White Paper

USING PPPOE TO AUTHENTICATE WIRELESS LANS

G. PATERNÒ

Dedicated to the people who devote
Their lives for the sake of the others

Giuseppe Paternò
gpaterno@gpaterno.com

TABLE OF CONTENTS

COPYRIGHT AND DISCLAIMER

This document and the information contained herein is provided on an "AS IS" basis and Giuseppe Paterno' DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

EXECUTIVE SUMMARY

Current wireless LANs technologies provide a feeble security architecture that can be broken by motivated malicious users. Moreover, these technologies do not allow to uniquely identify the user that is accessing the network: as a result, corporations and ISPs are unable to apply appropriate rights and/or services to the end-users.

Through this paper, the author proposes the adoption of the Point-To-Point Protocol over Ethernet in wireless LANs as an authentication methodology and as an additional security component. Furthermore, it explores how consumers, corporations and ISPs will benefit of the aforementioned protocol as an alternative, cost-effective solution to IEEE 802.1X.

CURRENT WIRELESS LANS SCENARIO

The wireless standard IEEE 802.11

The need for mobility and network coverage in open spaces or places where cabling is difficult (such as airports, hospitals, warehouses or old buildings) has accelerated the development of Wireless alternatives. Different technologies exist for transmitting data "over-the-air", for example GPRS, Bluetooth and IEEE 801.11, also known as Wireless Ethernet. This last technology is becoming popular among corporations and consumers because of easy configuration, flexibility and performance with low costs.

In brief, the IEEE 802.11 protocol emulates an ethernet network and most of today's access points are acting as mediators (i.e. Bridges) between an existing Local Area Network, for example the corporate LAN, and the wireless network. Furthermore, the protocol itself includes an optional security feature in the form of encryption, via the Wired Equivalent Privacy (WEP).

Unfortunately, it has been demonstrated that WEP can be broken: a malicious user might gain access to the network without supplying any credential. WEP contains an algorithm, called CRC-32, that was initially designed to verify data integrity: through the observation of CRC-32 over a given number of packets, it is possible to obtain the original WEP encryption keys, be it a 64-bit or even a 128-bit one.

The Wired Equivalent Privacy therefore gives a false security feeling to the end-user, and sensitive data that is not encrypted in the presentation layer, through SSL for example, would be easily eavesdropped.

Moreover, using layer 3 network addresses over the wireless LAN raises some concerns. For example the use of DHCP might represent a disadvantage for those service providers that are unable to identify a specific user, typically for AAA purposes. We must also consider that, once a malicious user gains access to the WEP keys, DHCP immediately gives an IP address and network information to the intruder (DNS, WINS, routing, etc.).

The IEEE 802.11 protocol tries to solve this problem by using MAC addresses to identify uniquely the users. However, the use of MAC addresses introduces another issue, one of manageability: if a user changes the wireless adapter, for example to replace a broken one, he/she should contact the ISP and provide the new MAC address for the old one to be removed. In addition, MAC addresses can be changed easily and guessed by malicious users to gain access to the Wireless LAN.

Existing Wireless LANs authentication methodologies

Recently, the IEEE 802.1X standard, based on EAPOL (Extensive Authentication Protocol Over Lan), has been proposed to solve the problems associated with Wireless LANs. The protocol has been designed to provide user authentication for both wireless and wireline LANs, giving ISPs and corporations the opportunity to provide their users with personalised services such as grouping in specific Virtual LANs.

Although IEEE 802.1X provides flexibility and extended LANs support, purchasing compliant hardware is still an expensive solution for small businesses and consumers. In fact, as of today, many of the Wireless Access Points and hub/switches do not support EAPOL. Furthermore, many 802.1X compliant hardware do not implement the dynamic WEP-key exchange feature (EAPOL-Key), adding potential security issues.

Most consumers, small ISPs and small corporations will not be able to afford such equipment, but are nevertheless in need of security and of being able to identify users accessing their resources: some malicious users today are gaining access to home users' equipment through WLANs in order to attack remote sites and preserve their anonymity.

PROPOSED SOLUTION

A layered approach

As suggested by the OSI specifications, a good solution might be the adoption of a layered approach, focusing on specific aspects of a given layer. By analysing access, authentication and encryption separately the advantage is that the resulting framework would allow changes in one layer to occur without affecting the other layers. As Wireless LANs, including IEEE 802.11, will evolve and new standards become available, authentication and encryption will remain unchanged or vice versa.

Proposed authentication solution: PPPoE

With the introduction of cable and ADSL technologies, ISPs have adopted a methodology for resolving the authentication layer problem for the broadband world.

In standard configuration, these technologies are able to emulate an ethernet network. Although DHCP is easy to deploy for a Service Provider and to configure from an user perspective, it does not provide a way to authenticate the user, and therefore cannot be used for accounting or authorization.

This need was solved with the introduction of the Point-To-Point over Ethernet protocol (PPPoE), described in RFC-2516. Through the adoption of this protocol, access control, billing and several type of services can be performed on a per-user, rather than a per-site or cell basis.

The 802.11 technology, in a similar way to the aforementioned broadband technologies, is able to emulate the ethernet network. The idea then is to apply PPPoE technology to Wireless LANs. The advantage is clear: consumers, corporations and Internet Service Providers can perform authentication, authorisation and accounting easily on the wireless users without adding new components and, more importantly, with little effort.

A practical aspect of this technology might be to provide, for example, fixed IP addresses to a roaming wireless user: wherever the user is located, he/she can have his/her IP address and chosen (as per subscription) class of services.

Furthermore, the use of PPP will introduce another to obstacle to malicious users, that would have to break both the WEP and the PPP layer to gain access to the IP-based network. It is envisaged that passwords MUST NOT be exchanged through the PAP authentication methodology: a stronger protocol such as CHAP (RFC-1994), MS-CHAPv2 (RFC-2759) or better should be used instead.

From a traditional ISP and corporations perspective, there is no real benefit in using PPPoE technology over IEEE 802.1X: a big disadvantage of using PPPoE is the PPP frame overhead and the MTU size problem. However, one aspect must be considered when deploying IEEE 802.1X: the current implementations of this protocol are based on EAP-TLS. This authentication methodology requires the ISP/corporate to distribute X.509 certificates to end-users, which might be quite expensive if a valid Certification Authority is used and, furthermore, they are hard to distribute if organisations have several thousands of customers. Moreover, if the ISP or corporate already owns non 802.1X compliant Access Points, such hardware should be replaced.

For consumers, small businesses and local ISPs such a PPPoE limitation is not an issue, if compared to the cost of deploying both hardware and EAPOL compliant software to the client. The advantage is that, by preserving the existing access points and with a simple additional component (the PPPoE server), they are able to protect their LANs by identifying uniquely the user. As a result, adding a PPPoE server is a great deal easier than deploying EAPOL with EAP-TLS, that requires a more complex infrastructure. Moreover, most of today's operating systems are shipped with a PPPoE client, resulting in a low cost deployment for this technology.

Finally, Access Point manufacturers can easily embed a PPPoE server in their products, that might be distributed as a firmware update, and provide an easy user configuration to the consumer, for example through a web interface.

It is envisaged that to handle the MTU issue, its size should be set to 1412.

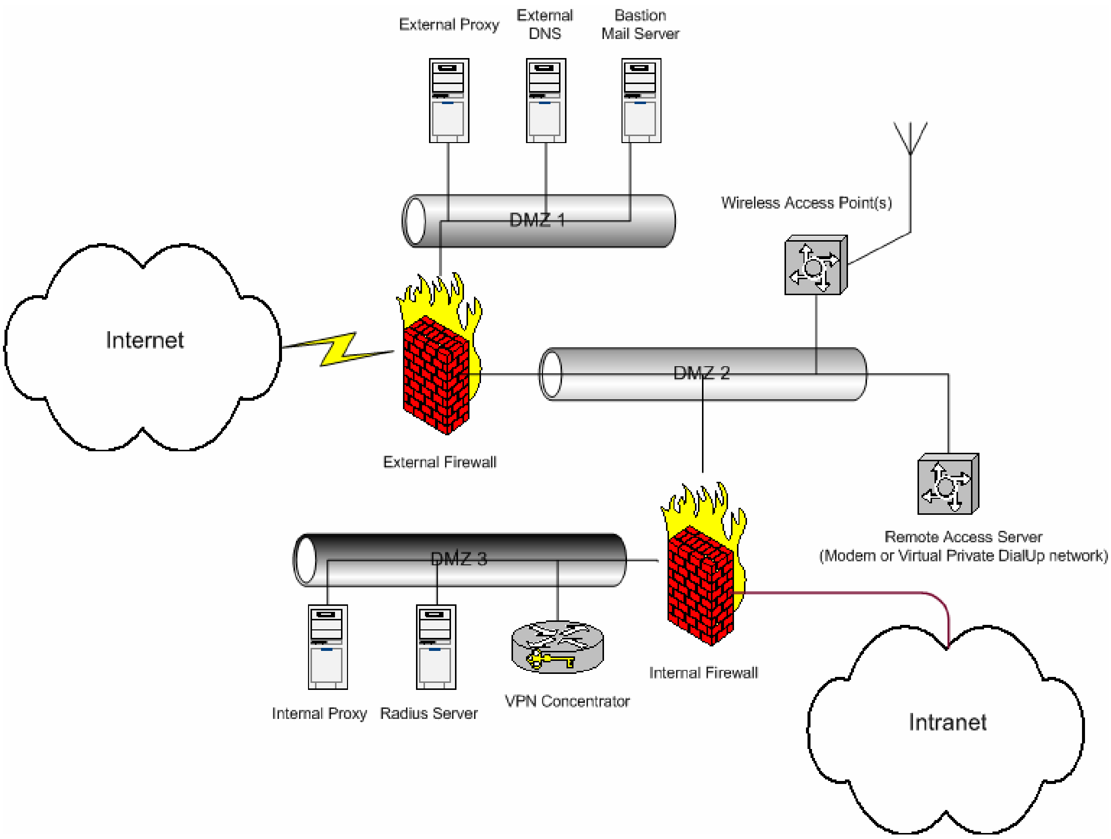
The encryption layer

A Wireless LAN, being over the air, might be considered a public switched network, in a similar way of the plain old telephone network. For example, in the traditional POTS world, a malicious user intercept PPP packets by tapping the phone wire. The Wireless LAN can be managed therefore as a dial-up connection to the corporate and encryption and/or access policies should be applied, such as protecting the access through a firewall or a proxy, allowing only specific applications.

It is recommended that users that need privacy should add an encryption layer on top of their connection, be a wireless LAN or a standard PPP over modem. There can be different approaches for this layer: a simple solution for companies who needs low privacy can be the Microsoft Point-To-Point Encryption Protocol (RFC-3078) extension. A step further would be using stronger encryption technologies to access the corporate LAN, such as for example IPSec (RFC-2401) and the de-facto standard PPTP (which is in turn based on the MPPE).

AN ARCHITECTURE EXAMPLE

In the previous chapter, the Wireless LAN has been compared to a dial-up infrastructure from a security perspective. Using this similarity, a typical corporate scenario can be analysed as an example.



We mentioned that remote access systems, such as modems, are subject to "wardialing", i.e. the attempt of a malicious user of guessing the modem telephone number and accessing the corporate network. Today, most of the corporate IT security policies do not allow to connect a modem and an analogue phone line to internally connected computers. In a security infrastructure, dial-up users are usually subject to an IP-based inspection (be a firewall or access lists) to limit access to corporate resources. While creating a security policy, dial-up user are usually considered more "trusted" than global Internet users, since appropriate credentials should be required.

In the example above, a border firewall separates global Internet access from both externally visible services (DNS, Mail, Proxy, etc..) and remote access users, creating two demilitarised zones, DMZ1 and DMZ2 respectively. DMZ2 should be more secure than the external services, that can be compromised by a malicious user: this zone is suitable for dial-up (be a RAS server or outsourcing through a Virtual Private Dial-up Network) and Wireless LANs user, that should supply credential to gain access to IP-based network.

Once a dialup/wireless user has obtained access, a second firewall connects the DMZ2 to a DMZ3 and the corporate Intranet. DMZ3 hosts a radius server to authenticate users, an internal proxy and a VPN concentrator, if not included with the firewall. The VPN concentrator implements the encryption layer, offering a secure connection to the Intranet. An optional data flow, if encrypted, can be established from DMZ2 to the Intranet, for example IMAPS or HTTPS, so that VPN will be required only for specific unencrypted applications, such as TN3270E (RFC-2355) mainframe access.

CONCLUSIONS

At the time of writing, it is extremely easy from a malicious users perspective to gain access to wireless networks, even if encrypted. Many Wireless LANs are unencrypted and their access points are configured to release dynamic IP address through the Dynamic Host Configuration Protocol. In such a configuration, it is even easier for an intruder to gain access to the network. Moreover, this raises some legal concerns: in some countries it is not illegal to gain access to a network that is not protected in any way or limited through a warning statement, for example through the usual "restricted area" banner, because the user is not accessing the Wireless LAN by "forcing" the system.

Public services, such as ISPs and free wireless networks, will not take advantage of any evolution of the WEP protocol. Today the encryption keys are unique for the whole Wireless LAN segment, which means that keys should be made publically available, in turn making the WEP protection mechanism ineffective.

For consumers and corporations, using WEP or future protocols to encrypt "over-the-air" transmission is still an advantage: although easy to decrypt, the intruder should be very motivated to enter the network because an observation of thousands of interesting packets is needed to gain access to the encryption keys.

Through this paper the author analyses the advantages of using Point-To-Point over Ethernet protocol as a solution for a Wireless LAN authentication layer: it has been demonstrated that, through the reuse of existing elements of the network and without changing the existing infrastructure, consumers, corporations and Internet Service Providers can take advantage of PPPoE, resulting in a more secure environment with no or little additional cost.

After a draft of this document was released to the public, some implementations of PPPoE authentication were deployed, demonstrating the willingness to implement this methodology: in fact, two premier US universities, a premier German university and few private users, including free access city wireless networks, implemented the PPPoE solutions for their Wireless LANs.

BIBLIOGRAPHY

- RFC 2516, "A Method for Transmitting PPP Over Ethernet (PPPoE)"
- Roaring Penguin PPPoE implementation
- RAS PPPoE protocol implementation, by Robert Schlabbach

ACRONYMS

DMZ	Demilitarized Zone
EAP	Extensible Authentication Protocol
EAPOL	EAP over LAN
ISP	Internet Service Provider
MPPE	Microsoft Point-To-Point Encryption Protocol
POTS	Plain Old Telephone System
PPPoE	Point-To-Point Protocol over Ethernet
PPTP	Point-To-Point Tunneling Protocol
VLAN	Virtual LAN
WEP	Wired Equivalent Privacy
WLAN	Wireless LAN

ACKNOWLEDGMENTS

The author of this document wishes to thank Luca Sciortino for his precious moral support and his contribution to this document, Silvio Danesi and Daniele Todde for providing the technical infrastructure. Many thanks go to Maria Di Biccari, Alberto Paterno' and Elisa Stella for their patience and loveliness.