

Novel WLAN Hotspot Authentication

Stephen McCann, Robert Hancock, Eleanor Hepworth

Siemens Roke Manor, UK, {stephen.mccann, robert.hancock, eleanor.hepworth}@roke.co.uk

Keywords: WLAN, Hotspots, Authentication, Public Access

Abstract

The following paper describes the challenges of providing consistent authentication procedures across WLAN hotspots owned by different operators, where the set of credentials that the user should present to the network can be quite large depending on user subscription and inter-operator roaming agreements. This paper provides a description of the set of features that are needed to support secure, authenticated access to the network, and highlights how current authentication solutions provide at least some of these features. Finally the paper introduces two new techniques for enhancing the operation of these authentication solutions to provide a consistent “look and feel” and level of security across different hotspots.

1 Introduction

Increasingly Public Access Wireless LAN (PWLAN) hotspots are being deployed that allow users to access Internet services via a WLAN enabled device such as a laptop or PDA. Generally, hotspot providers charge the user for the services they are accessing, and therefore require a way to verify the identity of the user.

Authentication for PWLAN access has evolved differently to the authentication model used in cellular systems. This is due in part to the short-range nature of the wireless technology, which has led to a certain amount of market fragmentation, with smaller non-cellular operators entering the market. The other contributing factor to this difference is the relatively low cost associated with deploying and operating a WLAN hotspot.

Current PWLAN operators tend to have direct relationships with the users accessing the service, i.e. the WLAN operator provides both the network access infrastructure and the subscription to the user. However, this limits the number of users that can access the network to those that can be persuaded to buy a temporary or permanent subscription (which tends to prohibit spontaneous use).

Since the major revenue for the hotspot operator comes from transport of data, hotspot operators are trying to increase their customer base by offering access to not only their direct subscribers, but also to roamed users, where roamed users have subscriptions with other service providers. As a result,

more complex business models have evolved involving three parties; the subscriber, the service provider and the hotspot operator. Whilst this scenario is analogous to support for roamed users in cellular systems, roaming in the public WLAN scenario is not transparent to the user in the same way that it is for cellular networks. This is because the market fragmentation has led to hotspot using a variety of pricing structures, offering a diverse range of services, and even offering alternative authentication models that have to be used to access the network.

The following section describes the scenario under consideration, before introducing a generic authentication model to highlight the different functions that need to be considered when offering a secure, authenticated service to a user. The paper then goes on to compare the existing hotspot authentication techniques against these identified functions and highlights where there are gaps or shortcomings. Finally, two novel approaches for mitigating these shortcomings are described.

2 Motivation and Background

The scenario under consideration is that of a mobile user connecting directly to the Internet via a WLAN access network within a public environment. The WLAN access network uses roaming agreements with different service providers to carry out control plane functions such as authentication and billing for users accessing their network. User plane data is sent directly out across the Internet to the correspondent node participating in a data session.

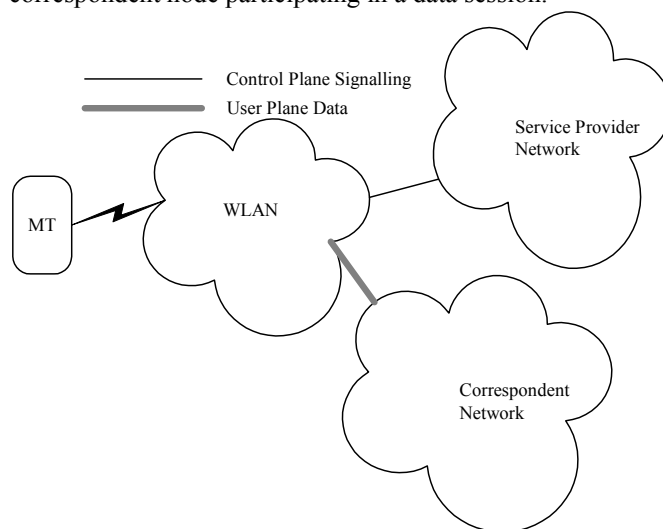


Figure 1 : WLAN Network Architecture

Within Figure 1 below, the following entities are identified:

- **WLAN Access Network:** incorporates multiple WLAN access points and the wired connectivity between them.
- **Service Provider Network:** maintains user subscription and identity information, and is always the same for a given user.
- **Correspondent Network:** the destination/source network for the user plane traffic travelling to and from the Mobile Terminal (MT).

Typically, when the user enters the WLAN hotspot, they are expected to provide authentication credentials that allow the network to verify the user identity to support charging and billing. As a side effect of this authentication process, it is possible to derive keying information that can be used to protect user traffic across the air interface.

3 Authentication Models

The following section introduces a generic authentication model that captures the different aspects of the authentication procedure that it is desirable to carry out before allowing data exchanges between the MT and the network. The different parties involved in the authentication exchange all have different requirements (or expectations) about what they wish to achieve or support as part of the authentication process. It is useful to consider these requirements when identifying functions required by an authentication procedure.

3.1 Requirements

The main goals for each party are:

- **User:** the user would like a single subscription (so only a single set of credentials that can be used in multiple hotspots), ease of use (including a common look and feel for hotspot access regardless of the operator or authentication model in use in the network), and some way to protect their data and ensure that the network is trustworthy, especially if they are billed for access.
- **Hotspot Operator:** the hotspot operator would like to support as wide a range of users as possible (since this is the main revenue source), and some way to ensure that the user is who they say they are in situations where the user is charged for access.
- **Service Provider:** would like to enhance their service portfolio by offering additional services to their subscribers that may be optimised for the WLAN environment.

3.2 Generic Authentication Model

In order to provide authenticated secure access to the network, the authentication model should support a number of features. These include:

- **Subscription Selection:** where the user device selects which credentials to supply to the network for the purposes of authentication. For different networks operated by different providers the user credentials that can be used to authenticate may be different. Therefore, the MT has to have some way to distinguish which credentials to present based on information provided by the network. Otherwise, a trial and error approach may have to be taken.
- **Verification of Network Identity:** which allows the terminal to verify the identity of the network via which it will be communicating. A key part in supporting secure communication is providing a means for the MT to check that the network via which they are communicating is actually the network it claims to be. This, in combination with the verification of user identity, is referred to as mutual authentication.
- **Verification of User Identity:** which allows the network to verify the identity of the user. This is important in scenarios where the user is being charged for access. It also provides an index into policy related information associated with that user as part of their subscription profile that may be used to control the services that the user accesses.
- **Establishment of Secure Communication:** where the data transmitted by the user is protected via encryption. The encryption keys are derived from the authentication exchange.

These are illustrated in Figure 2.

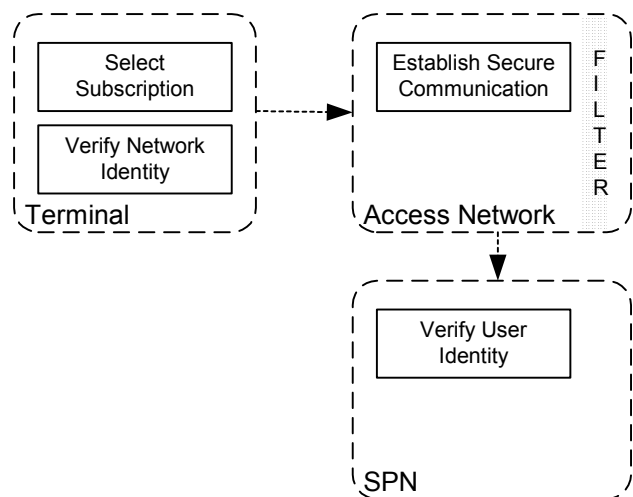


Figure 2 : Generic Authentication Model

The filter within the access network represents the controls placed on user access before authentication, i.e. pre-authentication the user is unable to freely access data in the Internet or exchange anything other than authentication information with devices beyond the access network.

3.3 Current Authentication Solutions

There are currently two techniques suggested for authentication of WLAN users; Universal Access Method (UAM)[1] and IEEE 802.11i[2].

3.3.1 Universal Access Method

UAM is the recommended practice for WISP roaming, widely implemented in current hotspot deployments. The architecture relies on a gateway device within the access network that performs filtering of IP traffic based on whether the user is authenticated or not, only traffic from authenticated MTs is permitted to pass beyond the gateway. This is illustrated in Figure 3.

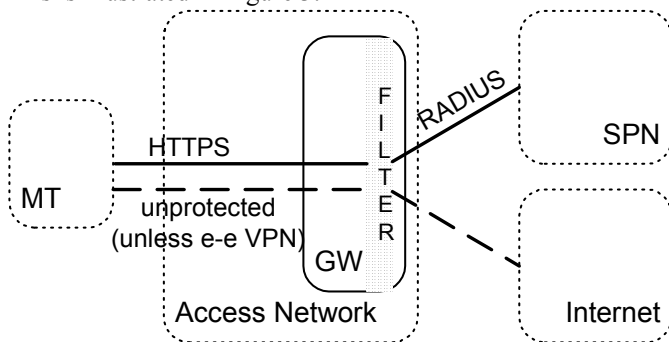


Figure 3: Universal Access Method Architecture

Authentication is performed via a portal page, where the user enters a username and password pair into a page displayed in their web browser. This information is securely relayed to the gateway using secure HTTP (HTTPS [3]), before being encapsulated in RADIUS for transmission to the SPN. The RADIUS exchange is protected by IPsec. On successful authentication, the filter within the gateway is configured to allow traffic from that user to pass into the Internet.

Within this solution, the access points within the access network provide no access control, so any MT is able to attach to the network and generate IP traffic towards the Internet. Therefore, the access network is accessible to both authenticated and non-authenticated users.

From a user perspective, there is an implicit requirement on the user to start up their web browser first in order to perform the authentication exchange, but the browser also provides a convenient mechanism for giving feedback on status, roaming agreements, and other information to the user.

In terms of the generic authentication model; UAM addresses the following functions:

- **Subscription selection:** the UAM specification does not in itself define procedures to support subscription selection, but some hotspots support manual service provider selection via the portal page. A key feature of UAM is support for new user sign up, where users can establish new subscriptions “on-the-fly” via the portal.

- **Verify Network Identity:** The login procedure between MT and gateway is protected using SSL, which also provides certificate information that the MT can use to verify the identity of the access network operator. However, the user has no way to verify whether they are communicating with their service provider network since the user simply provides username and password credentials, and receives nothing in return from the SPN. This can lead to man in the middle attacks by malicious hotspots who can effectively steal user credentials.
- **Verify User Identity:** the SPN receives a username and password pair from the user, but this information is not protected end-to-end, and could be tampered with by a malicious hotspot operator.
- **Establish Secure Communication:** Current UAM authentication does not provide a means to derive keying information for user data protection. In addition to this, there is no way to identify which AP the MT is communicating with in order to download the keying information to the appropriate AP. As a result, UAM recommends users to establish higher layer VPNs to protect their data.

3.3.2 IEEE 802.11i

Recent standardisation work has developed a WLAN authentication model where filtering of non-authenticated user traffic occurs at the edge of the network in the WLAN access points. Therefore, until the user is authenticated, they have no access to the access network infrastructure and are only able to send and receive data supporting the authentication process. This is illustrated in Figure 4.

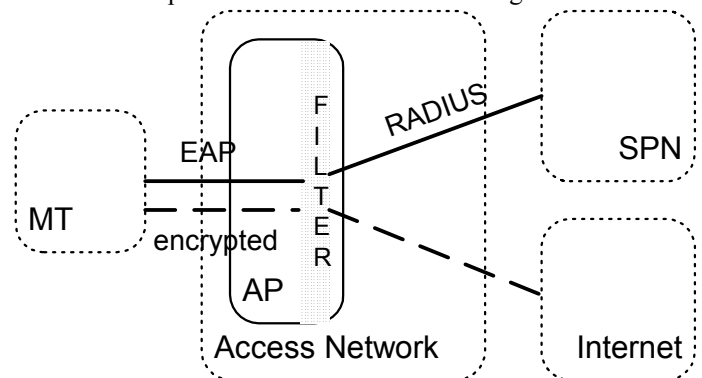


Figure 4: IEEE 802.11i Architecture

An authentication exchange is initiated by the access network requesting identity information from the user. The user identity includes the identity of the SPN with which the user expects to authenticate. The credentials are relayed to the appropriate SPN using RADIUS, and an end-to-end mutual authentication exchange is carried out using the Extensible Authentication Protocol (EAP) [4]. On successful authentication, the filter within the gateway is configured to allow traffic from the user to pass into the Internet.

In terms of the generic authentication model; IEEE 802.11i

addresses the following functions:

- **Subscription selection:** this solution does not currently specify means to advertise operator information other than the identity of the hotspot operator. There are no ways to provide roamed partner information to the user, and solutions are harder in this scenario than for UAM since only a limited communication is permitted between MT and access network (link layer only until completion of a successful authentication). However, proposals have been suggested that allow the exchange of this information either by modifying information provided to the terminal in link layer association messages (e.g. by extended the SSID information), or by extending the initial EAP message from the access network to include roaming partner information [5]. Registration of users is currently not possible in this authentication approach.
- **Verify Network Identity:** the network identity of the service provider is verified either as part of a mutual authentication exchange or unilaterally as part of the setting up of a secure channel (e.g. TLS) between the SPN and MT. The identity of the access network is verified by the service provider.
- **Verify User Identity:** the identity of the user is verified by the service provider. The user credentials may take a wide variety of formats from SIM credentials, one-time passwords, username and password pairs etc. The exact format that the user credentials should take is defined by the service provider. The user interface towards providing these credentials is not consistent. Some approaches require no input from the user, also sacrificing good user feedback functionality. Other approaches require users to configure information in device driver configuration dialogue boxes.
- **Establish Secure Communication:** keys for the purposes of encryption are generated as part of the authentication process. In order to support encryption across the air interface, the SPN downloads a key to the access point, which is used to derive keys for encrypting the air interface. The MT has also derived the same keying information during the authentication procedure.

3.3.3 Comparison of Approaches

From the previous section, a number of gaps in the solutions can be identified. For UAM, there is no support for mutual authentication between MT and SPN, and the range of user credentials that can be used is limited. This limitation prevents hotspot operators from offering roaming services to users with subscriptions based on credentials such as SIM cards. In addition, these credentials cannot be protected end-to-end, and support for distribution of link layer encryption keying information is not possible. This means that the UAM approach is vulnerable to a number of attacks including user identity hijacking, and eavesdropping.

The IEEE 802.11i solution addresses many of these security threats, and is likely to be the authentication mechanism of

choice for future hotspot deployments. However, given that UAM is the approach most familiar to the current subscriber base, IEEE 802.11i lacks some services that are currently available. Most noticeable are the lack of support for new user registration and the lack of a clear feedback procedure to the user to update them as to the status of their authentication procedure. In addition, the interaction between this method and the user is very different to the procedure defined by UAM. Therefore, some way to support the migration of hotspot deployments from UAM to IEEE 802.11i is required that will cause minimal disruption to existing users, and will allow roamed users with any type of subscription to use any hotspot.

4 Authentication Migration

This section presents two novel solutions to address some of the drawbacks of the above approaches, and to try and unify the look and feel of the different authentication approaches for the user.

4.1 Transparent portal page authentication

The first solution provides a way for the traditional UAM hotspot to extend the range of credentials that can be used to authenticate with the network, and to reduce the involvement of the user in the authentication process for those users who prefer a more automated procedure. For example, a user would be able to exchange their SIM card credentials with the authentication server.

The solution operates as follows:

1. the user opens a web browser
 - a. the gateway redirects the user to a login page
 - b. the login page is processed internally within the user device (transparent to the user) where an XML based schema retrieves credentials from the SIM card or hardware token
 - c. an authentication exchange is carried out between the UE and the network to mutually authenticate
2. the user is provided with feedback as to the result of the authentication procedure.

The retrieval of credentials can be carried out by a new content handler implemented as a plugin to the browser, and a new MIME type could be defined to identify when this processing is needed. XML is proposed as a possible way to implement the internal processing on the MT, but there may be other alternative approaches. Keying material is generated as a side effect of this authentication exchange may be used to secure the user data.

There are a number of architecture alternatives that can be considered when developing this solution. In the first of these, the credentials are relayed to the border gateway in HTTPS, and the gateway requests information from the user's SPN to allow it to authenticate the user. This is analogous to

the downloading of GSM triples to the VLR in cellular systems. This requires a strong trust relationship between the two networks, and the development of a transport protocol to transfer the authentication information over IP to the gateway.

In the second option, the credentials are encapsulated in HTTPS and exchanged end-to-end with the SPN. Here, the authentication server in the SPN must support both HTTPS, and be able to understand the format of the credential information within HTTPS.

Finally, the credentials can be encapsulated in an EAP exchange end-to-end that is relayed over HTTPS to the gateway, then backhauled over RADIUS to the SPN. However, a suitable EAP method to support this would need to be selected or developed¹.

4.2 Secure authentication using a local proxy

The second solution provides an IEEE 802.11i solution, whilst retaining the look and feel of conventional web browser authentication, typically using a user name and password. Although IEEE 802.11i addresses perceived UAM security shortcomings, it provides a totally different user experience (i.e. does not involve a web based portal page). The main operation of the terminal is to exchange user name and password credentials with the network using some common authentication exchange protocol (e.g. EAP-MD5).

The solution is to provide a virtual interface on the users device as part of the software upgrade to their equipment to support IEEE 802.1X that presents a UAM interface to the user, but actually implements IEEE 802.1X authentication with the network. The user credentials are exchanged with the network using a suitable EAP method, and Protected EAP [6] is used to carry out the mutual authentication between the MT and the SPN, and to provide the necessary key derivation to support the link layer encryption mechanisms.

The solution operates as follows:

- The user starts up their web browser.
- A local user space DNS server stub (on the user's terminal) replies with a local address.
- The browser then does a HTTP 'GET' request to this address
- The user space web server stub replies with a simple HTML page, created locally on the terminal.
- This HTML page displayed on the browser requests user name and password
- The browser then performs a POST operation on the page, which is passed back through to the user space application, where the user name and password are extracted.
- The user name and password are then passed into a suitable message type (e.g. MD5) and the supplicant

¹ EAP methods exist for many types of credentials, including EAP-SIM[7] for SIM cards, EAP-AKA[8] for USIMs.

initiates a corresponding protocol (e.g. EAP-MD5) exchange with the network, typically using a raw Ethernet socket.

It is important to note, that the use of this local proxy is not a true web server. It only appears that way to the user. It is the ability to manipulate the lower layer data within this proxy, still within the terminal, that provides the secure aspects to this proposal.

4 Conclusion

WLAN hotspot authentication typically follow one of two models, one based on UAM and one based on IEEE 802.11i. It can be concluded that the common features which must be included are: Subscription Selection, Verification of Network Identity, Verification of User Identity and Establishment of Secure Communication.

This paper introduces two novel enhancements to these authentication models to present roaming users with a consistent interaction with the WLAN hotspot when authenticating, and to support a wider range of user credentials.

It is hoped that this work will now be taken forward within various standardisation bodies looking at the issues of PWLAN authentication.

References

- [1] B. Anton, et al., "Best Current Practices for Wireless Internet Service Provider (WISP) Roaming", Wireless Ethernet Compatibility Alliance, 2002
- [2] IEEE P802.11i-2004 (Approved Draft), "Standard for Telecommunications and Information Exchange Between Systems—LAN/MAN Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Specification for Enhanced Security"
- [3] E. Rescorla, "HTTP Over TLS", RFC 2818
- [4] B. Aboba, et al, "Extensible Authentication Protocol (EAP)", RFC 3748
- [5] J. Arkko, B. Aboba, "Network Discovery and Selection Problem", <http://www.ietf.org/internet-drafts/draft-ietf-eap-netsel-problem-01.txt>, July 2004
- [6] A. Palekar, "Protected EAP Protocol (PEAP) Version 2", <http://www.ietf.org/internet-drafts/draft-josefsson-pppext-eap-tls-eap-08.txt>, July 2004
- [7] H. Haverinen et al, "Extensible Authentication Protocol Method for GSM Subscriber Identity Modules (EAP-SIM)", <http://www.ietf.org/internet-drafts/draft-haverinen-pppext-eap-sim-13.txt>, April 2004
- [8] J. Arkko et al, "Extensible Authentication Protocol Method for UMTS Authentication and Key Agreement (EAP-AKA)", <http://www.ietf.org/internet-drafts/draft-arkko-pppext-eap-aka-12.txt>, April 2004