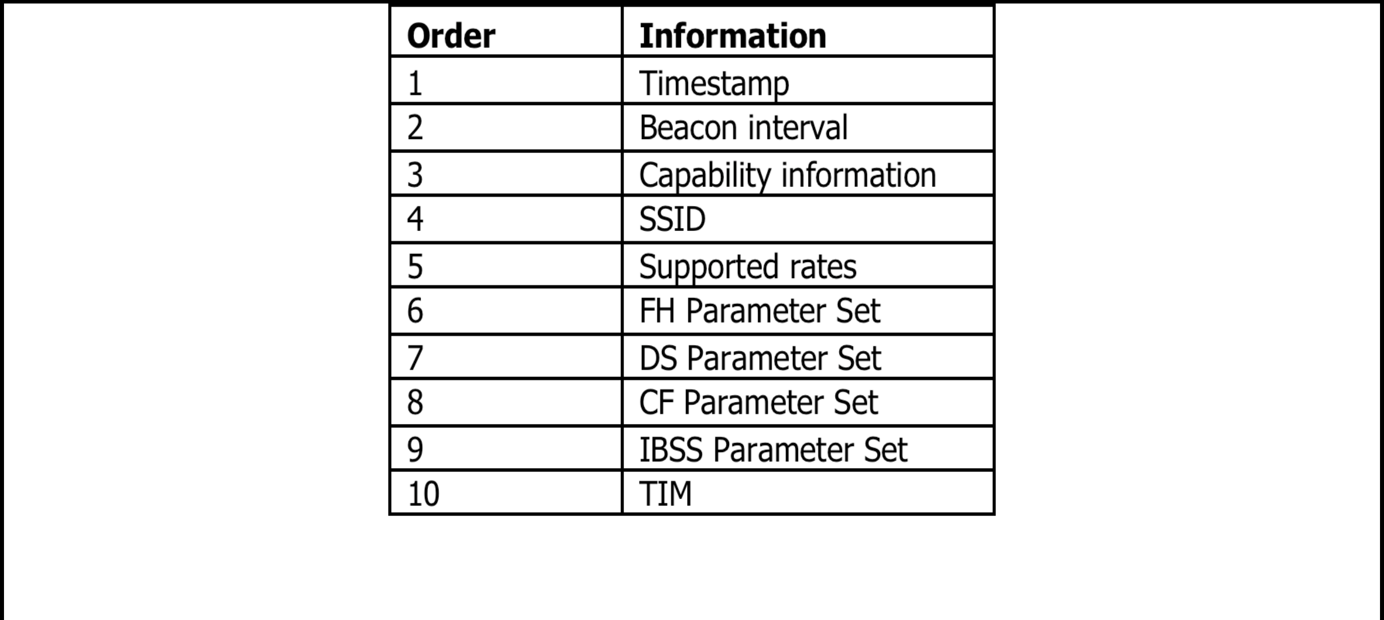
Octets: 2	2	6	6	6	2	0 - 2312	4
Frame Control	Duration	DA	SA	BSSID	Sequence Control	Frame Body	FCS

MAC Header

Right here in the frame body!

A Beacon Frame

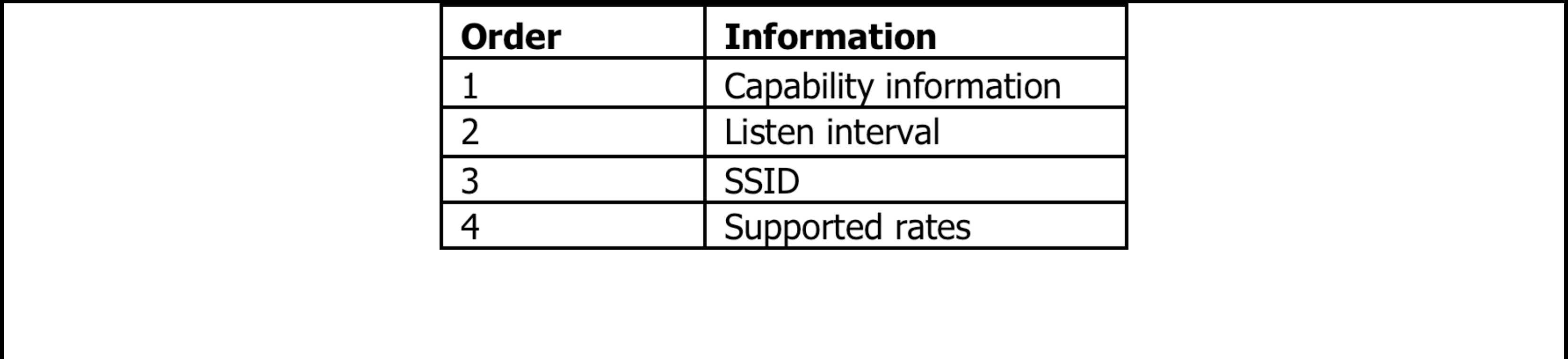
- The Frame Body looks like this:



Order	Information
1	Timestamp
2	Beacon interval
3	Capability information
4	SSID
5	Supported rates
6	FH Parameter Set
7	DS Parameter Set
8	CF Parameter Set
9	IBSS Parameter Set
10	TIM

An Association Request

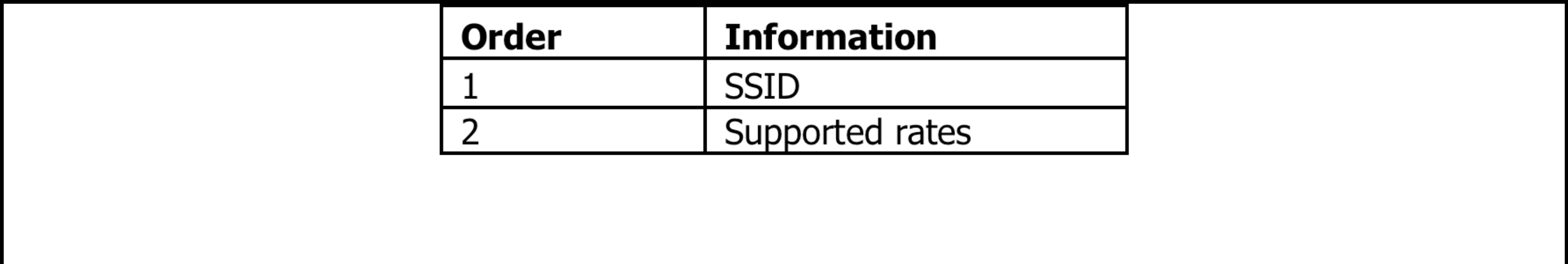
- The Frame Body looks like this:



Order	Information
1	Capability information
2	Listen interval
3	SSID
4	Supported rates

A Probe Request

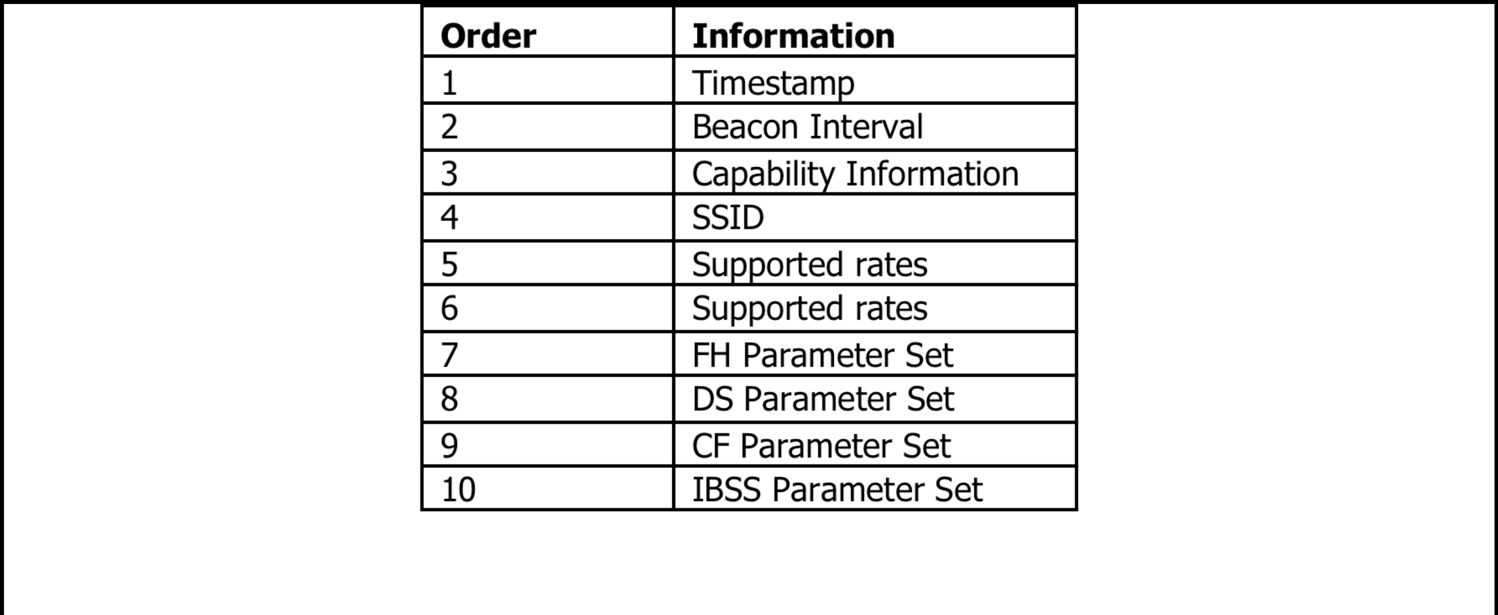
- The Frame Body looks like this:



Order	Information
1	SSID
2	Supported rates

A Probe Response

- The Frame Body looks like this:



Order	Information
1	Timestamp
2	Beacon Interval
3	Capability Information
4	SSID
5	Supported rates
6	Supported rates
7	FH Parameter Set
8	DS Parameter Set
9	CF Parameter Set
10	IBSS Parameter Set

So How Do We Find Them?

- The FHSS network is stealthy and invisible right? We can’t sniff those over the air, so they might as well be inside on a private wire, right?

- There’s always been ways – the equipment has been expensive, possibly illegal to own, or very proprietary to a manufacturer… (things like protocol analyzers, manufacturer test equipment, etc.) – even given the expense it might not do exactly what we want anyway…

- Enter Software Radio (GNURadio) and cool stuff like the USRP (or USRP2)

But Wait a Second…

- Its not all kittens juggling bunnies, ice cream, and picnics with nana from there…

- We still need to know stuff about the PHY to define it in Software Radio.

- Namely, we need to know things about data rates, modulation, structure, whitening (scrambling), transmission, etc.

- You will see how very, very similar to Bluetooth this all is…

Frequency Hopping

- Operates in part of the microwave ISM band (2.400 GHz – 2.495 GHz

1 MHz wide

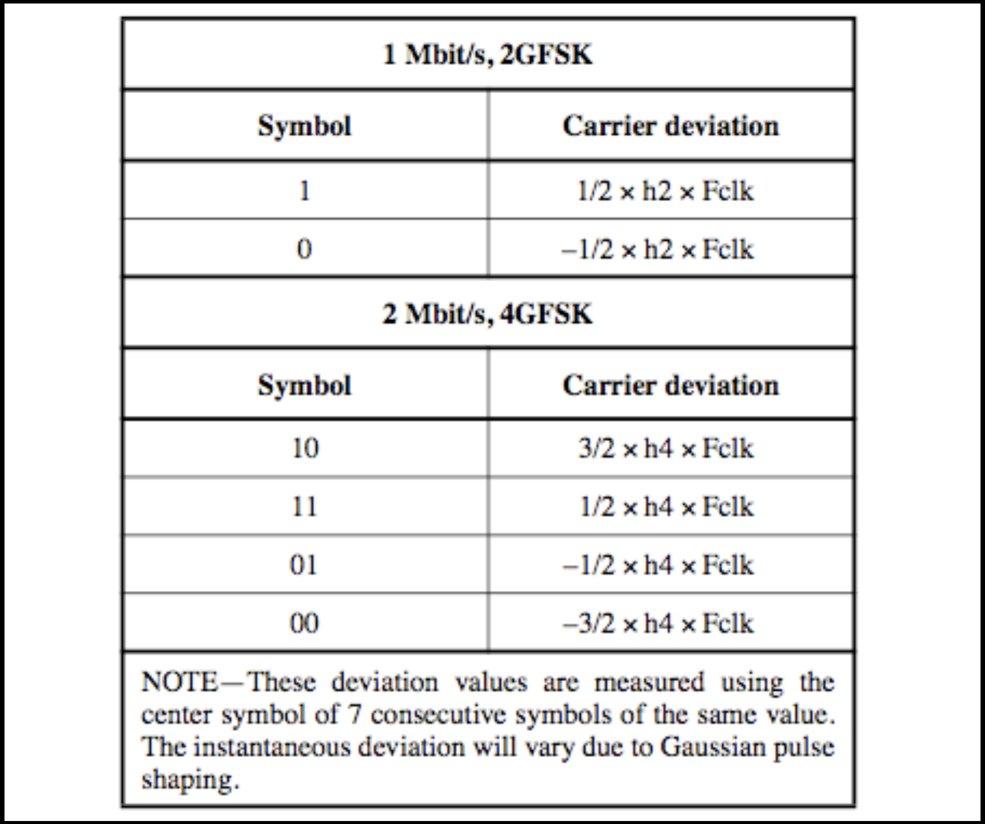
Channel	Frequency
2	2.402 GHz
3	2.403 GHz
…	…
79	2.479 GHz

Both ETSI in Europe and FCC in the US allow channels 2-79 to be used

Dwell time on a Channel is approx. 400 milliseconds

Modulation

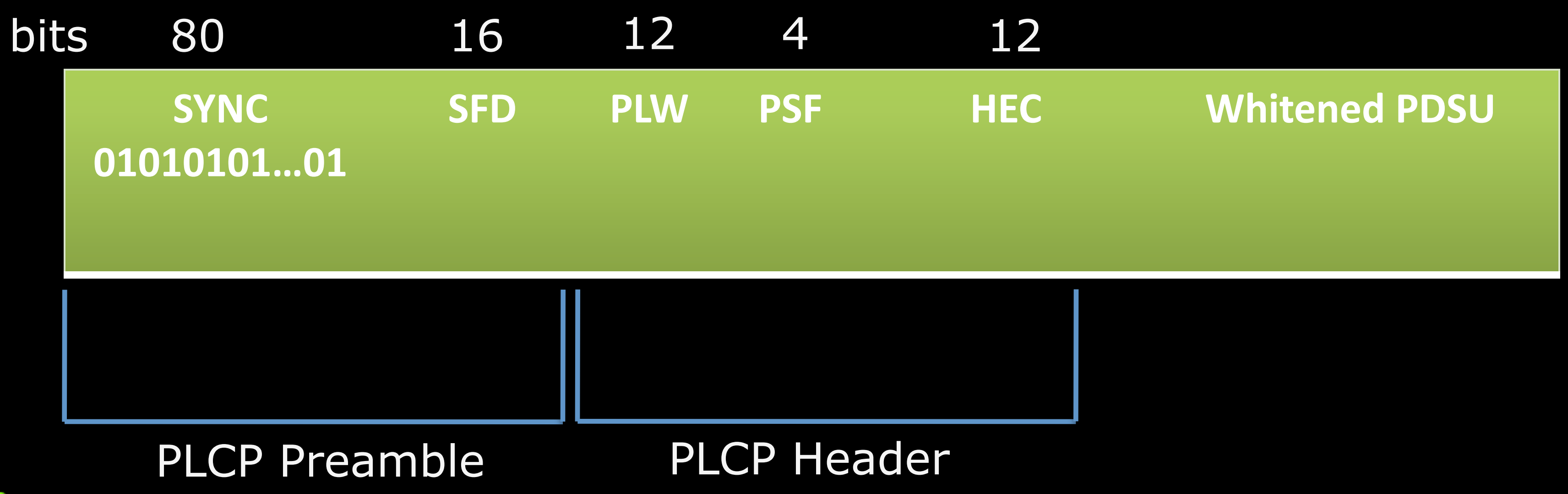
- Uses 2 Level or 4 Level GFSK Modulation - 2 level encodes 1 bit per symbol – 4 level encodes 2 bits per symbol and thus doubles the data rate.



1 Mbit/s, 2GFSK	
Symbol	**Carrier deviation**
1	1/2 × h2 × Fclk
0	–1/2 × h2 × Fclk
2 Mbit/s, 4GFSK	
Symbol	**Carrier deviation**
10	3/2 × h4 × Fclk
11	1/2 × h4 × Fclk
01	–1/2 × h4 × Fclk
00	–3/2 × h4 × Fclk
NOTE—These deviation values are measured using the center symbol of 7 consecutive symbols of the same value. The instantaneous deviation will vary due to Gaussian pulse shaping.	

Source: ANSI/IEEE Std 802.11, 1999 Edition

Framing



bits	80	16	12	4	12	
	SYNC 01010101…01	SFD	PLW	PSF	HEC	Whitened PDSU

PLCP – Physical Later Convergence Protocol
SFD – 16 bit pattern of: 0000 1100 1011 1101
PLW – informs the receiver of the length of the MAC frame
PSF - encodes the speed (either 1 or 2 Mbit/s – 000 or 010)
HEC – 16 bit CRC Checksum

Whitening

- The PDSU is Whitened (scrambled).

- The PLCP data whitener uses a length-127 frame-synchronous scrambler followed by a 32/33 bias-suppression encoding to randomize the data and to minimize the data DC bias and maximum run lengths. Data octets are placed in the transmit serial bit stream LSB first and MSB last.

- The same scrambler is used to scramble transmit data and to descramble receive data.

Very Similar to Bluetooth

- Everything about this is very similar to Bluetooth (Modulation, Hop patterns, etc.)

- In 2007 Dominic Spill and Andrea Bittau publish “BlueSniff: Eve meets Alice and Bluetooth” more recently Dominic Spill and Michael Ossman expand the concept further with: “Building an All Channel Bluetooth Monitor”

- The project can be found here: http://gr-bluetooth.sf.net

- The Bluetooth ideas and methods can be directly applied here.

- Only 802.11 FHSS is much, much easier…

Attacking the Networks

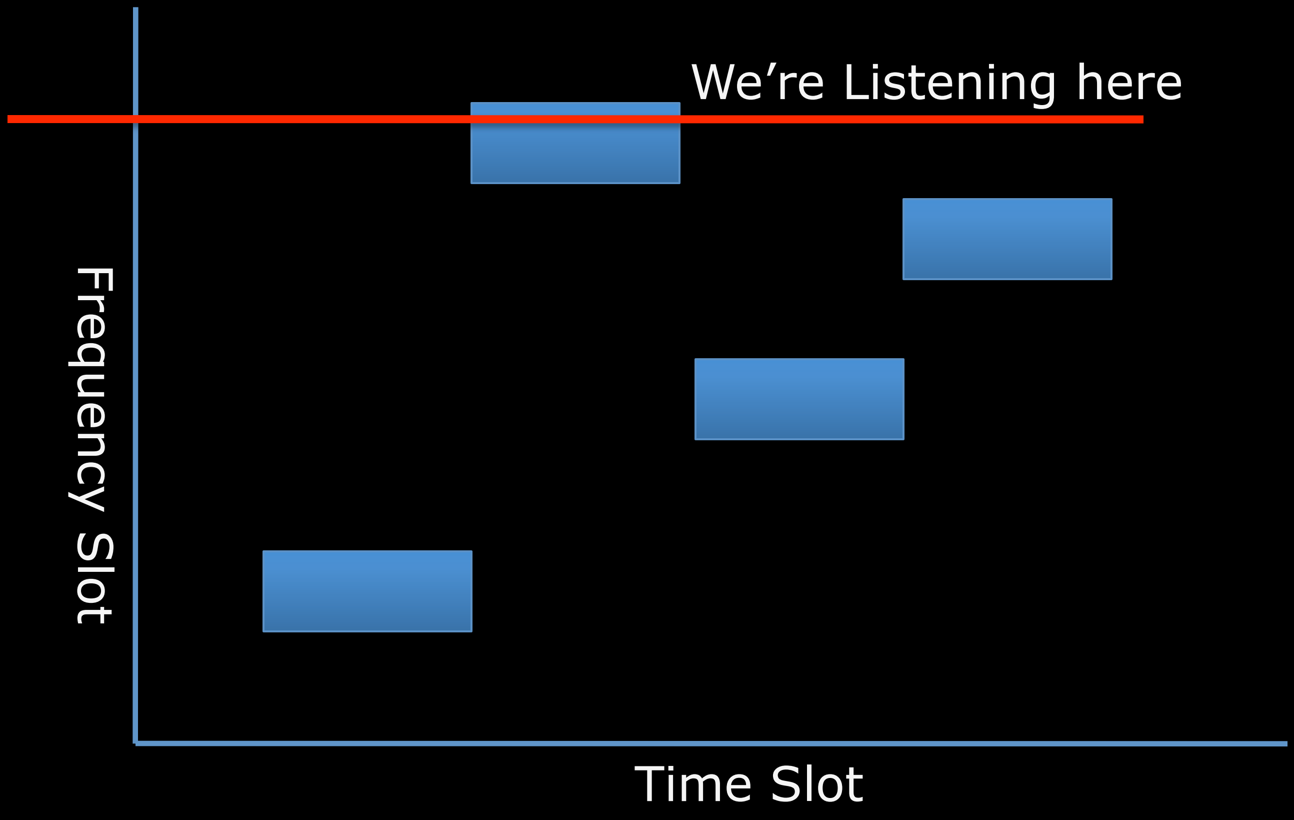
- So don't you either need to know the hop pattern to sniff (which you can't know unless you sniff) or listen in on all 79 channels?

- NO! No you do not…

- We need such a tiny bit of info from the network in order to connect, it really is sufficient to simply use Software radio to listen in on a single fixed channel, or a few fixed channels and wait for the network to hop by.

- Very soon we will have a management frame.

Attacking the Networks



Attacking the Networks

- If w D
info, r
conne

- Now
correc

- If w et
those
space
packe

Some Further Reading

GNU Radio – http://www.gnuradio.org

The USRP – http://www.ettus.com

BBN ADROIT (802.11 code for GNU Radio) - https://acert.ir.bbn.com/projects/adroitgrdevel/

GNU Radio Bluetooth project - http://gr-bluetooth.sf.net