Wireless LAN – Security Issues

Petter Edström, Zhao Zhengjian

Royal Institute of Technology

Stockholm, Sweden

{pettered, zzha}@kth.se

***Abstract*—Wireless Local Area Networks, also known as Wireless LANs, are increasingly popular among modern users of data communication. However, the security aspects of these network installations are often overlooked, neglected, or quite simply not taken seriously for sake of convenience and simplicity. This paper provides a brief insight into these matters.**

Keywords—Wireless LAN, Security

I. Introduction

A. *Background*

As part of the course 2G1704 – Internet Security & Privacy, a written assignment with a rather limited scope shall be presented, handling a predefined topic of interest for a group of two students. In this case the chosen topic was “Wireless LAN - Security Issues”.

B. *Outline*

This paper describes some security properties of wireless local area networks. However, this paper only handles networks based on the IEEE 802.11 standards [1], commonly known as Wireless Fidelity or Wi-Fi networks. Section II handles the basics of a wireless network configuration. In section III the security issues of using an over-the-air-interface while transmitting information are handled. Finally, conclusions are drawn in section IV.

II. Local Area Network Basics

A. *Wireless LAN Technologies*

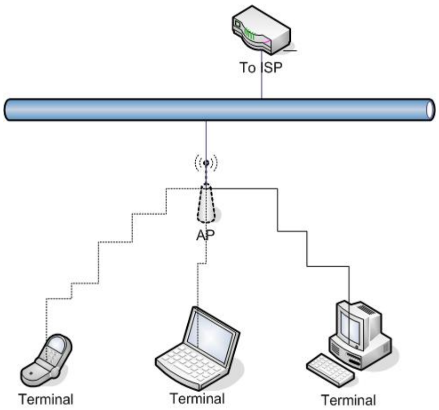
Wireless Local Area Networks are based on the IEEE standards 802.11x that were accepted in 1997 [1] (not to be confused with IEEE 802.11X which is used for port-based network access/admission control). A number of subchapters of 802.11 are applicable to modern Wireless LANs, however 802.11a, 802.11b and 802.11g are currently most widely used, providing theoretical data rates ranging from 11 Mbps (802.11b) to 54 Mbps (802.11a and 802.11g). 802.11a uses the 5GHz frequency band and a modulation technique called FHSS [2]. 802.11b and 802.11g operate on the 2.4 GHz frequency band with the modulation technique DSSS [3]. The details of the modulation schemes are however outside the scope of this paper.

A lower frequency (used with 802.11b/g) ensures better radio propagation properties resulting in better coverage. However, the 2.4 GHz frequency band is also used by microwave ovens and Bluetooth devices that increase the risk of interference during wireless LAN transfers. Which frequency band (802.11a/802.11g) technique to choose for higher data rates is a complex issue depending on a number of factors; user density (many users over a limited bandwidth renders lower throughput), device compatibility (there are specific processing and power requirements for 802.11a capable devices), and the potential interference from other technologies using the same frequency band.

Currently there is work ongoing to standardize a new 802.11 subchapter called 802.11n that aims to standardize the details for data rates of up to 600 Megabits per second. Due to a conflict of interests between two groups of companies each trying to put forth a separate standard, an alliance has recently been created in an effort to merge the many ideas in this area [4]. Hopefully this work will result in inter-operability between the 802.11a and –b/–g standards. 802.11n will likely specify the use of spatial multiplexing which enables reception and transmission over one to four antennas simultaneously.

B. *Initial Set-up*

Wireless LANs consist of two main components, wireless clients and access point. The client can be a wireless notebook, or for that matter any computer with a wireless card. The access point (AP for short) is the center of a wireless network. Its function is like that of a router, only with a radio transceiver. The AP may also have Ethernet ports for wired cable connections. See picture 1.



Picture 1: Wireless Network Setup

To set up a wireless LAN you first need to configure the AP. Then there are a few concepts to keep in mind;

1) SSID: the Service Set Identifier (often referred to as Network Name) is sent in packet headers over a Wireless LAN and used to distinguish one AP from another. Clients trying to connect to one AP must all use the same service set identifier.
2) Channel: A channel number defines which frequency that should be used to provide the wireless connection service. It is advisable to choose it differently from the default setting.
3) Mode: it decides what transmission capabilities the AP will use, usually there are up to 11 Mbps (802.11b) and up to 54 Mbps (802.11g) to choose from.

After the configuration of the AP, the clients can detect that a wireless network with the given SSID exists, and connect to it using the specific configuration of the client software.

The AP can be set up to accept a limited number of clients, in an attempt to restrict access to the wireless networks that has been set up. The technique is called MAC filtering and is discussed further in a later chapter.

III.Security Issues for Wireless LANs

A. *How Easy is it to Listen in on WiFi Systems?*

As mentioned in the description of techniques used to secure data transmission over the radio interface, there are security flaws in almost every encryption methodology and algorithm available. One needs to consider both the integrity and privacy aspects of a connection when choosing algorithms and the methods with which they are used. The time and effort needed for an intruder to destroy the service or listen in on and alter the transferred data are other aspects that are crucial when selecting a sufficiently effective but not too complex and time-consuming algorithm.

Although many attacks can be preventing using up-to-date hardware and software, most every-day users are subject to de-authentication and disassociation attacks, some time referred to as MIC Denial-of-Service (DoS) attacks, via the use of unauthorized access points. An intruder can impersonate the access point's MAC address and tell connected LAN users to disconnect from the network (via a de-authentication message). This causes all users to be disassociated with and lose the service of the network.

By telling users that they need to re-locate to a different access point, a potential attacker can also make users reconnect to an access point that they control. With control over several users, man-in-the-middle attacks can take place, providing control over desired networks.

Other potential risks for such intrusions are mischievous intra-net users. Is it relatively easy for an intra-net user to grant access to external non-authorized users, by simply setting up an additional access point.

B. *What Measures are Taken to Prevent Attacks?*

Every 802.11 standard specifies one or several security algorithms to be used in order to prevent attacks on ongoing data transmissions.
This section of the paper handles but a few, however hopefully interesting and useful techniques.

MAC filtering

MAC (Media Access Control) filtering is a low-level security technology. Since all wireless cards have their own unique MAC address, the access point in question can set up a predefined list of all the MAC addresses that are allowed to set up a wireless connection towards that specific access point.

WEP

Wired Equivalent Privacy, WEP was as the name implies initially intended to provide the security level of a network using wired cables. However, wireless LANs use radio waves which first of all means that the network cannot be protected in the same way as a physically confined network using cabling inside a building. Since WEP is designed to use only the two lowest layers of the OSI-model [5], no end-to-end security is provided. The authentication part of WEP is not much to speak of and the algorithm itself was considered weak already in the beginning of the standardization of IEEE 802.11.

The flaws of WEP ignited work on a security standard call 802.11i (also known as WPA2). However, creating standardized enhancements that required hardware upgraded devices (for improved security), is a very lengthy process. In the meanwhile, the WPA protocol was developed by the WiFi Alliance [8], as a stepping-stone from WEP towards safer encryption techniques.

WPA

WPA (Wi-Fi Protected Access) has been designed as a software upgrade in WEP-capable hardware to make up for the shortcomings of WEP, still keeping the ongoing 802.11i standardization work in mind. Basically WPA was designed based on 802.11i, with the exception of the AES encryption algorithm (that requires powerful hardware implementations). Mainly two things stand out as improvements in WPA; enhanced data encryption using the TKIP protocol [6], and user authentication through the EAP protocol [7].

Even though 802.11i now is finally standardized, the equipment based on the older versions of 802.11 will likely be around for many years more. This will mean that WPA will be used quite extensively for some time still.

802.1X Port Based Network Access Control

Port-based Network Access or Admission Control provides authentication for devices on a specific LAN port and makes sure that that LAN port is closed if the authentication should fail. The technique is thus used when an access point needs to be a closed access point (see the section on WEP security). A stand-alone RADIUS server [14] is usually handling the actual (mutual) authentication of both sender and receiver.

The EAP protocol is used as a basis for authentication (Extensible Authentication Protocol). It supports a wide variety of authentication methods, for example certificated-based authentication, smartcards, token cards, one-time passwords, et c. Since EAP merely is a framework and not specific software, new authentication methods can be added without the need to upgrade the switch or access point, by adding software on both host and the authentication server.

C. *How well Do Taken Security Measures Work?*

MAC filtering

A MAC address can be impersonated using software a simple software tool [15]. This means that the list of approved MAC addresses stored in the AP would need to be updated on a regular basis to reduce the risk of unauthorized LAN usage towards that AP.

WEP

As an encryption method, WEP is not very effective nor very safe. WEP has for some time been known to be relatively unsafe and even cracked [9]. It could be argued that the algorithm for many applications would be safe enough in that it would make a potential intruder choose a different point of attack for convenience, although the encryption key itself is easy to decrypt. However, the use of other more advanced algorithms (like WPA or IEEE 802.11i-compatible improvements that will be described shortly) are strongly recommended.

WPA

The basic set-up of a session using WPA involves a so called session key that needs to be created and verified There are mainly two types of attacks that one needs to consider in details before trusting your deepest secrets with WPA encryption on a wireless LAN; the WPA-PSK password attack and the MIC DoS threat. The latter has been described in section III A.

In pre-shared key mode (for non-commercial use), a master key needs to be used by both the client and the AP in order to set up a session key used on both sides. If a short password (< 21 characters if you ask the WiFi Alliance) is used, an offline dictionary attack can easily be performed. If that happens at the same time as a de-authentication/disassociation attack (see chapter III B), the damage done can be even more severe.

More details on the WPA-PSK password attack are described in [12].

In addition to this, it needs to be considered that RC4, a symmetric key streaming cipher that has been used for many years, is still used with WPA. The used key can, depending on the chosen key-length, be cracked using brute force (in terms of time and processing power). This means that 802.11i compliant devices should be the aim for all applications claiming to have integrity and security.

802.1X Port Based Network Access Control

Even though the authentication protocol EAP is a versatile frame work which results in lots of ideas for authentication methods that make use of EAP, wireless authentication requirements are met by only a few of these. Based on [11], a few methods are proposed for Wireless LANs using EAP as authentication [10]. It should be noted that several of these standardization RFCs (Request For Comments) are still in draft versions, hence not yet approved Internet community standards.

IV.SUMMARY AND CONCLUSIONS

A. *Summary*

A number of techniques for authentication and privacy and their security flaws are described briefly; MAC filtering, WEP, WPA, WPA2 and Port Based Network Access/Admission Control.

Generally, there are lots of people studying the wireless network security issue at present, not only the experts who designed them, but also lots of people who are interested in more general terms. As more advanced security techniques emerge, so do the techniques to crack them. A collection of vulnerabilities are identified in [13].

Despite these, there are ways of using a non-commercial wireless connection with a reasonable amount of both privacy and security. However, the concept of “the weakest link” needs to be considered so that the efforts of ensuring safety are concentrated to when and where attacks are most likely to occur, or so that transferred data no longer is of importance in case of an attack.

B. *Conclusions*

We have introduced common security issues existing in a wireless network. Maybe there is nothing really secure on earth, so when we talk about “the security issue”, we will always face the dilemma of security and the cracking thereof.

When discussing wireless network security, one would assume that potential intruders have the advantage, since a wireless signal is a lot easier to listen too, physically. However, very likely there are theoretically sufficient means of wireless security.

Making a problem is always much easier than solving one. However, given that long, coded abbreviation passwords are used at the same time as the 802.11i standard is followed and pre-shared keys are changed on a regular basis, any mischievous activities will probably not succeed when transferred data still is of interest. At least not on your wireless network…

REFERENCES

[1] IEEE Website, “802.11”, Accessed on November 12, 2005 from URL: http://grouper.ieee.org/groups/802/11/

[2] Webopedia Website, “What is OFDM”, Accessed on November 12, 2005 from URL: http://www.webopedia.com/TERM/O/OFDM.html

[3] Webopedia Website, “What is DSSS”, Accessed on November 12, 2005 from URL: http://www.webopedia.com/TERM/D/DSSS.html

[4] The Enhanced Wireless Consortium Website, Accessed on November 12, 2005 from URL: http://www.enhancedwirelessconsortium.org/home

[5] Behrouz A. Forouzan, ”TCP/IP Protocol Suite”, 3rd International Edition, Published by McGraw-Hill

[6] Informit.com Website, “Security Reference Guide - TKIP”, Accessed on November 13, 2005 from URL: http://www.informit.com/guides/content.asp?g=security&seqNum=75&rl=1

[7]The Internet Engineering Task Force, Request For Comments, RFC 2284, Accessed on November 13, 2005 from URL: http://www.ietf.org/rfc/rfc2284.txt

[8] WiFi Alliance Website, Accessed on November 13, 2005 from URL: http://www.wi-fi.org/OpenSection/index.asp

[9] Article Provided Courtesy of Prentice Hall PTR, “Cracking WEP”, Accessed on November 13, 2005 from URL: http://www.informit.com/articles/article.asp?p=27666&seqNum=1

[10] The Unofficial 802.11 Security Web site, Accessed on November 19, 2005 from URL: http://www.drizzle.com/~aboba/IEEE/

[11] The Internet Engineering Task Force, Request For Comments, RFC 4017, Accessed on November 19, 2005 from URL: http://www.ietf.org/rfc/rfc4017.txt

[12] Wi-Fi Net News, “Weakness in Passphrase Choice in WPA Interface”, Accessed on November 19, 2005 from URL: http://wifinetnews.com/archives/002452.html

[13] The website of William A. Arbaugh at the University of Maryland, USA, “802.11 Security Vulnerabilities”, Accessed on November 19, 2005 from URL: http://www.cs.umd.edu/~waa/wireless.html

[14] The Internet Engineering Task Force, Request For Comments, RFC 2548, Accessed on November 22, 2005 from URL:http://www.freeradius.org/rfc/rfc2548.html

[15] The KLC consulting Website, “The SMAC tool”, Accessed on November 22, 2005 from URL: http://www.klcconsulting.net/smac/