Trustwave®
Information Security & Compliance

Yes it is too Wi-Fi, and No its not Inherently Secure

Rob Havelt

March 27, 2009

A Whitepaper for Black Hat Europe 2009

Table of Contents

List of Tables

1 Introduction

802.11 wireless network devices come in many flavors. The earliest 802.11 physical layer (PHY) service specifications detail three different physical layer types for wireless LAN media. Those are:

- Direct sequence spread spectrum (DSSS) for the 2.4 GHz ISM band
- Infrared (IR) near-visible light in the 850 to 950 nm range
- Frequency hopping spread spectrum (FHSS) for the 2.4 GHz ISM band

The focus of this paper are those 802.11 wireless LAN's that utilize FHSS for the 2.4 GHz ISM band. The purpose of this paper is to familiarize the reader with the mechanics of these FHSS based networks; provide background as to historical and modern usage of these networks, provide some insight as to the common architecture of these networks in the overall infrastructure of many organizations, present some of the common misconceptions regarding the inherent security of these networks, and finally to highlight some of the issues of "security through obscurity" by positing a practical attack scenario against these networks.

1.1 History

Historically FHSS was in fact designed as a security protocol during World War II, as a secret communications system that could guide torpedoes to their target without being intercepted by the enemy. The idea to send radio signals from transmitter to receiver over multiple frequencies in a random pattern was originally patented by movie actress Hedy Lamarr and composer George Antheil. This was actually accomplished by outfitting the sender and receiver with identical paper rolls perforated with a pseudo-random pattern utilizing 88 different frequencies.

FHSS in the context of wireless networking PHY is not much different. 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) every 400 milliseconds. Synchronization info is sent between access points (AP) and stations (STA) or between STA in an Ad-Hoc situation in certain management frames such as beacon frames and probe responses, which contain an FH Parameter Set element that contains all parameters necessary for transmitter and receiver to stay in synchronization (Dwell Time, Hop Set, Hop Pattern, Hop Index).

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. Rules imposed by the FCC in the USA limit channel width to 1MHz, which greatly limits the number of signal transitions that can be used to encode data. With a straightforward two level encoding, each cycle can encode one bit; at this rate 1MHz equates to a data rate of approximately 1 Mbps. This can be improved upon with doubling the symbol encoding for a data rate of 2 Mbps.

In the original 802.11 specifications the DHSS PHY also had speeds of 1 and 2 Mbps but it was clear that this PHY had the potential for much higher speeds than frequency hopping technologies and handily became the PHY of choice. At this point however, many organizations had already made a significant investment in 802.11 LAN infrastructure based on FHSS. Therefore as DHSS and other PHY strategies went on to ubiquitous usage and wide scale dissemination FHSS lingered as "the legacy wireless network".

1.2 FHSS Today

Since the publication of the original ANSI/IEEE 802.11 standard there have been many additions and new standards defining other Wireless LAN technologies based on DSSS and other physical layer strategies. FHSS with its modest data rates rapidly fell out of favor. One would be hard pressed to see a brand new implantation of a wireless LAN based on the FHSS PHY today in 2009. However, many organizations, even very large organizations, adopted the technology when it was in favor, and still maintain large deployments of 802.11 FHSS today. Many of these deployments can be found among large retailers and manufacturers (specifically in their warehouse facilities) and are typically used for applications such as wireless barcode scanners, wireless printers, and wireless IP phones. The most prolific brand of 802.11 LAN technology based on the FHSS PHY is Symbol Spectrum24 equipment, but also you can find RangeLAN2, and Proxim AP and STA equipment.

There are many potential reasons for these legacy networks to still be maintained and utilized these are:

- **For many, FHSS is seen as a security feature, and the conventional thinking is that these networks are hidden from attackers and robust against eavesdropping.**
- The initial deployment of these networks was a significant investment, and they still serve their primary purpose well.
- It would be another significant investment to update these networks and there is not a clear gain from increased features and/or speed.
- Due to the first assumption, updating these networks to other technologies would require an additional security investment and network architecture to increase segmentation and access control (additional routing hops, firewalls, IPS, NAC, etc.)

Many of these reasons are built on the faulty first premise that **FHSS is a security feature**. Whereas that might have been true during World War II, and even in earlier days of 802.11 FHSS, it can only be described as simple security though obscurity.

There was a time when any attack against any wireless LAN PHY strategy was thought to be impractical because gaining access to the PHY layer and eavesdropping on network communications in any Spread Spectrum scheme was seen as the domain of radio geeks with multiple thousands of dollars of equipment at their disposal. However as of this writing it would be seen as sheer gross negligence to operate a completely open 802.11b, 802.11g, or 802.11n network especially one that had direct access to sensitive corporate assets with no form of

access control. However right now, today, there are literally hundreds of organizations doing just that with 802.11 FHSS networks.

In the 2002 paper "Intercepting Mobile Communications: The Insecurity of 802.11" Boristov, Goldberg, and Wagner warn: "As such, there might be temptation to dismiss attacks requiring link-layer access as impractical; for instance, this was once established practice among the cellular industry. However, such a position is dangerous."

1.3 Security Implications

As was touched upon in the previous section, the most dire security implications for 802.11 FHSS network implementations stem from the belief that FHSS is a security feature and that eavesdropping in these environments to gain even the most basic information (such as single beacon, client probe, probe response or other management frames) is well beyond the capabilities of the average attacker. This could not be further from the truth.

Sadly the belief in the inherent security of these types of networks leads to poor decisions about architecture and access control. I've even seen this position validated by security consultants who have posited outright fallacies such as:

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

And where outright fallacies were not used, highly misleading statements such as the following were issued:

```
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
```

Which is technically accurate but completely irrelevant and highly misleading.

With the "FHSS is a security feature" myth being perpetuated by so-called security professionals and penetration testers, what chance does the average organization have to truly understand the exposure and the risk they are accepting?

2 802.11 FHSS LAN Details

To understand the security implications of an 802.11 FHSS LAN, it is very useful to understand some technical details of how they function. Whereas this information is generally available, the information tends to be scattered piecemeal across multiple sources.

2.1 Common Architecture and Implementation

As was previously mentioned, due to the belief that FHSS is a security feature in an 802.11 FHSS LAN, most implementations of this network type do not make use of basic security features or secure architecture. One thing to remember is that many of these deployments were implemented before many of the warnings regarding secure architecture for wireless networks. As such many of these Wireless LANS are simply an extension of the regular wired corporate LAN. In many warehousing environments where they are used the AP is a simple bridge between the wireless and wired segments of the overall LAN. On the back end the Warehouse may be connected to the rest of the organization by a simple routing hop without access control. Should an attacker manage to access the 802.11 FHSS LAN, they would have the same access level as that they would by entering the building and sitting at a connected terminal.

Available security controls for 802.11 FHSS networks are very basic. Since many of the devices (STA and AP) that comprise these networks are themselves at the end of the lifecycle from the manufacturer they cannot be updated with more modern security controls. Controls for many of these devices are limited to MAC address filtering and 40 bit Wired Equivalent Privacy (WEP) encryption.

As we take a look at some of the inner workings of 802.11 MAC, FHSS PHY, and management and control frame types it should become obvious how an attack scenario such as the one presented in the next section may work.

2.2 802.11 Frame Types

There are many frame types specified in the 802.11 standard. The most important to understand are 802.11 management frames which are used for a STA to establish, maintain, and terminate communications.

The general management frame format is as follows:

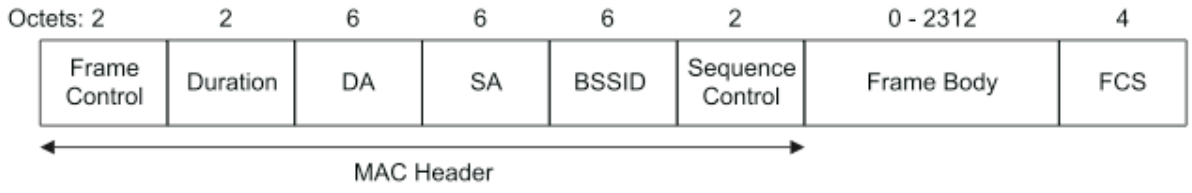

Figure 1 - 802.11 Management Frame Format

There are many subtypes of the frame body. Some important ones to note:

The beacon frame body, which contains the SSID, and the FH parameter set:

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

Table 1 - Beacon Frame Format

As was mentioned in the last section, the FH parameter set is an element that contains all parameters necessary for transmitter and receiver to stay in synchronization (Dwell Time, Hop Set, Hop Pattern, Hop Index).

Some documentation will refer to the SSID as the "network name" or even the "network number" because it is frequently assigned some character string. The SSID here is really a string of characters between 1 and 32 bytes that basically assigns the BSSID to a larger amalgamation. Keep in mind that knowledge of this string of bytes is, for most implementations the only thing that an attacker would need to join the WLAN.

The Association request frame body, which also contains the SSID:

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

Table 2 - Association Request Frame Format

The Probe request frame body, which contains the SSID as well:

Order	Information
1	SSID
2	Supported rates

Table 3 - Probe Request Frame Format

The Probe response frame body, which contains much the same information as a Beacon:

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

Table 4 - Probe Response Frame Body

2.3 802.11 FHSS PHY Layer

The FH PHY uses Gaussian Frequency Shift Keying (GFSK) modulation. All frequency shift keying encodes data as a series of frequency changes across a carrier. The advantage to this is that noise tends to change the amplitude of a signal, but systems that ignore amplitude tend to be relatively immune to noise. There are 2 basic flavors of GFSK used for transmission; they control the symbol rate (which basically amounts to 1 million or 2 million symbols per second). In 2 Level GFSK (2GFSK), two different frequencies are used depending on whether the data transmitted will be a 1 or a 0. To transmit a 1 the carrier frequency is increased by a certain derivation, and to transmit a zero the frequency is decreased by the same derivation. In 4 level GFSK (4GFSK) the same basic approach is used, except with 4 symbols instead of two. The four symbols (00, 01, 10, 11) each correspond to a discrete frequency and therefore twice as much data is transmitted at the same symbol rate.

The FHSS PHY specification is actually broken into three functional entities encompassing rules for the physical media dependant (PMD) sub layer which provides the transmission media between STA (i.e. modulation), the physical layer convergence procedure (PLCP) which is responsible for providing a method of mapping the IEEE 802.11 MAC protocol data units into a suitable framing format, and a physical layer management entity (PLME) which manages the physical functions in association with the MAC functions.

Since we've already discussed the PMD to some extent, let's touch on the PLCP frame format. The PLCP protocol data unit (PPDU) frame format provides for the asynchronous transfer of MAC sub-layer MPDU's from any transmitting STA to all receiving STA's within the wireless LAN's basic service set (BSS).

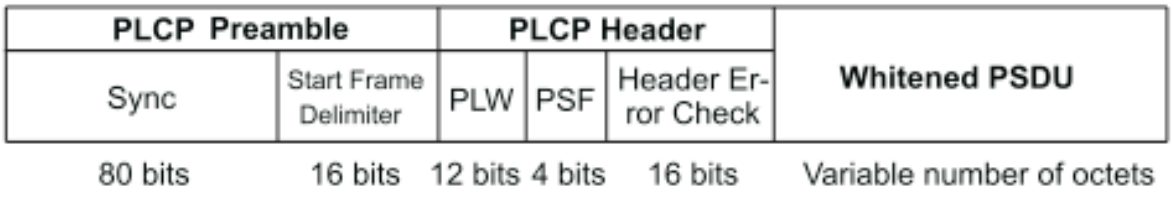

Figure 2 - PLCP Format

The important parts to know here are that the Preamble SYNC field is an 80-bit field containing an alternating zero-one pattern, transmitted starting with zero and ending with one, to be used by the PHY sublayer to detect a potentially receivable signal.

Data whitening is done on the PDSU (MAC Frame part of the transmission) in the in order to randomize the data from highly redundant patterns and to minimize DC bias in the packet.

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 frame synchronous scrambler uses the generator polynomial S(x):

$$S(X) = x^7 + x^4 + 1$$

3 Attacking 802.11 FHSS Networks

Given the limited to nonexistent levels of security on 802.11 FHSS networks, attacking them should be a trivial exercise. There is a very limited set of information required by an attacker who wishes to join the network. That would be:

- An SSID
- In certain cases a MAC address of an authorized client
- In some instance a 40 bit WEP key

As we saw in the management frame examples the first two are readily available in a client probe request frame, and the SSID alone is available in multiple frame types. If we could simply sniff a few frames over the air, we could likely find a beacon, client probe request, client probe response, or association frame in relatively short order.

The main problem seems to be the lack of an implemented promiscuous mode in 802.11 FHSS client cards. We can overcome this obstacle by using software-based radio. GNU Radio can be used to sniff packets.

From http://www.gnuradio.org:

> Software radio is the technique of getting code as close to the antenna as possible. It turns radio hardware problems into software problems. The fundamental characteristic of software radio is that software defines the transmitted waveforms, and software demodulates the received waveforms. This is in contrast to most radios in which the processing is done with either analog circuitry or analog circuitry combined with digital chips. GNU Radio is a free software toolkit for building software radios.
> Software radio is a revolution in radio design due to its ability to create radios that change on the fly, creating new choices for users. At the baseline, software radios can do pretty much anything a traditional radio can do. The exciting part is the flexibility that software provides you. Instead of a bunch of fixed function gadgets, in the next few years we'll see a move to universal communication devices. Imagine a device that can morph into a cell phone and get you connectivity using GPRS, 802.11 Wi-Fi, 802.16 WiMax, a satellite hookup or the emerging standard of the day. You could determine your location using GPS, GLONASS or both.

The radio receiver used to facilitate sniffing was the Universal Software Radio Peripheral (USRP) from Ettus Research. Also from http://gnuradio.org:

> The Universal Software Radio Peripheral, or USRP (pronounced usurp) is designed to allow general-purpose computers to function as high bandwidth software radios. In essence, it serves as a digital baseband and IF section of a radio communication system.

```
The basic design philosophy behind the USRP has been to do all of
the waveform-specific processing, like modulation and
demodulation, on the host CPU. All of the high-speed general-
purpose operations like digital up and down conversion,
decimation and interpolation are done on the FPGA.
The true value of the USRP is in what it enables engineers and
designers to create on a low budget and with a minimum of effort.
A large community of developers and users have contributed to a
substantial code base and provided many practical applications
for the hardware and software. The powerful combination of
flexible hardware, open-source software and a community of
experienced users make it the ideal platform for your software
radio development.
```

In order to eavesdrop on the network and pull the pieces from the data stream that we need it is not necessary to know the hop pattern of the network. Luckily we have much existing research and code that was already developed and can help out greatly with this task.

In 2007 Dominic Spill and Andrea Bittau published a paper entitled "BlueSniff: Eve meets Alice and Bluetooth" (the continuing project and code is located at: http://gr-bluetooth.sf.net) where they described a method of sniffing Bluetooth networks. This is not at all dissimilar to what I'm positing as Bluetooth is another FHSS technology utilizing GFSK modulation at the PHY.

In order to sniff Bluetooth the method used was to lock the USRP to a single channel in the band and wait for traffic to hop by.

This method is more than adequate for our purposes. We know that 802.11 FHSS utilizes 79 channels in the ISM band, and we know that each channel can only be 1 MHz wide. By simply locking on a single channel in the band and waiting we will receive one of the four types of management frames that will provide us with needed information.

In leveraging this method we also benefit from the myriad of development work done with the USRP and 802.11 such as the ADROIT project (as well as others code and examples – the GNURadio development community is extremely productive, friendly, and helpful). This greatly simplifies the technique as we can re-use code developed for other purposes.

Once we have the information that we need to connect to the network (in most cases a simple SSID) doing anything complicated such as defining a hopping pattern to cover all 79 channels is unrealistic, and due to the limitations of the USRP some code has been released which can send and receive 802.11 at 1 mbps. However, USB 2.0 is too slow to support two-way 802.11 interactions. However we can utilize a 802.11 FHSS STA at this point and simply connect to the network normally. Certain NIC's such as a Symbol Spectrum23 LA-3020-500 work extremely well for this function and they can still be easily purchased online from multiple vendors.

Once the attacker connects to the network they are now free to explore the corporate LAN environment in most cases. With the lack of security controls in place in most organizations, the LAN and WAN environment can become a veritable candy store.

As we discussed in the section on architecture, most times 802.11 FHSS AP's are implemented as simple wireless to wired bridges, so once the attacker is on a WLAN as they are in the same broadcast domain as the Wired networks Layer 2 attacks against the wired side such as ARP cache poisoning are entirely feasible.

One attack scenario might be:

1. The attacker uses the USRP to gain access information for the WLAN environment
2. The attacker connects to the WLAN as a client and realizes the entire facility is one broadcast domain.
3. The attacker executes an ARP cache poisoning attack.
4. The attacker uses Ettercap filters to inject an SMB path leading back to his device into every web page.
5. As victims browse either internal or external web sites they send the attacker an LM + Half Challenge as they try to authenticate to the SMB path.
6. The attacker collects the hashes and compares them to rainbow tables and now has network credentials for a majority of the users in the facility.

This is just one of many attack scenarios that could be leveraged once the attacker has access to the 802.11 FHSS network.

4 References

GNU Radio Frequently Asked Questions - *http://gnuradio.org/trac/wiki/FAQ*

BlueSniff: Eve meets Alice and Bluetooth – *D. Spill and A. Bittau - http://gr-bluetooth.sf.net*

Building an All Channel Bluetooth Monitor – *M. Ossmann and D. Spill - http://shmoocon.org/slides/ossmann-spill-shmoo-2009.ppt*

Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications - *ANSI/IEEE Std 802.11, 1999 Edition*

Telecommunications Essentials: The Complete Global Source for Communications Fundamentals, Data Networking and the Internet, and Next-Generation Networks - *Lillian Goleniewski, Addison-Wesley Professional (January 5, 2002)*

802.11 Wireless Networks: The Definitive Guide, Second Edition - *Matthew Gast, O'Reilly Media, Inc.; 2 edition (April 25, 2005)*

Intercepting Mobile Communications: The Insecurity of 802.11 – *N. Boristov, I. Goldberg, D. Wagner - www.isaac.cs.berkeley.edu/isaac/mobicom.pdf*

BBN ADROIT Project - *http://gnuradio.org/trac/wiki/BBN_Technologies_Internetwork_Research_ADROIT_Project*

Characterizing the IEEE 802.11 Traffic: The Wireless Side – *J. Yeo, M. Youssef, A. Agrawala - www.lib.umd.edu/drum/handle/1903/1344*

The USRP under 1.5X Magnifying Lens! - *Firas Abbas Hamza*