A proposed scheme for securing IEEE 802.11 wireless LANs

I Pavlosoglou, T Stergiou, M S Leeson and R J Green

Communications & Signal Processing Group, School of Engineering, University of Warwick, UK

Abstract: The objective of this paper is to provide an overview of a protocol implementation, based on a public key infrastructure, for securing the current IEEE 802.11 standard. Taking into account the known vulnerabilities, in terms of the different types of attack that this standard suffers from, we aim to provide an alternative to the traditional architecture that has been proposed by task group b. Finally, bearing in mind the continuous need for securing this medium and the on-going efforts of task group i, we provide a short description of a protocol architecture that has been found appropriate for facilitating our security model.

1 Introduction

The continuous emergence of mobile devices in daily life has necessitated the use of wireless techniques for communication between them. In this rising demand for service availability to non-fixed users with varying locations, achieving the same level of connectivity but without the presence of a physical link has proven to be a substantial challenge. Both industry and academia have expended considerable effort in the search for functioning, clean-cut implementations encompassing modulation techniques and spectrum availability, bandwidth requirements and protocol standardisation.

Following the increasing demand for standardisation in this field, the IEEE project 802 committee (motivated by the US Federal Communications Commission (FCC) decision to release the use of the industrial, scientific and medical (ISM) bands to the public) established working group IEEE 802.11. The objective was to develop a Medium Access Control (MAC) and Physical layer (PHY) specification for wireless connectivity in fixed, portable and mobile stations within a local area. As a result, the 802.11 standard for Wireless Local Area Networks (WLANs) was first published in 1997 [1], with a number of supplementing implementations (named 802.11a to 802.11g) released since then.

Having as an objective the offering of the connectivity of the 802.3 IEEE Ethernet standard [2], 802.11 sets quite a high level of requirements for a protocol that works over no specific medium. It is a standard that can operate via either Radio Frequency (RF) or Infrared (IR) transmissions, depending on the physical layer present. Also, it can either be based on Direct Sequence Spread Spectrum (DSSS) or Frequency Hopping Spread Spectrum (FHSS) technique in the 2.4 GHz RF band, as well as on Pulse Position Modulation (PPM) when utilising an IR channel [3].

Further to the development of the original standard, a number of task groups have been established with responsibilities for enhancing the capabilities of 802.11 [4]. Each focuses on a specific area (e.g. task group i wants to improve security in the current 802.11 MAC), which aims to overcome the problems that have been outlined to define their existence.

From this ongoing effort, it is clear that the transition from wired to wireless is proving to be quite demanding. In the development of this standard, the prime objective has been to offer networking capabilities in a wireless fashion and so far this has been a success. However, as a direct result of this other issues have been neglected and one of these is security. Consequently, it appears that one of the current drawbacks of upgrading to wireless is the lack of the provision of secure connections to do so. In this paper, we offer an overview of the most representative security problems that the current standardized versions of 802.11 (namely a, b and g) suffer from. Furthermore, motivated by the ongoing work of task group i, we propose a scheme based on a previously known security infrastructure, with the objective of bridging the gap that has been created in protecting WLAN communications.

2. A security overview of the 802.11 standard

This section aims to provide a brief overview of the security disadvantages of 802.11, together with information regarding different attack types that can compromise the integrity of the system. The basis of our discussion is centred on a single user model, where a wireless client is attempting to access a stationary server via an access point, which is part of the wired network infrastructure. This model (as presented in Figure 1) illustrates a typical WLAN topology, created to emulate the functionality supported by the 802.11 standard. Consequently, we can categorise the types of attack on the network into two main categories. The first one encompasses issues regarding the wireless network, whilst the second entails details of the protection of the wired network.

For the wireless access network, several attacks have been described in relation to the authentication techniques of 802.11 [5-7]. The WEP[1] protocol uses a challenge-response mechanism for mutual authentication, with the random challenge sent in cleartext format. An attacker could masquerade as a legitimate Access Point (AP) to disclose information sent in the user packets, intercept those denying their transmission or deceive the sender in sending vital information towards the AP. Furthermore, there exists the possibility that messages may be sent authenticated but not encrypted and similarly encrypted but without validating the legitimacy of the client. There is no point in authenticating information without affording message integrity, and encryption without authentication does not guarantee the legitimacy of the sender. If the attacker is able to breach the integrity of the transit data, he/she will be able to disclose information regarding the user identification.

Weaknesses identified for the proposed RC4 stream cipher [11], increase the possibilities that such attacks will be successful. Finally, the choice of the CRC-32 checksum as the Integrity Check Value (ICV) used by WEP, leaves the network susceptible to further manipulations [12]. CRC-32 is a linear function, and hence can be reversed, revealing the information used to produce the checksum. By altering the contents of the data and that of the ICV value, an attacker will be able to forge messages as valid, given the verification of the illicit checksum at the receiver.

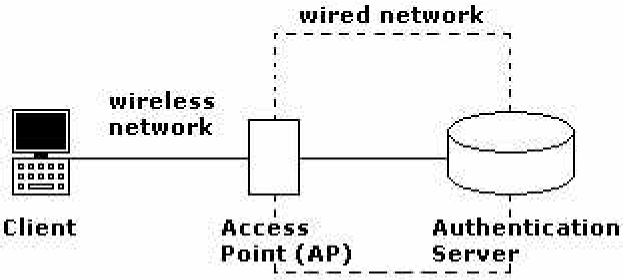

Figure 1: WLAN topology

Of importance for our proposal are the access control pitfalls of the WLANs when operating in ad-hoc mode. In this method, clients are directly communicating with each other, eliminating the need for an AP. Whenever a client wishes to communicate with another node outside the cell perimeter, then another client is used to route the user messages. Problems can arise by malicious nodes, which either interrupt the connection by dropping the packets, or modify those altering their contents. In the former case, the illicit client is successful in launching a Denial of Service (DoS) attack. In the latter case, even if messages are encrypted, the vulnerabilities of the WEP will result in the attacker distorting the data at will.

In relation to the wired network part, an attacker could monitor the communication of the AP and authentication server obtaining information concerning secret keys and IV. The provision of Virtual Private Networks (VPN) that has been suggested to secure these associations [13] is limited by the lack of a functional public-key infrastructure and a universally accepted IPsec implementation. When a VPN is established with the client, it is clear that on-demand network access cannot be achieved, since the scheme can only be offered to users who are already known. In the following section, we present our proposal for securing WLAN systems, overcoming the pitfalls associated with the existing standards.

3. Filling in the gaps of 802.11

As seen in the previous section, the first attempt to incorporate security (through the WEP protocol) into the 802.11 standard has been unsuccessful. From key re-usage in the ciphertext, to weaknesses in the chosen algorithm and lack of key management (to say nothing of issues of authentication) prospective attackers have a wide range of options for compromising the security of the network. The concept of a protocol that can offer the equivalent security of wire (which we know how to bypass) has left us with a scheme lacking any security to a basic intelligent attack.

As a starting point in our proposal for securing WLANs, we begin by acknowledging the presence of a central authority in the authentication server (Fig. 1) on the network, having the ability of identifying all data travelling across the network. Consequently, a way of recognising each individual client is required. This does not imply that all clients should be previously known to the server, as this would substantially reduce the ad-hoc nature of

[1] The second implementation of the 802.11, namely 802.11b, describes a security protocol that utilises a form of encryption called Wired Equivalent Privacy (WEP). This protocol, despite of aiming to provide confidentiality, user authentication and data integrity in the wireless channel [8], fails to enforce all three of these requirements [9], due to the misinterpretation of some cryptographic primitives [10], in the design.

the wireless network. Each client should uniquely be identifiable on the network, through the information it exchanges on it. For this to take place, a Public Key Infrastructure (PKI) as a way of managing public keys under a Certification Authority (CA) would be required. To join the PKI, a client would generate a public/private key pair and keeping the private key secret, publish the public key to the CA for signing. When transmitting information to another client, not necessarily in the presence of an AP, all data exchanged could be traced back to its original sender.

Implementing a PKI at a LAN level is a feasible task in the presence of a CA but leaving the implementation at that level could result in a malicious user, who, having obtained its public key certification, roamed the network causing damage. This is equivalent to signing a postal service special delivery to a ticking bomb. You accept the parcel because you trust the postal service, but neither you nor the postal service can guarantee the quality of the contents you receive. As a result, we can see that a PKI is not enough to secure WLANs.

In order to tackle this issue, we introduce the concept of access levels on the network. A user, upon requesting certification on the network, receives a *Level of Operation (LOP)* incorporated into the signature from the CA, initially granting him enough rights to access the network and communicate with other devices. The objective of the LOP is to act as an independent monitoring currency [14] on the network. Since, as a PKI prerequisite, each client has to sign all traffic placed on the network for it not to be ignored by others, a receiving host can simply look up the LOP of any client from the signature of the CA. Consequently, due to the passive nature of incoming communications in WLANs, by introducing the concept of LOPs, each client still has the ability to act freely on the network, but how serious their requests will be processed, will depend on their LOP defined by the CA.

Furthermore, each user will have the ability to report back to the CA about the performance of other clients. By placing requests regarding what they believe the LOP of specific users should be, they would enable the CA to further decide in upgrading or downgrading LOPs of specific users. If we assume the LOP to have single byte length, with 0 being the minimum and 7 the maximum, a weighted vector could be used to derive the new LOP, as shown in Equation (1).

$$LOP_1^{new} = \frac{1}{7\left(n+1\right)}\left(LOP_2 \times LOP_1^2 + LOP_3 \times LOP_1^3 + ... + \left(LOP_1^{old}\right)^2\right) \quad (1)$$

Where: $LOP_1^{new/old}$ is the respective new and old LOP of host 1.

LOP_1^2 is the suggested LOP of host 1, by host 2.

n is the total number of hosts who have submitted a request to the CA.

All mathematical operations are assumed to be integer based, rounded to the smallest integer within the byte range. Since the new LOP evaluated by the CA depends on the number of feedback requests received, a further point worth establishing would be the minimum threshold for Equation (1) to apply. This would be network specific, dependant on the number of hosts (on average) utilising the network, as well as the amount of traffic being produced. Finally, due to the overhead created by this traffic, special considerations would have to be made regarding the slotted times that this information exchange would take place.

The FCNS reference architectural framework [15] has been chosen to securely transmit the LOP parameter to the authentication server and clients. FCNS is a protocol stack designed to overcome disadvantages of the OSI security model and to provide a simple and easy to manage security architecture. The model has also been developed to counter attacks and implementation pitfalls of standardised network protocol architectures, such as the IPsec [16].

The idea of using the FCNS as the means of transferring the required security parameters to the AP and authentication server lies on the flexibility of the protocol to support a wide range of security mechanisms. Its use entails the compatibility of vendor-specific systems and at the same time the removal of the systems' independence to already exploited architectures such as the IP. The principles governing the operation of the FCNS lie on the placement of the stack security functionality into a single layer, namely the Security Layer (SL). The provision of the SL signifies the security of the communication process at any desired level, without the need of additional protocols to support the protection of a specific protocol layer.

As a consequence, the LOP could be transmitted with the highest possible protection levels, ensuring that only the legitimate network nodes are made aware of the communication. The transmission of the LOP information could be piggybacked into the FCNS frames, decreasing the network latency that would built up due to the redundant data. When the wireless links are idle, the traffic padding mechanisms of the FCNS could ensure a degree of protection against passive monitoring and traffic analysis attacks.

4. Conclusions

In this paper, the 802.11 security features have been presented, with emphasis being given on the disadvantages and implementation pitfalls of the proposed architecture. The problems associated with the deployment of 802.11b and consequently WEP protocol render WLANs security defective.

To provide a more flexible and adequate security solution, the IEEE committee and the Wi-Fi alliance developed the 802.11i standard, implementing the Wi-Fi Protected Access (WPA) system. The WPA protection scheme supports stronger authentication and encryption mechanisms, to counter known WEP vulnerabilities. The problems with this proposal lie on the use of the WEP encryption techniques and the fact that further cryptographic updates may reflect on the existing hardware equipment. Stronger ciphers will result in necessary upgrades to compensate for the enhanced processing requirements of algorithms such as the Advanced Encryption Standard (AES). Furthermore, the deployment of such a scheme strongly depends on its acceptability by WLAN vendors, pending any future standardisation by the IEEE.

To address the need of ad-hoc WLAN security, we have proposed an access control scheme based on the level of operation of each client, given a functional PKI. Users communicate with the CA parameters regarding the behaviour of each network node, which will in turn decide upon the assignment of resource access privileges. Depending on the LOP value, users will be granted access to forward information into the WLAN, or act as intermediate routers in case information needs to be transferred outside the network boundaries.

Due to the importance of the information in transit, we have also proposed the FCNS reference architecture as the transport mechanism of the respective certification. FCNS provides for the security of the stack structure at all possible levels of the communication, depending on the administrator demands and the environment on which the protocol runs. Its design enhances the flexibility of the system in reflecting network system and cryptographic advances and, at the same time offers a simple managed network solution. Its advantages over currently used architectures make it a strong candidate for client information delivery over a diverse network.

References

[1] Institution of Electrical and Electronic Engineers (IEEE), *Wireless LAN Medium Access Control (MAC) and Physical layer (PHY) specification*, LAN MAN Standards of the IEEE Computer Society, IEEE Standard 802.11, 1997.

[2] J F Kurose, *Computer networking: a top-down approach featuring the Internet*, Addison Wesley, pp. 415-427, 2001.

[3] B O'Hara and A Petrick, *The IEEE 802.11 Handbook: A Designer's Companion*, Standards Information Network IEEE Press, 1999.

[4] P Nicopolitidis, M S Obaidat, G I Papadimitriou and A S Pomportsis, *Wireless networks*, Wiley, 2003.

[5] J. Weiss, *Wireless networks: Security problems and solutions*, SANS Information Security Reading Room, SANS Institute, 2002.

[6] J. Craiger, *802.11, 802.1x and wireless security*, SANS Information Security Reading Room, SANS Institute, 2002.

[7] W. Arbaugh, N. Shankar and Y.C. Wan, *Your 802.11 wireless network has no clothes*, Department of Computer Science, University of Maryland, USA, 2001.

[8] I Goldberg, *An analysis of the Wired Equivalent Privacy protocol*, Black Hat briefings, http://www.cypherpunks.ca/bh2001/mgp00001.html, University of Berkeley, 2001.

[9] J R Walker, *IEEE P802.11 Wireless LANs Unsafe at any key size: An analysis of the WEP encapsulation*, IEEE 802.11 Committee 802.11-00/362, 2000.

[10] N Borisov, I Goldberg and D Wagner, *Security of the WEP algorithm*, University of Berkeley, http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html, 2001.

[11] N. Borisov, I. Goldberg and D. Wagner, *Intercepting mobile communications: the insecurity of 802.11*, Proc. of the 7th Annual International Conference on Mobile Computing and Networking, July 16-21, 2001.

[12] K. Tyrrell, An *overview of wireless security issues*, SANS Information Security Reading Room, SANS Institute, 2003.

[13] P. Congdon, *Edge Access Security*, HP Invent, WCNC 2003, New Orleans, USA, 2003.

[14] I Pavlosoglou, M S Leeson and R J Green, *Towards bottom-up network architectures*, Proceedings of the 4th annual postgraduate symposium PGNet 2003, pp. 21-24, 2003.

[15] T Stergiou, R J Green and M S Leeson, *Protocol Stack Design for 3rd Generation Mobile Systems - UMTS Core Network*, Proc. of the Third International Network Conference 2002, July 2002.

[16] N. Ferguson and B. Schneier, *A cryptographic evaluation of IPsec*, Counterpane Internet Security Inc, Feb. 1999.