WIRELESS NETWORK ARCHITECTURE TO SUPPORT MOBILE USERS

Maryna Komarova, Michel Riguidel
Ecole Nationale Supérieure des Télécommunications, 46 rue Barrault, Paris 13, France

Keywords: Mobility, Authentication, 802.11i, PANA.

Abstract. In this paper we propose a compound method for user authentication in a public access wireless LAN when the latter requires separate authorization to access internal network services and the Internet. The approach we develop aims to minimize a risk of attacks at network nodes conducted by unauthenticated users provides key establishment and strong encryption between a mobile node and an access point and decreases overall handover latency. An authorized user is granted network and Internet access as a result of a single authentication process that combines 802.11i and PANA operations.

1 INTRODUCTION

With the growth of the number of wireless portable devices, the need for Internet access anywhere is also increasing. WiFi networks are low-cost and they offer a relatively high quality of service (QoS) level for their users. Public access WLANs, also called hotspots, are becoming more numerous. The natural consequence of the fact that coverage areas of different network access points overlap is the user's need to move between them without an active session interruption. The presence of roaming agreements makes it possible for one hotspot subscriber to use an infrastructure of another to access the Internet.

Inter-domain handover management is not only a technical issue. The possibility for this kind of mobility depends on the providers' good will and policies.

Users of mobile terminals need to maintain access to their services while moving between different hotspots. Moreover, many applications, such as VoIP, video transmission or remote program execution, have real-time restrictions. That is why a handover process must be transparent and not impact on the QoS level. To satisfy these conditions, authentication methods must not require user intervention to chose an ISP or enter a login/password.

Authentication and trust establishment procedures take up the majority of the overall handover latency. Some mobile devices are equipped with two network interfaces and this allows simultaneous connection to two networks. In this case time restrictions are more tolerant, but the duration of a soft handover is limited by the time of a mobile node's stay in a zone of different APs coverage areas overlapping.

This paper is focused on reduction of user authentication time in a foreign WLAN, protection of visited network's internal entities and negotiation of user's encryption key, all in a single process.

The rest of the paper is organized as follows: Section 2 provides an overview of the current state of the art in the public access wireless domain and defines the purpose of the work, Section 3 describes a modified method for user authentication in a hotspot, and Section 4 provides a conclusion.

2 STATE OF THE ART AND PURPOSE

Today some public access WLAN providers offer services only for their subscribers, while others can serve visitors, subscribed to a trusted domain. More and more users need to have Internet access anywhere. Several projects on the creation of common wireless access areas are being proposed. The Spanish provider FON, Skype and Google claim that every Internet Service Provider (ISP) supports their idea of shared wireless connection. Their goal

Komarova M. and Riguidel M. (2006).
WIRELESS NETWORK ARCHITECTURE TO SUPPORT MOBILE USERS.
In *Proceedings of the International Conference on Wireless Information Networks and Systems*, pages 325-330

is to build 1 million shared hotspots by 2010 with multi-level subscriptions (Jaanus 2006). Another project starting in Chicago aims to cover the whole city with WiFi networks (The Chicago Tribune 2006). If hotspots share access, it is natural to presume that users will be nomad between them.

User's mobility nowadays is not limited to a home administrative domain, and therefore new authentication technologies are being developed. They take into account the more important handover characteristics: latency and the level of security. User's Single Sign-On mechanism is destined to meet the transparency requirement. The secure roaming management problem can be broken down into several tasks: (1) Fast user authentication in a visited domain; (2) Dynamic trust establishment between administrative domains in a user-transparent manner; (3) Visited network identity verification by the user; (4) Secure communication between authentication servers; (5) Soft handoff execution and (6) Fast and secure redirection of the current session with a correspondent node (CN).

To get Internet access via a foreign network, a mobile user must execute the following steps: (1) Association with an access point (AP), (2) IP address acquisition, (3) Communication with external networks via an access router (AR) or network access server (NAS) and (4) Redirection of its current session with the CN.

Both the mobile node (MN) and the visited network should be protected against spiteful behavior. A fake AP can usurp a user's identity with the aim of using his account or conducting attacks in his name. A malicious user presents several threats to a network's nodes and authenticated users.

IEEE 802.11i (IEEE 2003a), Web authentication and PANA (Parthasarathy 2005, Forsberd et al 2005) are commonly used hotspot authentication approaches today. The first one requires authentication with an AP, others allow network access to any user, but traffic from unauthorized users is filtered by a gateway device. The Universal Access Model offers user authentication via a portal page, while communication between it and the user is protected by an Https tunnel, and a gateway uses the RADIUS protocol to communicate with a user's service provider. Liberty Alliance operates at the application layer of the OSI model, using Web services and Web redirection. Both may require user interaction in an authentication process (entering credentials and choosing a home service provider).

PANA is a protocol for an MN's authentication to a first access router. It serves to transport EAP packets over an IP network and does not depend on a link-layer carrier.

Authentication with an AP protects all internal entities from unauthorized use while authentication with an AR opens a possibility for different types of attack on internal network nodes: on APs, DHCP server etc. Web authentication presents the same risks.

A compound layer-2 and Web authentication scheme is proposed in (Matsunaga et al 2003) to ensure cryptographically protected access in public wireless LANs. According to this scheme, the user first establishes an L2 session key by using 802.1X guest authentication. After that he embeds an L2 session key digest in the web authentication. Guest access to the network may cause a security problem: an unauthenticated user can monitor a wireless channel, acquire an IP address and perform DoS attacks against network entities and authenticated MNs. In addition, time taken by Web authentication often does not permit a real-time application to continue running.

A network can propose different types of services. Some authenticated users need only to have Internet access to continue a session, others need to use internal network services. Such a scenario can require a separate user's authentication between a link-layer connectivity provider and an Internet service provider (Das 2003).

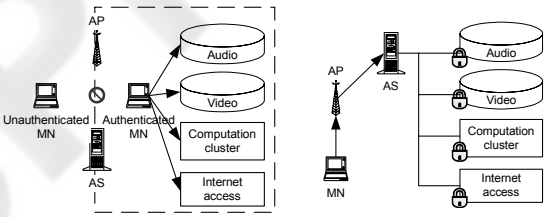

Figure 1: Types of users access to network services.

A mobile user arrives in a new network intending to continue a real-time session with a certain correspondent node. Fig.1 depicts two types of network services access: network managed and user managed. Several scenarios for user access to services are possible: (1) The MN authenticates with the AS via an AP using 802.11i and after that it has access to all services in the network; (2) The MN authenticates with the AS via an AP and must be authenticated to get access to each service and (3) The MN does not authenticate (or performs guest authentication) with an AP and must be authenticated to a network access server (the case of PANA use).

The majority of mobile users need access to an AR to communicate with external networks. To prevent unauthorized network usage, the AR must

know the user's identity. There are various ways to achieve this: (1) When the MN authenticates with an AP, the latter transmits its identity-related information to an AR; (2) The MN must execute authentication with an AR itself; and (3) Authentication with the AP and the AR is done at the same time.

For real-time applications the main requirement is that the time taken to change a point of attachment should be as little as possible. So, there is a need to combine an authentication to an AP and authorization to a service (an Internet service provider) in a single process. Other services do not require transparency.

The paper focuses on the first full user authentication in a new administrative domain, but fast authentication methods for subsequent cell and subnet handovers; for example, 802.11i predictive authentication (Bargh et al 2004, Kassab et al 2005) and PANA mobility optimization (Patil, Tschofenig, Yegin 2005) might be implemented.

3 MODIFIED AUTHENTICATION PROCESS

3.1 Model and Assumptions

Certain networks may offer access to a limited topology (link-layer connectivity and limited network layer access) for unauthenticated visitors, but any access beyond this topology requires authentication and authorization (Das et al 2003).

To communicate with a PANA Authentication Agent (PAA), an MN must have an IP address. The PANA draft (Forsberd et al 2005) assumes that a user can have different addresses before and after his authentication. Unauthenticated clients cannot communicate with internal network entities because of address filtering (see Fig.2, a). The purpose of this action is to separate the traffic of authorized and unauthorized users to protect the former.

In this case the access network is divided into two (or more) logical networks. The access process consists of the following phases: (1) Association with an AP; (2) Guest IP address acquisition; (3) PANA authentication; (4) Key establishment between the AP and the MN; (5) User IP address acquisition and (6) Updating address information at the PAA.

As the user can communicate with nodes in the internal network before being authenticated, many attack possibilities are open. Other shortcomings of the scenario are: (1) All "guest" network communications are insecure until cryptographic keys are negotiated between the AP and the MN; (2) Double address acquisition increases handover time and (3) The DHCP server is situated in a "demilitarized zone" (DMZ), all unauthenticated users have access to it, and the service is vulnerable to different kinds of attacks.

According to (Parthasarathy 2005), the PAA and the AS, the PAA and the Enforcement Point (EP) have a priori trust relationships and it is natural to assume that paths between them are protected. An arriving PANA authentication Client (PaC) does not trust any network entity.

To reduce authentication latency and vulnerability of internal network entities, a modified architecture may be used (Fig. 2, b).

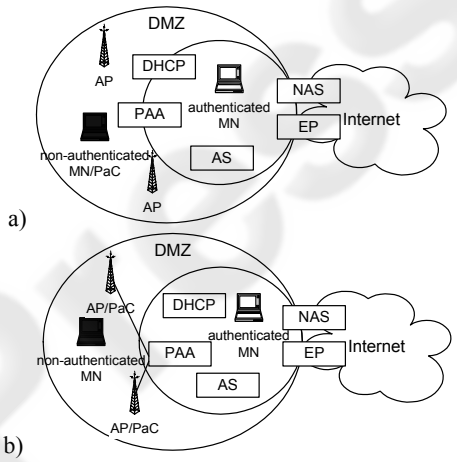

Figure 2: Authentication infrastructure: a) PANA model, b) modified model.

In the proposed architecture an AP has trust relationships with the PAA (via IPSec or TLS). All network entities having an IP address are in the protected internal network. Unauthenticated MNs and all APs are situated in a kind of "quarantine zone". A non-authenticated MN has no IP address in the candidate network; it associates with an AP that opens a communication port only for authentication messages. The AP asks for the MN's identity and acts as a PaC, sending messages to the PAA. EAP authentication is executed between the MN and its home AS via a local AS, the PAA and the AP/PaC.

A combination of 802.11i and PANA protocols was chosen because the 802.11i standard provides a way to secure layer 2 encryption and integrity keys establishment between the MN and the AP. Non-authenticated MNs must not have access to any network entity (see Fig.2), and this is achieved by using the 802.1X controlled/uncontrolled port

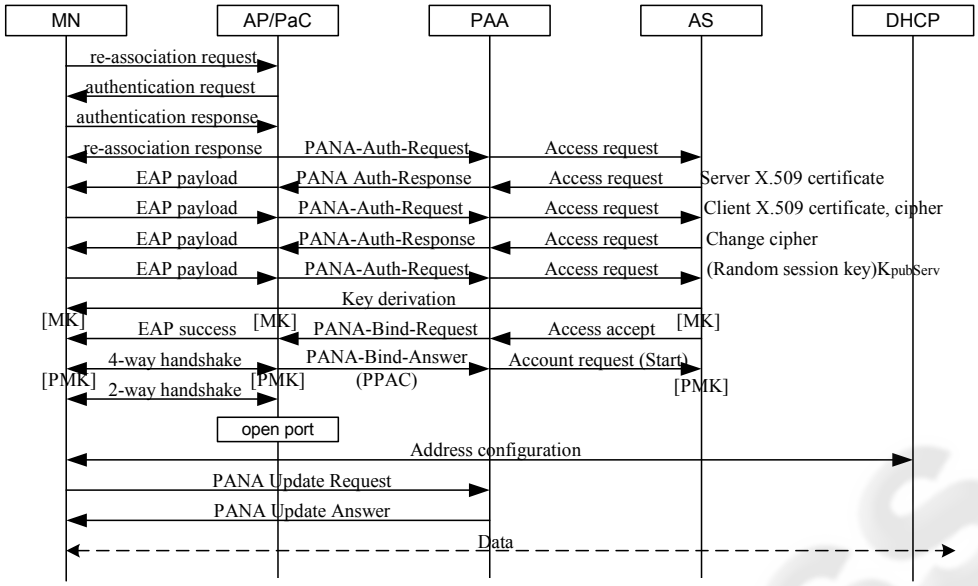

Figure 3: Authentication exchange, EAP-TLS method.

scheme. PANA transports authentication messages and grants or refuses network access to a user. It does not provide key establishment for layer 2 communications. PANA and 802.11i share out tasks: the former is employed for user authentication while the latter - for key negotiation and granting general network access. The authentication process is proposed for the first MN's authentication in an administrative domain, which is longer than subsequent ones in the same network.

There is much work to be done to develop a secure context transfer scheme between administrative domains (IEEE 2003b, Loughney et al 2005). It is quite difficult to deliver any secure information from one AP to another in different domains, because APs often have only internal (non-routable) IP addresses and cannot be directly reached from an external world. Another problem concerns establishing secure communications between APs in different domains. That is why ARs are attractive candidates to participate actively in inter-domain context transfer and therefore it is desirable to place authenticator functionality at the AR.

For a proposed model the following assumptions have been made: (1) all resident entities in an "internal" network have trust relationships and strong security associations. Paths between the AP and the PAA, the PAA and the EP, the PAA (if they are not integrated) and the local AS must be protected by IPSec or TLS tunnels; (2) A visited network should have a certificate, which is understood by a visitor; (3) There are roaming agreements between administrative domains, where a mobile user can nomad, so that when an MN presents its credentials, a local AS in a visited network can recognize an MN's home AS and (4) A local AS puts authentication information into a cache for each visitor.

The second requirement is not too realistic, but if it is assumed that there are no a priori trust relationships between an MN and a visited domain, we must solve two tasks: (1) establishing dynamic trust relations between domains, and (2) visited network identity verification by the MN. This assumption allows one part of the mobility management problem described in Section 2 to be worked out.

3.2 Authentication Process

The proposed authentication approach includes operations of IEEE 802.11i, PANA and RADIUS/Diameter protocols. Fig.3 depicts a full authentication process using EAP-TLS method. This authentication method is set by default for Windows XP users, provides strong mutual authentication, is more high-performance than EAP-TTLS, and does not require a user's interaction.

Several modifications are proposed to the initial methods. An AP, communicating with the MN, acts as an 802.1X authenticator, and, communicating with the PAA, acts as a PaC, sending PANA messages to the PAA, instead of RADIUS messages

to a local authentication server. A discovery and handshake phase is eliminated from the PANA message exchange, since the AP knows the PAA address and there is a secure channel between them.

MN presents its identity in the form of the Network Access Identifier (NAI) (Aboba&Beadles 1999), which helps a local AS to find an MN's home AS: user@home_domain.com. The paper does not concentrate on optimization of communications between the local AS and the MN's home AS.

After a re-association process, an AP connects to a PAA. The AP acts on behalf of the user terminal, and transmits an MN's device identifier to the PAA. The following authentication process is done in the usual way. In the PANA-Bind-Answer the Post-PANA address configuration option must be indicated to inform a PAA that an MN will change an IP address.

The PANA authentication process is optimized according to (Forsberg et al 2005): all PANA-Auth-Answer messages carry EAP payload instead of acting as an acknowledgement. This optimization is possible because there is a channel between the AP and PAA; communications are carried by wired media over a short distance, so there is a very low probability of packet loss.

Normally, the visited network is not a home for the MN, so a local authentication server must operate in proxy mode. This proxy AS may either know a path to an MN's home AS (if there are roaming agreements) or know a path to a central AS, which redirects it to the MN's home AS. Communication with the AS in an MN's home network significantly increases the overall authentication time because of round-trip time that can be high value. Optimization of inter-AS communication and routing is outside the scope of this paper.

3.3 Performance Analysis

PANA packet retransmission timer values are too large to meet fast handover requirements (the Initial Retransmission timeout is 1 sec, Maximum Retransmission Timeout is 30 sec (Forsberg et al 2005)), taking into account the high probability of packet loss in a wireless network. If traffic is managed by an AP at the MAC layer, detection of lost packets and their retransmission takes less time (the minimum value of acknowledgement timeout is about 3 ms, the maximum value is about 52 ms).

Fig.4 depicts a set of operations that the MN must execute to be granted Internet access in the visited network for initial (cf. Section 3.1) and modified approaches. Time taken by both scenarios is shown in Fig.5.

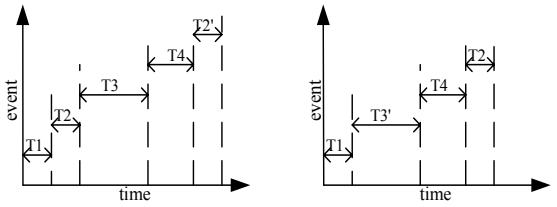

Figure 4: Network access time for standard (a) and modified method (b).

T1 –association with an AP, T2 – DHCP operation, T2' – DHCP operation without its address discovery, T3 – PANA authentication, T3' – proposed authentication, T4 – layer 2 keys establishment between the MN and the AP.

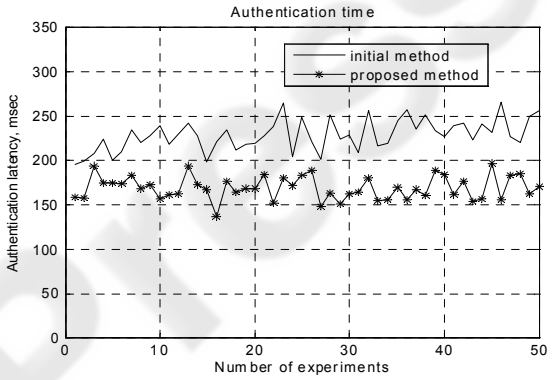

Figure 5: Authentication time for initial and proposed methods.

A proposed scenario avoids double IP address acquisition. Time value T_3 (Eq.1) consists of the

PANA Discover and PANA Authentication phases. Value T_3' corresponds to an authentication process. As all entities execute the same methods, the message processing time and message exchange time are supposed to be equal for both cases. Message processing time for each entity is taken as an average value of time to process different messages by this entity. Links are supposed to be symmetric.

Authentication time, taken by initial scenario execution:

$$T_3 = T_{PANA\text{-}Discover} + T_{PANA\text{-}Auth} = 10T_{MN\_AP} + 10T_{AP\_PAA} + 7T_{PAA\_AS} + 5T_{MN\_proc} + 10T_{PAA\_proc} + 4T_{AS\_proc}, \quad (1)$$

where T_{MN_AP}, T_{AP_PAA}, T_{PAA_AS} are times to transmit a message between the MN and the AP, the AP and the PAA, and the PAA and the AS

respectively; T_{MN_proc}, T_{PAA_proc} and T_{AS_proc} present time to process a message by each participant. The proposed authentication approach takes up

$$T_3' = T_{modif-Auth} = 6T_{MN\_AP} + 8T_{AP\_PAA} + 7T_{PAA\_AS} + \\ + 4T_{MN\_proc} + 8T_{PAA\_proc} + 4T_{AS\_proc} + 7T_{AP\_proc} . \quad (2)$$

$$\Delta T_3 = T_3 - T_3' = 4T_{MN\_AP} + 2T_{AP\_PAA} + \\ + T_{MN\_proc} + 2T_{PAA\_proc} - 7T_{AP\_proc} . \quad (3)$$

The time difference (Eq.3) shows that, in comparison with PANA authentication, the proposed authentication gains the time taken by the PAA Discovery phase and loses the time taken by AP message processing, which is relatively small.

4 CONCLUSIONS AND FUTURE WORK

Parallel authentication permits a mobile user to obtain Internet access as a result of a single authentication in a multi-service network. The proposed approach combines the operation of the two most commonly used protocols to authenticate a user to a network and a service and provide strong link-layer encryption for communications. An AR is a good candidate for the role of authenticator because this scheme may serve for pre-authentication using context transfer between different administrative domains.

The proposed approach does not allow communication between an unauthenticated MN and internal network entities. It aims to protect the DHCP server and access router from untraceable DoS attacks. The performance of the process may be improved due to the exclusion of PAA discovery and handshake phase from authentication and double IP address acquisition. The security level is not compromised; all communications inside the network are secured.

The paper does not take into account a time interval taken by searching for and communicating with an MN's home authentication server, as it concentrates on local authentication and improvement of security of network access.

The handover process still takes a long time and does not allow real-time applications to run without soft handover support. It may be possible to reduce the overall latency by using pre-authentication between administrative domains.

REFERENCES

McCann, S., Hancoc, R., Hepworth, E. (2004). Novel WLAN Hotspot authentication [Electronic version]. *3G Mobile Communication Technologies*, 59-63.

Jaanus (2006, February, 5). Skype invests in FON to increase Wi-Fi availability. Retrieved March, 2006, from http://share.skype.com/sites/en/news_events_milestones

The Chicago Tribune. It's a Wi-Fi kind of town (2006, February, 17). Retrieved February 18, 2006.

IEEE Computer Society. IEEE 802.11i Standard (23 July 2003).

IEEE Computer Society, IEEE 802.11F Standard (14 July 2003).

Parthasarathy, M. (March 2005). Protocol for Carrying Authentication and Network access (PANA) Threats Analysis and Security requirements. *RFC 4016*. Retrieved from www.ietf.org

Forsberd, D., Ohba, Y., Patil, B., Tschofenig, H., Yegin, A. (July 2005). Protocol for Carrying Authentication and Network access (PANA). *draft-ietf-pana-pana-10*. Retrieved from www.ietf.org.

Patil, B., Tschofenig, H., Yegin, A. (2005, October, 21) PANA mobility optimizations. *draft-ietf-pana-mobopts-01*. Retrieved from www.ietf.org.

Aboba, B., Simon, D. (October 1999). PPP EAP-TLS Authentication Protocol. *RFC 2716*. Retrieved from www.ietf.org.

Bargh, M.S., Hulsebosch, R.J., Eertink, E.H., Prasad, A., Wang, H., Schoo, P. (2004, October, 1). Fast authentication Methods for handovers between IEEE 802.11 Wireless LANs. *WMASH'04*. The ACM Digital Library.

Kassab, M., Belghith, A., Bonnin, J.-M., Sassi, S. (2005, October, 13). Fast Pre-Authentication Based on Proactive Key Distribution for 802.11 Infrastructure Networks. *WMuNeP'05*. The ACM Digital Library.

Loughney, J., Nakhjiri, Ed.M., Perkins, C., Koodli, R. (July 2005). Context Transfer Protocol (CXTP). *RFC 4067*. Retrieved from www.ietf.org

Aboba, B., Beadles, M.(January 1999). The Network Access Identifier. *RFC 2486*. Retrieved from www.ietf.org

Rigney, C., Willens, S., Rubens, A., Simpson, W. (June 2000). Remote Authentication Dial In User Service (RADIUS). *RFC 2865*. Retrieved from www.ietf.org.

Das, S., Patil, B., Soliman, H., Yegin, A. (2003, April, 28). Problem Statement and Usage Scenarios for PANA. *draft-ietf-pana-usage-scenarios-06.txt.* Retrieved from www.ietf.org

Matsunaga, Y., Merino, A.S., Suzuki, T., Katz, R.H. (September 2003). Secure Authentication System for Public WLAN Roaming. *WMASH'03*. Retriewed from http:\\berkeley.edu/paper