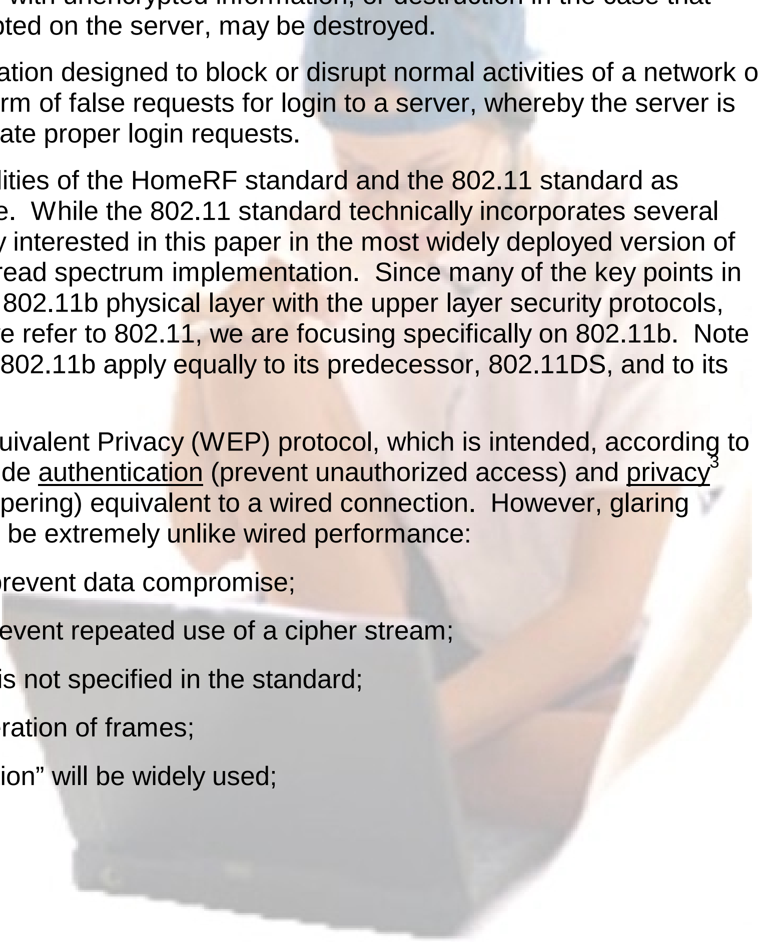
A Comparison of Security in HomeRF versus IEEE802.11b

Though the possibility of attacks similar to those leveled at 802.11b systems exist in theory for HomeRF systems, the relative level of difficulty is very different. HomeRF is stronger in preventing unauthorized access due to its frequency hopping technology and since attempts are not enabled by commercially available equipment.

Introduction

The security of wireless LANs has recently become an area of much concern. Several popular articles[1] and academic papers[2] have identified security concerns with the IEEE 802.11 standard. For most WLAN users there are three basic issues:

1. Data Compromise is any form of disclosure to unintended parties of information. Data compromise can be inappropriate access to payroll records by company employees, or industrial espionage whereby marketing plans are disclosed to a competitor.
2. Unauthorized Access is any means by which an unauthorized party is allowed access to network resources or facilities. Unauthorized access can lead to compromise, for example, if access is gained to a server with unencrypted information, or destruction in the case that critical files, although encrypted on the server, may be destroyed.
3. Denial of Service is an operation designed to block or disrupt normal activities of a network or facility. This can take the form of false requests for login to a server, whereby the server is too distracted to accommodate proper login requests.



In this paper we will examine the capabilities of the HomeRF standard and the 802.11 standard as regards these general areas listed above. While the 802.11 standard technically incorporates several different physical layers, we are primarily interested in this paper in the most widely deployed version of 802.11, the 802.11b direct sequence spread spectrum implementation. Since many of the key points in this paper relate to the interaction of the 802.11b physical layer with the upper layer security protocols, the reader can assume that whenever we refer to 802.11, we are focusing specifically on 802.11b. Note also that the basic flaws shown here for 802.11b apply equally to its predecessor, 802.11DS, and to its successor, 802.11g.

The 802.11 standard uses the Wired Equivalent Privacy (WEP) protocol, which is intended, according to clause 8 of the 802.11 standard, to provide authentication (prevent unauthorized access) and privacy[3] (prevent data compromise and data tampering) equivalent to a wired connection. However, glaring deficiencies exist which cause 802.11 to be extremely unlike wired performance:

- The 40-bit WEP key is too short to prevent data compromise;
- The 24-bit WEP IV is too small to prevent repeated use of a cipher stream;
- The manner is which the IV is used is not specified in the standard;
- The ICV is useless for detecting alteration of frames;
- It is probable that “Open Authentication” will be widely used;

[1] References 1-4.

[2] Reference 5, hereinafter the Berkeley” paper, and reference 6, hereinafter the “Maryland” paper.

[3] The Berkeley paper, page 2.

As is discussed in the Berkeley paper, the fundamental flaws in the WEP protocol compromise its ability to protect the network. In the Maryland paper, problems with access control are discussed. The 802.11e task group has recently issued a draft[4] specification intended to enhance the security of these networks. While the proposed changes address many concerns related to compromise and alteration of data and unauthorized access of the current design, these will be ineffective in preventing denial of service attacks[5] against 802.11 systems. The lack of protection of control fields and frames would require substantial change to the 802.11b physical layer.

As discussed below, in many of these areas the basic structure of the HomeRF architecture provides a measure of security beyond that available on 802.11 networks. This added security is especially important for home network users without the IT department resources to implement more advanced security measures for 802.11.[6]

Data Compromise

The issue of most importance to users is typically the protection from disclosure to unintended parties of the data they are sending or receiving. For example, if sensitive information is being sent from one computer to another the user will want to know that no other user with access to the network (legitimate or illegitimate) can eavesdrop on that data stream.

802.11b Encryption

The current 802.11WEP defines a 40-bit encryption key, which is, according to the Berkeley paper “short enough to make brute-force attacks practical to individuals and organizations with fairly modest computing resources.” The Berkeley paper further observes that the Initialization Vector[7] (IV) is too short, at 24 bits, making it likely that the IV, and hence the actual cipher stream, will be repeated in about half a day. Furthermore, the Berkeley paper continues, management of IVs in 802.11 is flawed, since the lack of specification of the manner in which IVs change allows implementations which change the IV in an undesirable manner; this means that the WEP protocol remains vulnerable to attack even with the use of longer, 128-bit keys. The new draft security standard from the 802.11e task group may address some of these deficiencies eventually. But users will benefit from such changes only by completely replacing all of their WLAN access points and client devices purchased before the new products are available (likely late 2002).

HomeRF Encryption

The HomeRF standard already defines 128-bit key encryption. More importantly, HomeRF uses a 32-bit IV; compared to the 24-bit IV used in 802.11, the time scale for repeated IV is half a year instead of half a day. In addition, the HomeRF management procedure completely specifies the manner in which IVs are chosen, and this is designed to minimize the likelihood of repetition of any IV value. Unlike 802.11, a brute force attack on HomeRF encryption is inconceivable for organizations without the resources of a government security agency.

[4] Reference 7.

[5] In fact, Kerberos (RFC 1510), which is invoked as an “upper layer” protection measure in the draft 802.11e specification, specifically indicates that it does not prevent denial-of-service attacks.

[6] In reference 8, the author states “We're effectively being told that unless we are a large enterprise with a dedicated IT staff and the necessary infrastructure to set up VPN servers and associated folderol we're not worthy of properly designed and implemented security. A flawed system is considered sufficient.”

[7] The IV is combined with the encryption key for stream cipher generation, which avoids repetition of the cipher stream between key changes **if** the IV does not repeat.

Unauthorized Access

The next layer in the discussion of security is access control. Users must know whether unauthorized users can gain access to the network and intercept the encrypted stream (in an attempt to break the encryption), inject other data into the stream, or perform some other undesired operation such as breaking into a server database.

802.11b Access Control

In this area, the two recent academic papers found flaws in the 802.11 standard, both with the WEP protocol and with other components of 802.11 access control.

The Maryland paper describes the basic process involved in a client device finding and associating with an access point on an 802.11 network. The basic steps are as follows:

1. The client listens for beacon messages from the access point(s);
2. The client uses a vendor-specific algorithm to choose an access point;
3. Authentication occurs by way of an exchange of management frames;
4. Association also results from an exchange of management frames.

The Maryland paper discusses the vulnerability of the 802.11 authentication procedure.[8] The default protocol in the 802.11 standard is known as "Open System Authentication" which means that the most systems will authenticate any user that make the request. Therefore, Open System Authentication means that there is no barrier to a hacker penetrating an 802.11 network.

A more robust, but proprietary, access control protocol, known as "Closed Network" has been implemented by Lucent in its products based on the 802.11b standard. Of course, once such a proprietary protocol has been enabled the products are no longer 802.11b-compliant; that is, they will not interoperate with products from other 802.11b manufacturers, only with other Lucent 802.11b products. The protocol is based on shared knowledge of a network name, or SSID. Only those clients with knowledge of the network name can join.

Clearly the Open System Authentication provides no measure of access control. The Maryland paper finds flaws in the Lucent Closed Network implementation as well because "several management messages contain the network name, or SSID, and these messages are broadcast in the clear by access points and clients." Therefore, the authors argue, "an attacker can easily sniff the network name – determining the shared secret and gaining access to the 'protected' network." The Maryland paper also points out that the Shared Key authentication of the 802.11 can be defeated because of the known frame structure and current lack of tamper protection; a recipe for circumventing the Shared Key authentication is given.

HomeRF Access Control

In HomeRF all devices make use of a "shared secret" network ID (NWID) without which compliant devices will not be permitted to communicate. Because HomeRF uses a frequency hopping physical layer (as opposed to the frequency static and code static 802.11b physical layer) a client device must synchronize its hopping sequence with the access point in order to receive the data. In order to synchronize, the client must have the identical security NWID. Without this parameter, the unauthorized radio will never synchronize, thus the over the air data cannot be captured via another HomeRF radio. In HomeRF the association process described above for 802.11b looks like the following.

1. A HomeRF node chooses a fixed frequency and listens for a period of time;

2. The MAC will only deliver packets to high layers in the following cases:

   a) The NWID of the receiver matches the NWID of the transmitter;

[8] The use of WEP to provide access control is compromised by the same flaws alluded to in the discussion of data integrity. It is likely that the work of the 802.11e security group will resolve many of these flaws.

   b) The transmitter has been directed to teach the NWID, and the receiver has been directed to learn the NWID;

3. Network IDs can be allocated to a device by the following means:
   a) By direct entry into the device (this would be the only method most IT managers would likely support);
   b) Or, optionally, by learning from another node per 2b above. The NWID can only be learned from a device that is "teaching" the NWID. The teaching function does not occur continuously (as in 802.11), but rather by physical intervention such as pressing a button. There is no equivalent in HomeRF to the 802.11b Open System Authentication.
4. Once the client associates with an access point with the same NWID, the 24-bit NWID prevents unauthorized access to the data stream.[9]

At first glance it would appear that the HomeRF access-control method using the NWID has the same vulnerability as the proprietary Lucent SSID[10] mechanism. This is not the case. The 802.11b physical layer is frequency-static and uses only a single direct-sequence spreading code. Therefore, it is relatively easy to search, using a standard client card, through the few center frequencies and receive data, even with WEP activated. While WEP is supposed to prevent unauthorized clients from *connecting to the network*, it cannot prevent passive listening, i.e. just receiving the data. So, even with encryption enabled, the intruder would have access to the encrypted data, and, as is mentioned above, the SSID data is not protected by encryption.

The reason why HomeRF is stronger in preventing unauthorized access is that attempts are not enabled by commercially available equipment. When evaluating a security threat it is necessary to consider not only the possibility of an attack, but also the level of difficulty to mount the attack and the probability that someone will try. Though the possibility of attacks similar to those leveled at 802.11b systems exist in theory for HomeRF systems, the relative level of difficulty is very different. Because of the frequency/code static nature of an 802.11b network it is possible for any compliant 802.11b device to be used as an eavesdropping device; this requires little cost invested by the hacker. The same is not true for a HomeRF frequency-hopping network. In order for a hacker to find the HomeRF hopping sequence information, he would need to build specialized equipment that would wait on a HomeRF frequency, acquire the signal and demodulate the transmitted information, and then, using knowledge of the structure of the HomeRF modulation and frame structure, decode the received information to determine the NWID and the hopping sequence. No commercially available HomeRF product in the world today, nor any future products compliant with the HomeRF specification, can be used directly to accomplish this feat.

So while such an attack against HomeRF is not *impossible*, it is important to understand the relative difficulties of the two kinds of attacks being proposed. The 802.11b systems have been shown to be vulnerable to attacks made using off-the-shelf, existing components. HomeRF would only be vulnerable to custom-built hardware and firmware designed to break into the system. Such an attack is orders of magnitude more complex than those required for 802.11b. If caught, possession of such custom-built equipment would signal clear malicious intent and increase the likelihood of prosecution.

[9] A 24 bit NWID has over 16 million possible values; guessing strategies are of little use.

[10] In fact, such a vulnerability was implied in the "Response from the IEEE 802.11 Chair on WEP Security", where the Chair states "Certain reports in the press have implied that frequency hopping wireless LAN systems would be less vulnerable to security attacks than other wireless LANs. This is not true given that in such frequency hopping systems the hopping codes and timings are unencrypted and consequently are easily available to an attacker." This analysis from the IEEE is not correct, as is clear when the physical layer is taken into account.

Denial of Service

The easiest way for an attacker to disrupt a network is to shut it down. This Denial of Service (DoS) attack is employed at protocol levels that cannot be protected by encryption, and many high profile events have occurred in recent years.[11] Spread-spectrum systems were originally developed to combat intentional jamming, the object of which is brute-force denial of service on a battlefield. DoS attacks on the Internet have been dramatic in number of users affected. These are an example of exploitation of protocols, rather than jamming, to disrupt network operations; they produce strong effects with subtle attacks. It is in this area that 802.11b networks are most vulnerable. These vulnerabilities cannot be "patched up" in the manner 802.11e attempts to fix WEP vulnerabilities, rather, they would require fundamental changes to the physical-layer architecture. This vulnerability is due to the *frequency-static, code-static* physical layer, which results in complete lack of protection of control sequences. HomeRF's frequency hopping physical layer provides a level of protection against denial of service that 802.11b systems cannot provide. And HomeRF's MAC layer also does not allow the easy Denial of Service protocol attacks that are prevalent in 802.11.

Wireless networks employ (optional) encryption to protect data payloads of packets; this is thought to be critical to access control and in some cases is also used for low-grade protection against data compromise. However, control portions of data packets, and all control packets, are sent "in the clear", with only the spread-spectrum signaling protecting control information. This only works if the spread-spectrum technique employed remains true to the principles originally conceived for that technique.

Denial of Service in 802.11b

The 802.11b DSSS is static in frequency and also uses a single DS "spreading code" for all time and all users, as specified in the standard. Anyone desiring to do so can generate valid 802.11b control packets which must be accepted by all 802.11-compliant equipment; alternatively, anyone can listen to all 802.11b control frames transmitted.

The complexity of wireless data-link protocols makes comprehensive enumeration of specific denial-of-service attacks impossible. Hackers on the Internet have, indeed, shown tremendous creativity in their nefarious activities. Examples of approaches a potential disrupter could employ[12] are:

1. Repeated requests for authentication, thus distracting an access point's from servicing legitimate requests for authentication;
2. Requests for de-authentication (hence, disassociation) of legitimate users;[13]
3. Mimicking AP behavior, thus collecting unsuspecting clients who cannot understand why the AP isn't offering higher-layer services;
4. Clearing the air by repeated transmission of RTS/CTS frames.

As concrete example, we consider the aforementioned RTS/CTS attack. While use of RTS/CTS exchanges is optional in the standard, any compliant 802.11 device hearing an RTS/CTS exchange *must* honor it by abstaining from frame transmission for the duration specified in the RTS and/or CTS frames. The RTS and CTS frames contain only MAC addresses, which can be entirely false (no knowledge of "secret" network ID is required). Because 802.11b is static in frequency and uses only a single spreading code, a disruptor unit can select a frequency channel based upon observed activity, then periodically transmit an (apparent) RTS/CTS exchange that clears the medium. Since the RTS/CTS exchange relative short, this process can hold off all legitimate activity with a very low duty factor. It is important to understand that this is not jamming; rather it is a protocol

[11] See reference 9. According to this article "At least seven top Web sites have been knocked offline in the past three days by an unprecedented level of attacks that have raised new concerns about Internet security. On Monday, the leading independent Web portal, Yahoo!, was attacked and made inaccessible. On Tuesday, Buy.com, Amazon.com, eBay and CNN.com were attacked. And so far today, technology site ZDNet and online trading site E*TRADE have suffered attacks."

[12] Any disruption strategy can also guarantee capture of the channel by slight violation the inter-frame space; this is generally unnecessary.

[13] De-authentication requests cannot be refused, per the standard.

attack. It is completely effective at extremely low duty factor, and the disruptor signals need not be strong, only a little above receiver threshold for a reasonable number of users.

The vulnerability of 802.11 to this type of attack is even worse than has been described. Because the duty factor is so low using RTS/CTS to clear the air, a single disruptor unit could operate sequentially over all eleven 802.11b frequency channels channels. With *no prior knowledge* this unit could effectively "take down" all 802.11b activity over a wide area. For example, a small device with a 1-W power amplifier and connectorized antenna could be set up on a hill to completely frustrate 802.11b activity in some area. A hacker might do that just for fun. If the hacker simultaneously sends some "useful" data over his "network" while shutting down an entire university campus for example, there is considerable opinion that his activity would not even be illegal under current FCC regulations.

Denial of Service in HomeRF

By contrast with 802.11b, HomeRF employs legitimate frequency hopping, which must be overcome in order to inject or detect control frames. In order for a disrupter to even send these confusing control frames to a HomeRF access point it would first have to determine where in the frequency regime that access point is going to be at any given point in time. This is not impossible, but as stated before, it is extremely more difficult than for 802.11b. Add to this the fact that an entire campus would have each of the many access points hopping on independent sequences and time bases, and add the fact that HomeRF MAC ignores commands from foreign network IDs, and one can only logically conclude that a mass Denial of Service is practically impossible for HomeRF instead of trivial for 802.11b.

Conclusion

Protection of data against tampering and compromise is, perhaps, the easiest to ensure using upper-layer protocols. There is no more secure way of protecting data than the use of end-to-end encryption.[14] This level of data security is independent of the underlying networking technology as long as the related end-to-end encryption keys are restricted to only intended parties. Numerous capabilities exist, such employment of a VPN connection between endpoints, for encrypting data with substantial protection against compromise and tampering. If properly implemented, upper-layer services can also enhance protection against unauthorized access; the draft 802.11e specification includes optional use of Kerberos, the capabilities of which include data protection and access control, all premised upon an underlying network that cannot be trusted. Such techniques can also be applied to HomeRF although the superior inherent security of HomeRF makes the need much less compelling.

However, upper-layer services cannot eliminate all potential problems incurred at the physical layer. If "wired-equivalent" anything is required, attention to the physical layer is critical. 802.11b offers a spread-spectrum physical layer that departs substantially from conventional DS practice in that a single spreading code is used; a single code for a DS system is equivalent to having only a single hop frequency for a frequency "hopping" system. By contrast, HomeRF uses legitimate FH sequences.

In summary, 802.11b may ultimately establish reasonable use of low-level encryption, overcoming present WEP limitations; however, 802.11b equipment purchased before the improved equipment is available (approximately late 2002) will almost certainly have to be retired rather than upgraded. Furthermore, the "upper-layer" solutions to some problems will not readily be accessible to home and small businesses users who lack the services of an IT manager in working out the details. Finally, the physical-layers issues making 802.11b vulnerable to a variety of Denial of Service attacks cannot be removed without substantial renovation of the existing DS PHY portion of the standard, equivalent to throwing it out and starting over. For these many reasons, HomeRF is the only realistic solution of the wireless LAN security problem for home and small-office users.

[14] An example would be the use of PGP, or the establishment of a VPN connection.

References

1. “Flaw in Popular Wireless Standard”, John Markoff, The New York Times, April 3, 2001.
2. “Hackers Delight”, Larry Mittag, Communications System Design, April 2, 2001.
3. “Researchers Find That Hackers Can Penetrate Wireless Network”, Jared Sandberg, Staff Reporter of The Wall Street Journal, February 5, 2001.
4. “War driving by the Bay”, Kevin Poulsen, The Register, April 13, 2001. http://www.theregister.co.uk/content/8/18285.html
5. “Intercepting Mobile Communications: The Insecurity of 802.11”, Nikita Borisov, Ian Goldberg, David Wagner. http://www.isaac.cs.berkeley.edu/isaac/wep-draft.pdf
6. “Your 802.11 Wireless Network Has No Clothes”, William A. Arbaugh, Narendar Shankar, Y.C. Justin Wan. http://www.cs.umd.edu/~waa/wireless.pdf
7. Draft Supplement to Standard for Telecommunications And Information Exchange Between Systems - LAN/MAN Specific Requirements - Part 11: Wireless Medium Access Control (MAC) And Physical Layer (PHY) Specifications: Specification For Enhanced Security.
8. “802.11 and Swiss Cheese”, Stephan Somogyi, ZDNet News, April 12, 2001. http://dailynews.yahoo.com/h/zd/20010412/tc/802_11_and_swiss_cheese_1.html
9. “Reno Vows Action: FBI Investigates Web Attacks; ZDNet and E*Trade are Latest Sites Hit”, Jonathan Dube, February 9, 2000, abcNEWS.com. http://abcnews.go.com/sections/tech/DailyNews/yahoo000209.html

Appendix A: Comparison of HomeRF and 802.11b Security

Security Area	***802.11***	***HomeRF***
Data Compromise	• 40 bit keys • 24 bit initialization vector (IV) • Undefined use of IV • New 802.11e standard will address several flaws in this area only	• 128 bit keys • 32 bit IV • Defined IV management
Unauthorized Access	• Open authentication • Frequency/Code static physical layer hobbles Closed network access control	• Shared secret network ID (NWID) • True frequency hopping physical layer lends strength to NWID access control • Compliant products are not usable to “sniff” NWIDs
Denial of Service	• Frequency/Code static physical layer leaves control frames completely vulnerable • Practical attacks using commercially-available hardware can disable all 802.11b networks over a wide area	• True frequency hopping physical layer protects control frames • An attack against a single HomeRF network takes considerable effort • An attack against all networks in an area is virtually impossible