I.J. Education and Management Engineering, **2012, 10, 34-38**
Published Online October 2012 in MECS (http://www.mecs-press.net)
DOI: 10.5815/ijeme.2012.10.06

Available online at http://www.mecs-press.net/ijeme

Analysis of Current Wireless Network Security

[a]Gu Jiantao, [a] Fu Jinghong, [b] Wu Tao

[a] College of Science Hebei United University Tangshan, China
[b] Modern Technology and Education Center Hebei United University Tangshan, China

Abstract

Wireless technologies bring great convenience, but they also introduce many new risks and vulnerabilities. Based on explaining the most famous Wireless LAN standard, the 802.11 network security threats and preventive measures are given.

Index Terms: Wireless Network; WLAN; Network security

1. Introduction

A. IEEE 802.11

WLANs are based on the IEEE 802.11 standard, which the IEEE first developed in 1997. The IEEE designed 802.11 to support medium-range, higher data rate applications, such as Ethernet networks, and to address mobile and portable stations.

802.11 is the original WLAN standard, designed for 1 Mbps to 2 Mbps wireless transmissions. It was followed in 1999 by 802.11a, which established a high-speed WLAN standard for the 5 GHz band and supported 54 Mbps. Also completed in 1999 was the 802.11b standard, which operates in the 2.4 - 2.48 GHz band and supports 11 Mbps. The 802.11b standard is currently the dominant standard for WLANs, providing sufficient speeds for most of today's applications. Because the 802.11b standard has been so widely adopted, the security weaknesses in the standard have been exposed. Another standard, 802.11g, still in draft, operates in the 2.4 GHz waveband, where current WLAN products based on the 802.11b standard operate.

Two other important and related standards for WLANs are 802.1X and 802.11i. The 802.1X, a port-level access control protocol, provides a security framework for IEEE networks, including Ethernet and wireless networks. The 802.11i standard, also still in draft, was created for wireless-specific security functions that operate with IEEE 802.1X.

* Corresponding author.
E-mail address: gujiantaolg@126.com

B. HiperLan

HiperLAN (High Performance Radio LAN) is a Wireless LAN standard. It is a European alternative for the IEEE 802.11 standards (the IEEE is an international organization). It is defined by the European Telecommunications Standards Institute (ETSI). In ETSI the standards are defined by the BRAN project (Broadband Radio Access Networks). The HiperLAN standard family has four different versions.

Planning for the first version of the standard, called HiperLAN/1, started 1991, when planning of 802.11 was already going on. The goal of the HiperLAN was the high data rate, higher than 802.11. The standard was approved in 1996. The functional specification is EN300652, the rest is in ETS300836. On the physical layer FSK and GMSK modulations are used in HiperLAN/1. HiperLAN features:

- range 50 m
- slow mobility (1.4 m/s)
- supports asynchronous and synchronous traffic
- sound 32 kbit/s, 10 ns latency
- video 2 Mbit/s, 100 ns latency
- data 10 Mbit/s
- HiperLAN does not conflict with microwave and other kitchen appliances, which are on 2.4GHz.

HiperLAN/2 functional specification was accomplished February 2000. Version 2 is designed as a fast wireless connection for many kinds of networks. Those are UMTS back bone network, ATM and IP networks. Also it works as a network at home like HiperLAN/1. HiperLAN/2 uses the 5 GHz band and up to 54 Mbit/s data rate. The physical layer of HiperLAN/2 is very similar to IEEE 802.11a wireless local area networks. However, the media access control (the multiple access protocol) is Dynamic TDMA in HiperLAN/2, while CSMA/CA is used in 802.11a. Basic services in HiperLAN/2 are data, sound, and video transmission. The emphasis is in the quality of these services (QoS). Good security measures are offered by HiperLAN/2. The data are secured with DES or Triple DES algorithms. The access point and the wireless terminal can authenticate each other.

C. OpenAir

OpenAir is the proprietary protocol from Proxim. As Proxim is one of the largest Wireless LAN manufacturer (if not the largest, but it depends which numbers you are looking at), they are trying to push OpenAir as an alternative to 802.11 through the WLIF (Wireless LAN Interoperability Forum). Proxim is the only one having all the detailed informations on OpenAir, and strangely enough all the OpenAir products are based on Proxim's module.

OpenAir is a pre-802.11 protocol, using Frequency Hopping and 0.8 and 1.6 Mb/s bit rate (2FSK and 4FSK). The radio turnaround (size of contention slots and between packets) is much larger than in 802.11, which allow a cheaper implementation but reduces performance.

The OpenAir MAC protocol is CSMA/CA with MAC retransmissions, and heavily based on RTS/CTS, each contention slot contains a full RTS/CTS exchange, which offer good robustness but some overhead. A nice feature of the protocol is that the access point can send all its traffic contention free at the beginning of each dwell and then switch the channel back to contention access mode.

OpenAir doesn't implement any encryption at the MAC layer, but generates Network ID based on a password (Security ID). This provide some security only because Proxim controls the way all the implementation behave (they don't provide a way to synchronise to any network as 802.11 manufacturers do). OpenAir also provide coarse power saving.

The research supported by Projects of Hebei Province Education Department (Z2010261)

D. HomeRF & SWAP

The HomeRF is a group of big companies from different background formed to push the usage of Wireless LAN in the home and the small office. This group is developing and promoting a new Radio Lan standard : SWAP.

The Home is a good market for Wireless LAN because very few houses are nowadays cabled with Ethernet wire between the different rooms, and because mobility in the home is desired (browse the web on the sofa). The use of the 2.4 GHz band allows a free worldwide deployment of the system.

The HomeRF has decided to tackle the main obstacle preventing the deployment of Wireless LAN : the cost. Most users just can't afford to spend the money required to buy a couple of Radio LAN cards to connect their PCs (without talking of the access point).

The main cost of a radio LAN is the modem. As this is analog and high power electronics, it doesn't follows Moore's law (the market trend that allow you to buy a Cray at the price of a calculator after a few years) and modems tend to be fairly stable in price. Frequency Hopping modems tend to be less expensive, but the 802.11 specification impose tight constraints on the modem (timing and filtering), making it high cost. The SWAP specification, by releasing slightly those constraints, allows for a much cheaper implementation, but still keeps a good performance.

The MAC protocol is implemented in software and digital, so doesn't contribute that much to the final cost of the product (except in term of development cost). Releasing some hardware constraints prevented the use of the 802.11, which anyway was much too complex and including too many features not necessary for the task.

The main killer application that the HomeRF group envisages is the integration of digital cordless telephony and the computing word, allowing the PC to reroute the phone calls in the home or to offer voice services to the users.

A new MAC protocol has been designed, much simpler, combining the best feature of DECT (an ETSI digital cordless phone standard) and IEEE 802.11 : a digital cordless phone and ad-hoc data network, integrated together.

The voice service is carried over a classical TDMA protocol (with interference protection, as the band is unlicensed) and reuse the standard DECT architecture and voice codec. The data part use a CSMA/CA access mechanism similar to 802.11 to offer a service very similar to Ethernet.

E. BlueTooth

Bluetooth is an open wireless technology standard for exchanging data over short distances (using short wavelength radio transmissions) from fixed and mobile devices, creating personal area networks (PANs) with high levels of security. Created by telecoms vendor Ericsson in 1994, it was originally conceived as a wireless alternative to RS-232 data cables. It can connect several devices, overcoming problems of synchronization. Today Bluetooth is managed by the Bluetooth Special Interest Group.

Bluetooth exists in many products, such as telephones, the Wii, PlayStation 3, PSP Go, Lego Mindstorms NXT, iPod Touch and in some high definition watches, modems and headsets. The technology is useful when transferring information between two or more devices that are near each other in low-bandwidth situations. Bluetooth is commonly used to transfer sound data with telephones (i.e., with a Bluetooth headset) or byte data with hand-held computers (transferring files).

Bluetooth protocols simplify the discovery and setup of services between devices. Bluetooth devices can advertise all of the services they provide. This makes using services easier because more of the security, network address and permission configuration can be automated than with many other network types.

2. network security threats

Most threats against wireless networks involve an attacker with access to the radio link between wireless devices. Several of the threats listed in following rely on an attacker's ability to intercept and inject network communications. This highlights the most significant difference between protecting wireless and wired networks: the relative ease of intercepting wireless network transmissions and inserting new or altered transmissions from what is presumed as the authentic source.

- Denial of Service: Attacker prevents or prohibits the normal use or management of networks or network devices.
- Eavesdropping: Attacker passively monitors network communications for data, including authentication credentials.
- Man-in-the-Middle: Attacker actively intercepts the path of communications between two legitimate parties, thereby obtaining authentication credentials and data. Attacker can then masquerade as a legitimate party.
- Masquerading: Attacker impersonates an authorized user and gains certain unauthorized privileges.
- Message Modification: Attacker alters a legitimate message by deleting, adding to, changing, or reordering it.
- Message Replay: Attacker passively monitors transmissions and retransmits messages, acting as if the attacker were a legitimate user.
- Traffic Analysis: Attacker passively monitors transmissions to identify communication patterns and participants.

3. Loopholes in existing security protocol

At the beginning of the WLAN design, security has been taken into account in its design. With the appearance of 802.11b, WEP also has been recognized by people. However, the serious loopholes in WEP [2] had become objects of attack. In order to overcome the shortcomings of the current wireless security measures, especially WEP, the 802.11i standard was created. The new standard contained much better ways to provide security, However, 802.11i is not perfect. The major WEP design flaws may be summarized as follows (Gast, 2002, pp. 93-96):

- Manual key management is a big problem with WEP. The secret key has to be manually distributed to the user community, and widely distributed secrets tend to leak out as time goes by.
- When key streams are reused, stream ciphers are vulnerable to analysis. Two frames that use the same IV are almost certain to use the same secret key and key stream, and this problem is aggravated by the fact that some implementations do not even choose random IVs. There are cases where, when the card was inserted, the IV started off as zero, and incremented by one for each frame. By reusing initialization vectors, WEP enables an attacker to decrypt the encrypted data without ever learning the encryption key or even resorting to high-tech techniques. While often dismissed as too slow, a patient attacker can compromise the encryption of an entire network after only a few hours of data collection.
- WEP provides no forgery protection. Even without knowing the encryption key, an adversary can change 802.11 packets in arbitrary and undetectable ways, deliver data to unauthorized parties, and masquerade as an authorized user. Even worse, an adversary can also learn more about an encryption key with forgery attacks than with strictly passive attacks.
- WEP offers no protection against replays. An adversary can create forgeries, without changing any data in an existing packet, simply by recording WEP packets and then retransmitting later. Replay, a special type of forgery attack, can be used to derive information about the encryption key and the data it protects.
- WEP misuses the RC4 encryption algorithm in a way that exposes the protocol to weak key attacks and public domain hacker tools like Aircrack, and many others exploit this weakness. An attacker can utilize

the WEP IV to identify RC4 weak keys, and then use known plaintext from each packet to recover the encryption key.

- Decryption dictionaries, which consist of a large collection of frames encrypted with the same key streams, can be built because of infrequent rekeying. Since more frames with the same IV come in, chances of decrypting them are more, even if the key is not known or recovered.
- WEP uses CRC for integrity check, encrypted using RC4 key stream. From a cryptography view point, CRC is not secure from an attack of frame modification, where the attacker modifies the frame data contents as well as the CRC value.

4. Some preventive measures

- Strengthening network access control
- Review website regularly
- Strengthening security certification
- Network testing
- Assign static IP to MAC address
- Reliable encryption protocol
- Isolate wireless network from core network

References

[1] US-CERT. “Using Wireless Technology Securely”. 2006. http:// www.us-cert.gov/reading_room/Wireless-Security.pdf

[2] N.Borisov, I.Goldberg, D.Wagner, "Intercepting Mobile Communications: The Insecurity of 802.11.", http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf , Published in the proceedings of the Seventh Annual International Conference on Mobile Computing and Networking, July 16-21, 2001.

[3] Gast, M. (2002) Wireless LAN security: A short history. Retrieved July 25, 2005, from http://www.oreillynet.com/pub/a/wireless/2002/04/19/security.html

[4] Gast, M. S. (2002). 802.11wireless networks: The definitive guide. CA: O’Reilly Media.