Global Information Assurance Certification Paper

HomeRF: Wireless with Security, for the Rest of Us?

The purpose of this paper is to provide an overview of the security aspects of the HomeRF standard, compare it to the IEEE 802.11b standard. This paper draws on a recent white paper issued by the HomeRF Working Group [HOM]. The issues of data compromise, unauthorized access and denial of service will be compared for both standards.

Researchers at UC Berkeley [BOR] and the University of Maryland [ARB] have identified several vulnerabilities in IEEE Standard 802.11, specifically 802.11b. These vulnerabilities are a cause for concern among users of Wireless LANs:

- The 40-bit Wireless Equivalent Privacy (WEP) key is not long enough to prevent compromise.
- The 24-bit Initialization Vector (IV) is too small to prevent frequent repeat of a cipher stream.
- There are reports of widespread use of the standard's Open Authentication.
- There is no prescription for the manner in which the IV should be used.
- The Integrity Check Value (ICV) is not adequate for detection of frame tampering.

These vulnerabilities provide opportunities for the following types of compromises of Wireless LANs:

- Disclosure of information/content to unintended destinations.
- System/network access by individuals/groups without appropriate authority.
- Disruption of system/network service in the form of a denial of service attack.

Previous papers published in the SANS Reading Room surveyed threats and countermeasures in wireless networks [WAN] and addressed the Bluethooth security architecture [ANA].

IEEE 802.11

While a detailed discussion of wireless LANs is not in order here, several tutorials that would lay a good foundation for our discussion are available [LOU] [RHO] [WLA] [ZYR]. A brief description of the 802.11 Wired Equivalent Privacy (WEP) protocol and the manner in which it constructs messages is in order [MEN].

WEP protocol uses a 40-bit shared secret key, Rivest Code 4 (RC4) Pseudo Random Number Generator (PRNG) encryption algorithm and a 24-bit initialization vector to implement security. Messages are encrypted using the following process. A checksum of the message is computed and appended to the message. At this point the message is still plain text. Concurrently, the shared secret key and the initialization vector (IV) feed the RC4 algorithm to produce a key stream. An exclusive or (XOR) operation of the key stream with the message/checksum grouping produces cipher text. The initialization vector is appended to the cipher text forming the encrypted message and it is sent to the intended recipient.

The recipient has a copy of the same shared key, and uses it to generate an identical key stream. XORing the key stream with the ciphertext yields the original plaintext message.

Data Compromise

The researchers at UC Berkeley [BOR] found several ways that the WEP protocol could be attacked successfully. Their discoveries were based in two areas:

- Keystream reuse
- Message authentication

Their conclusion was that WEP should not be relied upon for strong link level security and that additional precautions needed to be taken in that regard.

A well-known pitfall of stream ciphers is that encrypting two messages under the same IV and key can reveal information about both messages. In other words, XORing the two ciphertexts together causes the keystream to cancel out, and the result is the XOR of the two plaintexts. Having several ciphertexts that all use the same keystream we can eventually uncover the plaintext. The more such ciphertexts that we have the easier it will be to uncover the plaintext. Two conditions are required for this class of attack to succeed. There must be ciphertexts in which some portion of the keystream is used more than once. There must be partial knowledge of some of the plaintext.

The attacks shown to be possible by the researchers indicate that the use of stream ciphers leads to negative consequences and therefore is dangerous. Protocols that use stream ciphers should be precluded from the reuse of keystreams.

IEEE 802.11 does not specify how IVs are to be managed (changed) and this could lead to individual implementations that compromise keystream detection even with longer keys.

Unauthorized Access

The researchers at the University of Maryland [ARB] described a process by which a client device could find and become associated with an access point. Since the default authentication in 802.11 is “Open Authentication”, i. e., most systems will authenticate any user that requests connection. Shared Key authentication is described but not mandated in 802.11. Similarly, officials at Cisco Systems Inc.'s Aironet division estimate that only one-third to one-half of their users deployed WEP before the vulnerabilities surfaced [CIS] —which indicates a startlingly high number of users transmitting unencrypted data. Proprietary protocols developed by other vendors, while more effective, also severely limit the interoperability of such devices to other devices from the same vendor.

Additionally, The Maryland researchers describe a method by which even Shared Key authentication can be defeated.

Denial of Service

IEEE 802.11b uses Direct Sequence Spread Spectrum (DSSS), [GEI] which is static in frequency and uses a chipping code that is fixed. As such its packets can be crafted by an impostor and would be accepted by any 802.11-compliant equipment.
Examples to illustrate the use of this feature to create a denial of service (DoS) include: [HOM]

- Requests for authentication at such a frequency as to disrupt legitimate traffic.
- Requests for de-authentication of legitimate users. (These requests may not be refused according to the standard.)
- Impersonating the behavior of an access point and diverting unsuspecting clients to communicate with it.
- Repeated transmission of RTS/CTS frames silences networks in a wide area.

The last attack is relatively simple to mount, according the HomeRF Working Group paper.

> *"… 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…" is relatively "…short, this process can hold off all legitimate activity with a very low duty factor."*

As the authors point out, this type of attack could disrupt a relatively wide area by a single disruptor operating over all eleven 802.11b frequency channels. A single 1-watt power amplifier connected to an antenna placed strategically could disrupt all 802.11 traffic in the area.

HomeRF

The HomeRF Working Group recently ratified the HomeRF 2.0, specification [CHE]. HomeRF 2.0, which operates at data rates up to 10 Mbps, is intended to meet the wireless networking requirements of home users. It reportedly supports toll-quality voice and is claimed to integrate voice, data and streaming media capabilities across a wide range of devices including phones, PDAs, PCs and music and television devices. Its technical capabilities can be summarized as [CHI]:

- 10 Mbps peak data rate with fallback modes of 5 Mbps, 1.6 Mbps and 0.8 Mbps.
- Backwards-compatibility with installed base of HomeRF devices operating at 1.6 Mbps and 0.8 Mbps.
- Simultaneous host/client and peer/peer technology.
- Up to 8 simultaneous prioritized streaming media sessions for audio and video.
- Up to 8 simultaneous toll-quality two-way cordless voice connections.
- "Powerful and differentiating" security measures against eavesdropping and denial of service.

Data Compromise

The HomeRF standard defines 128-bit key encryption, uses a 32-bit IV and sets the time for repeated IV to half a year. HomeRF specifies a IV management procedure designed to minimize the possibility of IV value repetition. HomeRF working group believes that "a brute force attack on HomeRF encryption is inconceivable for organizations without the resources of a government security agency."

Unauthorized Access

All devices compliant with the HomeRF standard make use of a "shared secret" network ID (NWID). The devices will not communicate without this NWID. HomeRF also uses a

frequency hopping physical layer; therefore a client device must synchronize its hopping sequence with the access point in order to receive data. The client must have the correct security NWID in order to synchronize. Without the NWID an unauthorized device will never synchronize, precluding reception of over-the-air data.

The connection process follows the following steps:

- The node chooses a fixed frequency and listens for a period of time.
- Packets are delivered to higher protocol layers from the media access sublayer (MAC) if:
  - The NWID of the receiver matches the NWID of the transmitter.
  - The transmitter has been directed to "teach" the NWID (requires manual intervention) and the receiver has been directed to learn the NWID.
- Other than being directed to teach/learn the NWID, a device obtains the NWID through manual input by an administrator.
- The 24-bit NWID (2^{24} -over 16 million- possible values) essentially prevents unauthorized access to the data stream once client and access point associate.

Because the frequency hopping in HomeRF is not static as it is in 802.11b systems, it is essentially impossible to use commercially available equipment to eavesdrop on a HomeRF network. In fact, specialized equipment would have to be built to eavesdrop and find the HomeRF hopping sequence and subsequently acquire the signal and process it to ultimately decode the NWID for a particular network. This would be such an arduous endeavor and its likelihood is minimal, at best – high cost, low payback.

Denial of Service

Through the combined application of frequency hopping, a different frequency for most access points within a campus setting at any given moment and the fact that the MAC layer does not pass packets from foreign network IDs, a wide scale attack, such as described above, would be virtually impossible with a HomeRF environment.

Conclusion

Because vulnerabilities exist it is always best to protect against data compromise through the use of upper layer protection strategies such as direct data encryption or the use of virtual private networks (VPN). If properly applied such techniques could be effective even if the physical layer is vulnerable to attack as indicated in several of the references cited herein.

However, there appear to be implementations, such as HomeRF, [LAN] that are poised to provide reasonable assurance of confidentiality, authenticity and integrity without the use of these countermeasures. The principal benefit of these implementations is that wireless networks can then be deployed in small offices and homes, where technical staffs are small or non-existent, while allowing users to use their "tools of communication" without fear of compromise.

The following table (from [HOM]) summarizes the comparison of the IEEE 802.11 and HomeRF security features.

Security Area	802.11	HomeRF
Data Compromise	• 40 bit keys • 24 bit initialization vector (IV) • Undefined use of IV • 802.11e will address several flaws in this area.	• 128 bit keys • 32 bit IV • IV management defined
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 a considerable effort • An attack against all networks in an area is virtually impossible

Comparison of HomeRF and IEEE 802.11b Security [HOM]

References

[ANA] Anand, Nikhil, *An Overview of Bluetooth Security*, February 21, 2001, www.sans.org/infosecFAQ/wireless/bluetooth.htm (April 2001)

[ARB] Arbaugh, William A., Skankar, Narendar, Wan, Y. C. Justin, *Your 802.11 Wireless Network Has No Clothes,* March 30, 2001, www.cs.umd.edu/~waa/wireless.pdf (April 2001)

[BOR] Borisov, Nikita; Goldberg, Ian; and Wagner, David. *Security of the WEP Algorithm*. Internet Security, Applications, Authentication and Cryptography (ISAAC), Computer Science Division, UC Berkeley, February 2001, www.isaac.cs.berkeley.edu/isaac/wep-faq.html (April 2001)

[CHE] Cheney, Ann, *HomeRF Working Group Unveils Faster Standard for Multimedia Wireless Networks, May 2, 2001,* http://www.homerf.org/data/press/homerf/homerf20_ratification_50201.pdf (May 2001)

[CHI] Chinitz, Leigh, *HomeRF Technical Overview*, May 9, 2001, www.homerf.org/data/events/past/pubseminar_0501/tech_overview.pdf (May 2001)

[CIS] *Cisco Aironet Security Solution Provides Dynamic WEP to Address Reserachers' Concerns,* Cisco Systems, 2001, http://www.cisco.com (April 2001)

[GEI] Geier, Jim, *Spread Spectrum: Frequency Hopping vs. Direct Sequence,* Wireless-Nets, Ltd., May 1999, www.wireless-nets.com/whitepaper_spread.htm (April 2001)

[HOM] HomeRF Working Group, *A Comparison of Security in HomeRF versus IEEE 802.11b*, 2001, www.homerf.org/data/tech/security_comparison.pdf (May 2001)
[LAN] Lansford, Jim, *HomeRF: Bringing Wireless Connectivty Home,* (May 2001)
[LOU] Lough, Daniel L., Blankenship, T. Keith, Krizman. Kevin J., *A Short Tutorial on Wireless LANs and IEEE 802.11*, 1997
www.computer.org/students/looking/summer97/ieee802.htm (April 2001)
[MEN] Mehta, Princy C., *Wired Equivalent Privacy Vulnerability*, April 4, 2001,
http://www.sans.org/infosecFAQ/wireless/equiv.htm (April 2001)
[RHO] *Wireless Local Area Networks - for the home and office*,
www.rhowireless.com/lans.htm (April 2001)
[WAN] Wang, Sean, *Threats and Countermeasures in Wireless Networking*,
December 20, 2000, www.sans.org/infosecFAQ/wireless/threats.htm (April 2001)
[WLA] *WLANA: the Learning Zone for Wirless Networking*,
www.wlana.org/learn/security.htm (April 2001)
[ZYR] Zyren, Jim and Petrick, Al. *IEEE 802.11 Tutorial*.
www.wirelessethernet.org/whitepapers.asp (April 2001)