IPSec Implementation for a Better Security in IEEE 802.11 WLANs

Nadia Issa and Chris Todd
Department of Electronic & Electrical Engineering
University College London, U.K.

Abstract: *This paper gives an overview of IPSec implementation in IEEE 802.11 WLANs.*
The first part presents an overview of the IEEE 802.11 standard for WLANs, and highlights its current security weaknesses.
The second part gives an overview of the IPSec security architecture, with a brief description of its protocols and implementations.
The third part discusses the design decisions taken throughout the protocol's implementation for the wireless LAN's users, and presents the proposed solution for securing IEEE 802.11 WLANs by using IPSec.

1. Introduction:

Over the years, there has been a growing interest in wireless networking, so technology developers gave it a high importance. But with every new technology developed, some limitations were presented, specifically on the security level.
Although the Institute of Electrical and Electronics Engineers (IEEE) 802.11 standard provides a kind of protection using the Wired Equivalent Privacy (WEP) protocol, it still has a significant problem in security. The IEEE established a task group i to improve the standard and solve its security problems, meanwhile, several alternative security measures could be used to secure wireless networks based on 802.11 [1]
In this paper, Internet Protocol Security (IPSec) is proposed as a solution. It is the best protocol that can secure almost any internet traffic, protects against eavesdroppers, data modification, and unauthorized access.

2. Overview of IEEE 802.11 Standard:

The 802 standard was set by the IEEE to define networking connections for the interface card and the physical connections in Local Area Networks (LAN). [2]
The 802 is a project to develop LAN and Metropolitan Area Network (MAN) standards, started with establishing a work group in the IEEE computer society, and added other work groups by time, each group has a different working area (or standard) and a different number, for example group 1 which is the High Level Interface (HILI) working group works on standard 802.1, and group 11 which is the Wireless LAN (WLAN) working group works on standard 802.11, and so on...
The IEEE 802.11 standard is used for wireless Ethernet networking, its scope is to develop a Medium Access Control (MAC) and physical layer (PHY) specification for wireless connectivity for fixed, portable, and moving stations within a local area. [3]
The initial release of the 802.11 is capable of transmissions of 1 to 2 Mbps and operates in the 2.4 GHz band, different versions were released with different capabilities, and the most three deployed protocols are:

- IEEE 802.11a which transmits up to 54 Mbps, and operates in the 5 GHz band.
- IEEE 802.11b (also known as Wi-Fi) which transmits up to 11 Mbps, and operates in the 2.4 GHz band.
- IEEE 802.11g which transmits up to 54 Mbps, and operates in the 2.4 GHz band.

The 802.11 has two important operating modes: Ad-Hoc mode or Independent Basic Service Set (IBSS); in which all traffic travels peer to peer, this is a point-to-point operating mode, and infrastructure (cellular) mode or Basic Service Set (BSS); in this latter all traffic travels

through a central point called the Access Point (AP), which is responsible for all communications. Stations recognize their BSS using the BSSID, which is diffused by the AP through broadcasting. [4]
Although this type of network is flexible, easy to deploy, economic and interoperable with wired networks, it has a significant problem that puts security at fault, which is the lack of medium control. Any antenna placed in the volume of emission can collect radio transmission. This weakness in medium control is the base of a number of threats like: weakness in availability (Jamming and logical denial of service), weakness in access control and in integrity (identity usurpation and message modification), and weakness in confidentiality (by passive listening).
The 802.11 standard was not unconscious of all problems previously mentioned, so it did not leave this new technology proof without any kind of protection. It thus proposed a solution named Wired Equivalent Privacy (WEP) which is a protocol that was supposed to make the wireless networks as secure as the wired ones, to ensure the following three security services: access control, integrity and confidentiality [3], but it failed in doing so and encountered several problems in security.
Against these failures in the security mechanisms, the research for intermediate solutions was necessary. To mitigate these insufficiencies in security, a task group called 802.11i has been formed within the IEEE to enhance the current 802.11 MAC, to provide improvements in security. [5]
The 802.11i group proposed two solutions to solve the common problems of wireless security: a transit solution and a final solution. The 802.11i standard can assure an acceptable level of safety and provide a robust solution, but this is not implemented till now.
Since the WEP is not sufficient and the 802.11i is not in use yet, an additional security was necessary. Implementation of the IPSec on wireless LANs was the proposed solution.

3. Overview of IPSec security architecture:
IPSec is an abbreviation for Internet Protocol Security. It is a protocol that was developed by the Internet Engineering Task Force (IETF) to provide internet traffic security services.
IPSec operates at the network layer in the Open System Interconnection (OSI) model and offers security at the Internet Protocol (IP) level, for all applications and protocols carried over IP.
It is designed to provide interoperable, high quality, cryptographically-based security for IPv4 and IPv6. The set of security services offered includes access control, connectionless integrity, data origin authentication, detection and rejection of replays (a form of partial sequence integrity), confidentiality, and automated key management. [6]
The protocol uses two fundamental security protocols: Authentication Header (AH); to ensure that packets are from the indicated sender and have not been altered in transit, and Encapsulating Security Payload (ESP); to prevent unauthorized reading of packet contents. It allows implementation of the preceding protocols in different ways, in both IPSec modes, and permits use of several combinations. Both protocols security dependents on the cryptographic algorithms used.
Key management is provided by the Internet Key Exchange (IKE). The IKE is a protocol that provides secure negotiation services, initial user authentication and key management. [7]
IPSec can be run in one of two encryption modes: transport mode or tunnel mode.

- Transport mode encrypts/decrypts only the packet's payload, it is usually used between two end-stations.
- Tunnel mode encrypts/decrypts the payload and the header of the packet, it is usually used between gateways or between two networks, it allows off-site users to connect

and access to their remote networks securely [8]. Therefore in this paper, the mode used is the tunnel mode.

IPSec implementation is specified by the IP security policy created. An IP security policy defines the security rules for communications between computers or between networks, and the IP filters for the traffic going through the connection (wired or wireless connection). In every policy; several rules could be created. In tunnel mode; at least two rules are needed to establish any IPSec tunnel between two networks, one rule for each IP traffic direction. [9]

However; IPSec has its limitations as well, since it fails to support multicasting and broadcasting traffic.

Hereafter; a proposed solution for securing the IEEE 802.11 WLANs is by implementing IPSec policy in a wireless network, so all traffic between a mobile device (laptop) and the internet or the wired network is first encrypted and tunnelled to the AP, in a way that no one can peek at the traffic as it travels through the air.

4. Implementation and Configuration of IPSec in WLAN:

In this paper, since IPSec is chosen as the security technology, some design decisions must be taken, such as the WLAN topology, Operating System (OS), IPSec mode, IPSec protocol, authentication method, and others.

4.1. Topology: The interface between the wired and wireless networks is an IPSec gateway that acts as the router between the mobile device and the wired network infrastructure. The AP is directly connected to the router. Figure 1 shows the proposed topology for WLAN.

A security domain is a wireless environment managed by a single IPSec gateway; it is limited to a class C sub-network IP address range. In a security domain; there is a theoretical maximum number of 253 mobile devices, but in reality an AP would not manage more than ten active mobile devices at the same time, because of bandwidth constraints of the wireless connection. For each additional network interface in the IPSec gateway, a new security domain is supported.

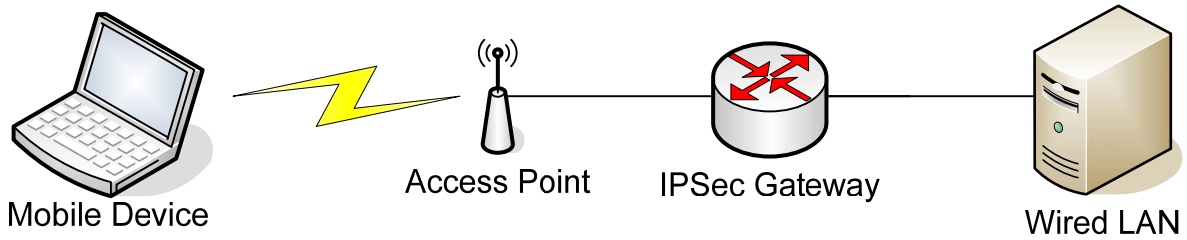

Figure 1. WLAN Topology

4.2. Operating System: Microsoft Windows XP was chosen because of several reasons, mainly because the majority of users run Microsoft Windows on their machines, and also because IPSec is already integrated in Windows XP.

4.3. Mode: As explained earlier in section 3, the tunnel mode is the best to use, tunnels are established between IPSec gateway and mobile devices, and the information about the different wireless users is centralized, which makes it not so difficult to update client data.

4.4. Protocol: Since AH does not include encryption, the option went to ESP, so Data Encryption Standard (3DES) is selected as an encryption algorithm and Secure Hash Algorithm (SHA-1) is selected as a hash algorithm.

4.5. Authentication method: IKE authentication in IPSec can be performed using one of these three methods: Preshared Keys, Certificates or Kerberos.

Since Kerberos is not suitable for small business use, and the digital certificates solution has some implications in our case [6], so the Preshared Keys authentication method is chosen.

A different Preshared Key (which could be any simple string) for every pair of IPSec gateway-mobile device is dynamically generated and refreshed for every new session. The configuration files containing information about the registered peer entities are kept on the IPSec gateway and the mobile device.

Before IPSec tunnels can be established in WLAN, some configurations in the participating entities must be accomplished first. These configurations could be classified in three categories:

- Configuration: This basic configuration for the IPSec gateway and the mobile device enables some necessary settings in the IPSec gateway and the mobile device, and prepares the entities for the tunnel negotiation protocol.
- Registration: Every time a mobile device enters a security domain, it has to register in it. This is done by using two databases, one is on the mobile devices and the other is on the IPSec gateway.
- IPSec policy creation: This dynamic configuration takes place every time a new user enters a new security domain and wants to establish an IPSec tunnel with the corresponding IPSec gateway. By doing so, it runs the authentication and security negotiation protocol, which grants authentication and refreshes the session for the Preshared Key, between the IPSec gateway and the mobile device.

This approach proposes a solution for the WLANs security problems, as it enforces access control, entity authentication between IPSec gateway and mobile devices, by the IPSec policy negotiation protocol and IKE authentication. It also provides confidentiality and data integrity by establishing IPSec tunnels between the IPSec gateway and the mobile devices in the security domain.

5. Conclusion:

IEEE 802.11 standard's security protocol WEP is not sufficient and needs improvements. Task group i currently works on 802.11i standard, which overcomes the vulnerabilities of WEP and offers a high level of security for wireless networks.

Until the previous proposal is globally standardized, an alternative security technique should be applied.

IPSec was proposed to secure the traffic of the legitimate users in a WLAN environment. Although it was not originally intended to secure WLANs, it is a good solution for solving the current wireless security problems.

6. References:

[1] Gunter Schafer, Security in fixed and wireless networks, 2003

[2] http://www.comptechdoc.org/independent/networking/guide/netieee.html

[3] Wireless LAN Medium Access Control (MAC) and Physical layer (PHY) specification, LAN MAN Standards of the IEEE Computer Society, IEEE Standard 802.11, 1997

[4] http://www.live.com/wireless/unix-base-station.html

[5] http://grouper.ieee.org/groups/802/11/Reports/tgi_update.htm

[6] S. Kent and R. Atkinson, Security architecture for the Internet Protocol, IETF RFC 2401, 1998 http://www.ietf.org/rfc/rfc2401.txt

[7] D. Harkins and D. Carrel, The Internet Key Exchange (IKE), IETF RFC 2409, 1998 http://www.ietf.org/rfc/rfc2409.txt?number=2409

[8] http://www.webopedia.com/TERM/I/IPsec.html

[9] Microsoft Knowledge Base Article 252735, How to Configure IPSec Tunnelling in Windows 2000, 2004 http://support.microsoft.com/default.aspx?scid=http://support.microsoft.com:80/support/kb/articles/Q252/7/35.ASP&NoWebContent=1