# ***Does Frequency Hopping Enhance Security?***

*Jim Zyren, Tim Godfrey, Dennis Eaton*

## Executive Summary

This report is written in response to claims regarding the security benefits of HomeRF Frequency Hopping Spread Spectrum (FHSS) technology relative to Direct Sequence Spread Spectrum (DSSS) technology as employed by IEEE 802.11b systems. Proponents of HomeRF technology have asserted that frequency hopping in HomeRF increases the difficulty of eavesdropping on or intercepting data, let alone decrypting it, compared with the static channel used in direct sequence 802.11b.

This assertion is incorrect. HomeRF systems do not enjoy any advantage over IEEE 802.11b systems in terms of preventing eavesdropping or interception of message traffic.

All WLAN systems employ various security measures. Both Frequency Hopped Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS) systems use data encryption methods to prevent unauthorized eavesdropping, and user authentication procedures to prevent unauthorized users from gaining access to sensitive data. Beyond these measures, proponents of FHSS WLAN technology often claim to have an addition level of security which is inherent to that technology. In fact, there is no inherent security benefit associated with FHSS as implemented in HomeRF systems. Hop sequences can easily be determined by very unsophisticated methods. As explained in greater detail below, the hop sequences of HomeRF radios can be determined in less than 5 seconds.

It should be pointed out that systems like HomeRF use FHSS modulation in order to comply with FCC regulations governing operation in the 2.4 GHz ISM band. These techniques are aimed at regulatory compliance, *not security enhancement*. As it turns out, HomeRF networks make no attempt to conceal the hop set. Again, the hopping algorithm is not considered a security measure. For this reason, the hopset identification information is transmitted in unencrypted format by the HomeRF Control Point (analogous to an IEEE 802.11 Access Point) in every beacon, which occurs each time the network hops channels (ie 50 times per second).

Even if the hopset identification information was not transmitted in an unencrypted manner within the Control Point (CP) beacon, the hopset could easily be determined. As the name implies, FHSS radios change their operating frequency in a pseudo-random manner. Because of the pseudo-random nature of the hop sequence, it would appear that some measure of protection against unwanted eavesdropping is gained. However, this is not the case. For HomeRF radios, the hop sequence can easily be decoded in less than 5 seconds for the following reasons:

1.) The hop rate is relatively slow at 50 hops / second (even Bluetooth is considered a “slow hopper” at 1600 hops /second).

2.) There are only a very limited number of different hop patterns defined for HomeRF radios, with each hop set consisting of 75 different frequencies. Each hop set repeats itself every 1.5 seconds.

3.) The patterns are published in the HomeRF specification (SWAP v1.3). Although the SWAP specification is available to HomeRF members only, hackers do not generally respect NDA’s.

4.) In the HomeRF protocol, a beacon is transmitted each time the network hops to a new channel.

As explained in greater detail below, by simply listening on to the beacons for a total of not more than 4.5 seconds, the hop set of a HomeRF radio can easily be decoded. Even if the beacon were encrypted (which it is not) merely detecting the burst of RF energy and accurately recording the time of reception would enable the hopset to quickly be determined. As easy as it is to decode the hop set for a conventional HomeRF system employing 75 channels, would be even simpler to do so for Wide Band Frequency Hopping (WBFH) systems which employ only 15 channels. Bottom line: FHSS systems do not enjoy any inherent security advantage over DSSS systems.

**Why Do Some Systems Employ FHSS Instead of DSSS?**

In order to transmit useful power levels for WLAN applications (> 1mW), Section 15.247 of the FCC regulations requires that either FHSS or DSSS modulation be used. It should be noted that the original intent behind these regulations was to spread out the energy of the transmitted signal in order to minimize interference to other users of the spectrum. This was considered to be a prudent measure by the Commission because the spectrum was unlicensed, and interference-reducing measures were considered necessary.

*FHSS was therefore adopted by some manufacturers for use in the 2.45 GHz ISM band because it is one of two methods mandated by the FCC --- not because it offers any security advantage.*

**Why is the Hop Sequence so Easy to Decode?**

As mentioned above, the FCC requires use of either DSSS or FHSS techniques for transmission of more than 1 mW of RF energy in the 2.45 GHz ISM band. Systems using FHSS or DSSS are allowed to transmit up to 1 Watt (1000 mW), thus making them very useful for WLAN applications. The algorithms used to determine the hop sequence for HomeRF radios is extremely simple, and is published in the SWAP specification. Again, the hop sequences are aimed at FCC compliance, not at security enhancement.

The easiest way to determine the hop sequence of a HomeRF radio is to simply tune to any channel at random and just listen for a beacon. HomeRF radios hop through each the 75 hopping channels at a rate of 50 hops per second in a total of 1.5 seconds, repeating the same pattern each time. In other words, the hopping channel is selected in a pseudo random manner from among a list of 75 frequencies on a “sample-without-replacement” basis. Assuming the HomeRF network is active, a beacon will be transmitted on any particular channel in less than 1.5 seconds. Even if HomeRF were to encrypt the beacons, the hop set could easily be determined.

The hop rate of a HomeRF radio is very slow. A HomeRF radio hops channels every 20 msec, or 50 times per second. In addition, the HomeRF Control Point (completely analogous to an IEEE 802.11b Access Point) transmits a beacon every time the network hops to a new channel. Further, there are only 75 separate hop sequences defined for HomeRF radios. As described above, the network hops through each of the 75 channels in the given sequence in a pseudorandom manner before returning to the first frequency in the sequence and repeating the process. Therefore, the hop sequences repeat themselves every 1.5 seconds (75 channels x 20 msec/channel). In order to decode the entire hop set, an eavesdropper need only determine which of the hop sequences is being employed, and which channel the network will hop to at any particular moment.

## OK, How is it Done?

As it turns out, decoding a HomeRF hop sequence is trivial. An eavesdropper could determine the hop sequence of a HomeRF network in less than two minutes simply by listening for beacons on each of the 75 channels and doing some simple arithmetic. Even if the beacons were encrypted (and they aren't), simply recovering the times at which the beacons are transmitted can be used to quickly determine the hop sequence.

Let's consider the "brute force" method. Assuming the eavesdropper has the ability to control the frequency of his or her receiver, but not the ability to read the beacon message, the hop sequence can be determined in less than two minutes using the following procedure:

1.) Tune to Channel X.
2.) Listen for the Control Point Beacon.
3.) When the beacon is received, the time of reception is recorded
4.) Tune to Channel Y and listen for the Control Point Beacon
5.) Record time of reception. Because the hop pattern repeats itself, the beacon should be detected in not more than 1.5 seconds.
6.) By accurately measuring the time between beacons, the eavesdropper could determine the entire hop sequence in about one minute on average, and not longer than two minutes worst case.

For the eavesdropper in a hurry, the hop sequence could actually be determined in less than 5 seconds. There are a very limited number of hop sequences defined for HomeRF radios. As it turns out, the hop sequence can be uniquely identified by determining the beacon timing on as few as three channels. This could be done in under 5 seconds. However, even this degree of effort is unnecessary because the hopset identification information is transmitted in the clear on every CP beacon.

## Conclusions

HomeRF radios have no inherent security advantage over DSSS radios. Both HomeRF and IEEE 802.11b radios must rely on encryption and user authorization procedures to ensure network security. FHSS radios use frequency agility to conform to FCC regulations, not for security enhancement. This is clearly demonstrated by the fact that the HomeRF beacon transmits the hop set identification information in unencrypted format in each CP Beacon.

Even if the hopset identification information were not transmitted "in the clear", the FHSS hopset can be easily determined by simply passively listening to traffic on each of the hopping channels. For these reasons, the frequency agility of HomeRF's FHSS systems do not offer any inherent security advantage over DSSS systems.