UniWireless: a Distributed Open Access Network[*]

Danilo Severina
Università di Trento, Italy
severina@dit.unitn.it

Mauro Brunato
Università di Trento, Italy
brunato@dit.unitn.it

Alessandro Ordine
Università di Roma “Tor Vergata”, Italy
alessandro.ordine@uniroma2.it

Luca Veltri
Università di Parma, Italy
luca.veltri@unipr.it

ABSTRACT

In this paper we describe the UniWireless framework, a nationwide distributed Open Access testbed that involves different research units collaborating in the TWELVE national project. The Uni-Fy AAA system, used to manage the collection of involved hotspots, is also discussed.

The most important aspect of the UniWireless framework is its compatibility with different authentication mechanisms; while most access networks enforce a particular authentication protocol upon their users, in the UniWireless system different mechanisms coexist, and each client can in principle use the one that it considers most suitable. Two different, independent and coexisting authentication protocols (capive portal and a SIP-based technique) have been implemented and are described in this paper.

Besides its academic and scientific value for demonstrating results and supporting research activities, the UniWireless framework is actually used to grant access to nomadic users that belong to different research units in all the hotspots related to the project. Every nomadic user can access network resources from every hotspot in the testbed by his usual authentication credentials. Experience gathered from more than one year of continuative use of the system is also discussed.

Categories and Subject Descriptors

C.2.0 [**Computer-Communication Networks**]: General—*security and protection* ; C.2.1 [**Computer-Communication Networks**]: Network Architecture and Design—*wireless communication* ; C.2.3 [**Computer-Communication Networks**]: Network Operations—*public networks* ; D.4.6 [**Operating Systems**]: Security and Protection—*access controls, authentication*

General Terms

Design, Security

Keywords

Open Access Networks, Wireless Networks, Access Gateways, Authentication, Authorization

1. INTRODUCTION

In the growingly popular “always on” perspective ubiquitous wireless networks have accustomed us to, a common problem is given by the plethora of not quite interoperable AAA (Authentication, Authorization and Accounting) systems that are being introduced by different vendors and standardization committees.

Network users need to access remote resources and services in the most comfortable way. On one hand, users want to be able to connect to network services everywhere. On the other hand the network must be readily accessible. In wired network, users are recognized and accounted for on the basis of their physical location, inferred by the physical link they are using. In wireless networks, more sophisticated user authentication systems are required. As GSM experience has shown, hardware identification is not sufficient for authentication and managing and secret-key based procedure are needed.

With the recent explosion of Wireless 802.11 LANs (WLANs), new concepts are required. A restricted environment, for instance a private organization, might be willing to provide nomadic access to its employees and to grant limited access to visitors. In wide area environments, for instance public hotspots in airports or stations, the WLANs are used to provide connectivity to nomadic users. However, for a user to be able to enter various different networks, he needs different access protocols and credentials, often translating into a number of installed resident programs and certificates, at the expense of transparency and ease of use.

In this paper we describe a nationwide testbed that involves different research units that belong to the TWELVE Project. In this project, all hotspots are unified by a framework for users and service management that we call UniWireless. The collection of hotspots is managed by a common authentication system called Uni-Fy, which can be modularly expanded to accept different forms of authentication; in particular, this paper will deal with a “lowest common” authentication functionality based on the *captive portal* technique and accessible by all wireless clients, and with a more transparent SIP-based authentication technique which can co-exist with the former.

The UniWireless framework is used to demonstrate project results and activities, but it is also deployed to grant access to nomadic users that belong to different research units in all hotspots involved in the testbed. Nomadic users can access to network resource from every place involved in the testbed using the same au-

[*] This work has been supported by the Italian Ministry of Education and Research (MIUR) under the TWELVE PRIN project

thentication set throughout the participating units. Sensitive data such as passwords or private keys are never shared among hotspots.

2. BACKGROUND AND STATE OF THE ART

In this paper we focus on two aspects of public wireless LAN, wireless hotspot management and distributed frameworks where nomadic users can access from several spots using the same account. These topics are closely related, so we try to focus their main features to describe the relationships between them.

Public hotspot management is a relatively new subject, so little literature and experience are available on this. Most wireless hotspots are managed by commercial owners with little interest in sharing customers. Some public hotspots, however, are based on the Open Access Network (OAN) philosophy: a horizontally layered network architecture and business model that separates physical access to the network from service provisioning [3]. The pioneering of OAN management has been the StockholmOpen project [19]. The project consists of a WAN connecting wireless and wired access points [9, 10]. The structure of the network allows the coexistence of different Internet Service Providers (ISPs) for user authentication and access to global network. Each ISP that joins in the project must connects its own gateway to the OAN infrastructure. Other OAN based on the StockholmOpen.net idea are deployed in other cities in Europe, North America and Oceania.

The OAN philosophy is based on distributed access spots where nomadic users can access remote resources, but it does not imply any lack of control: a user who wants to connect to global network must be authenticated by a remote authenticator trusted by the access system.

2.1 Authentication systems and techniques

The authentication mechanism can be based on the exchange of private information from the client to the remote server with different authentication techniques and protocols. The most diffused technique is the “captive portal” solution based on web pages: when a user connects to the network and requests a page, he is redirected to an authentication web page where, through a secure HTTP connection, he is invited to provide authorization tokens, which can be as simple as username and password, up to certificates or fingerprints. Some famous free and open-source authentication system based on the “captive portal” solution areWifiDog [21] and NoCat [6]. Recently also commercial solutions based on the same philosophy appeared on the market, like FirstSpot by Pantronsoft (a Windows-based manager).

All of these are software solutions that provide centralized access control and accounting and run on dedicated servers laying behind the physical access network. Recently, “Hotspot-in-a-box” solutions were developed: the authentication procedure is managed by the AP that provides both physical connectivity to backbone and the user authentication. Also in this solution the captive portal solution can be used.

An overview of the access managements techniques would of course be incomplete without mentioning the 802.1x [1] standard and the work done in 802.11i [2] Task Group. 802.1x defines techniques for user authentication (based on EAP, PEAP, TLS, TTLS, etc.) as well as implementation of secure communications (e.g. based on tunneling). Many of these solution can be used in hotspot management system with safe and scalable features. 802.11i is an amendment of the 802.11 standard that specifies improvement of secure mechanism for wireless network. The standard supersedes the previous security procedure called Wired Equivalent Privacy (WEP) which suffers of security weaknesses. 802.11i is a superset of features introduced by WPA (Wi-fi Protected Access) proposed by the Wi-Fi Alliance and is known as WPA2. It proposes an architecture that includes 802.1x authentication mechanisms, stronger block cipher, encryption protocol, and a 4-way handshake for authentication procedures.

2.2 Distributed access framework

Remote resource access management has been a hot topic in the last years. Some architectures based on user authentication to access web-based resources are related to the problem described in the article, however they do not implement an authentication and authorization system. Shibboleth [18] is an architecture that enables organizations to manage a network that allows users to access web resources. The architecture of Shibboleth defines how information must be exchanged between an organization and a provider of digital resources. All the organizations that use this system must previously join a federation. Athens [14] is another access management system to control access to remote resources and services. This management system allows access to protected resources with authentication based on Shibboleth.

Two more projects must be mentioned: IRAP and EDUROAM. IRAP [16] (International Roaming Access Protocol) specifies standard interfaces for exchanging authentication, accounting, and management interfaces between providers of public WLAN roaming. It also defines protocols to integrate WLAN with mobile phone network as GSM (2G and 3G), GPRS, UMTS, and cdma2000.

EDUROAM [15] (Education Roaming) is a framework for interinstitution roaming. The system uses a RADIUS-based infrastructure and 802.1X protocol to support roaming. In Europe several countries connect to Eduroam project and also non-European countries are members (Australia and Taiwan). The project involves research and education networks of several countries. The structure supports authentication and roaming is based on a RADIUS hierarchy and the European root is provided by TERENA (Trans-European Research and Educational Networking Association). The two servers act as roots are operated in Netherlands and in Denmark. The structure of the framework is an OAN. A user who wants to access remote resources from a network must be authenticated. All the traffic in a internal network flows through a programmable router called PAC (Public Access Control) and only authorized clients can access the external network. Authentication procedures are based using VPN, 802.1X and web-based solutions. The deployed solution is based on RADIUS servers because they can support 802.1X.

3. SYSTEM PHILOSOPHY AND ARCHITECTURE

In this section we describe the structure of the UniWireless framework and the entities that are involved in the global architecture. The first part of the section briefly describes the structure of the authentication system in its basic configuration. An in-depth description of the system can be found in [4]. The second part describes the development of new authentication procedure.

3.1 Basic configuration

A single HotSpot involved in UniWireless can be classified in two categories:

Connectivity provider An entity uses a Uni-Fy authentication system to grant network connectivity to authenticated users;

Authentication provider An entity supports a secure database of users that must be inquired to control users’ credentials.

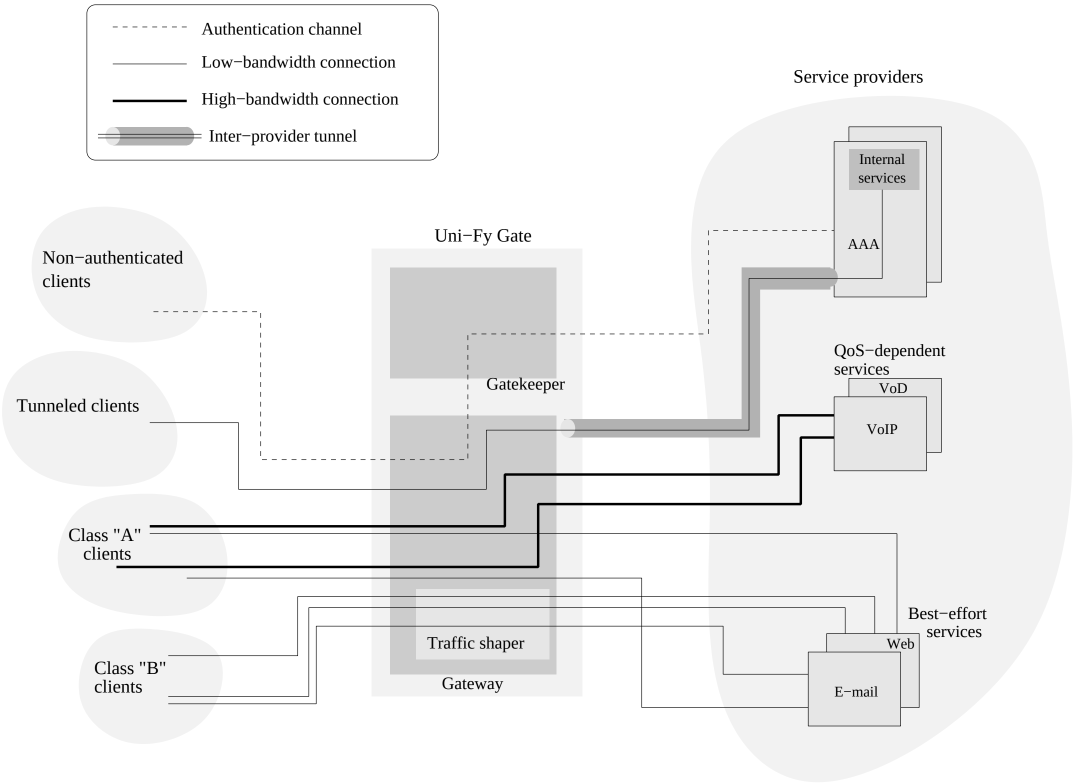

Figure 1: High level architecture of the Uni-Fy system

Obviously, a hotspot can simultaneously be a Connectivity Provider and an Authentication Provider.

3.1.1 Uni-Fy gate

Uni-Fy gate is a wireless hotspot management tool developed in the WILMA project under the name "WilmaGate" and now maintained by the TWELVE Project. The TWELVE team added functionalities and extended flexibility to the authentication system to support the UniWireless system. The Uni-Fy gate is a tool developed in C++ as a collection of user-space applications and its modular design is intended for easy addition of new features.

The main features of the Uni-Fy gate system are:

- support of multiple external authentication providers;
- support of several authentication techniques;
- firewalling;
- accounting.

As shown in Fig.1 the system is made up of two components, Gateway and Gatekeeper, and each component is composed of several C++ modules.

3.1.1.1 Gateway.

The Gateway component runs on a machine with at least two network interfaces and operates as a configurable Layer-3 switch. The component contains a firewalling rules table where, among other data, all (IP address, MAC address) pairs that belong to authorized users are stored. The Gateway receives all the packets from the internal network and manages them. Routing decisions are taken accordingly to the firewall rules table:

- if the packet's source addresses belong to an authorized client, the packet is forwarded to the external network;
- otherwise, the packet is submitted to the Gatekeeper component.

The list of authorized clients and the packet management policies are kept as simple as possible to avoid computational bottlenecks.

3.1.1.2 Gatekeeper.

The Gatekeeper component performs all tasks that require more computational processing than a bare packet inspection. It receives all the packets that are not managed by the Gateway through a dedicated channel between the two components.

The Gatekeeper performs both DHCP management and client authorization based on information received from a remote authentication provider.

The management of DHCP packets can be performed locally using a built-in DHCP server that implements an apprpriate subset of features of a real DHCP server or with interaction with an external DHCP server.

The authentication procedure is performed through interaction with a remote authentication system. At this time, Uni-Fy supports two authentication mechanisms, a captive portal technique and a SIP-based authentication method. A successful authentication procedure (carried out in any of the two methods, depending on the user's needs and capabilities) causes an update of the authorized client list both in Gatekeeper and in the Gateway. When a user is authenticated his traffic is forwarded by the Gateway from the internal LAN to the external LAN and the authorization is automatically renewed from time to time. An authorization can be revoked with an explicit client logout or when a preset authorization period expires with no renewal request. An in-depth description of supported authentication methods follows.

3.1.2 Authentication Server

An authentication database containing a list of known users is inquired by an authentication system to check the credentials that a user provides to access to network resources. Such database can be an institutional RADIUS or LDAP directory as well as an ad-hoc list. An agreement between remote authentication systems and Uni-Fy-driven hotspots must be enacted.

The authentication procedure is always started by the wireless client, which provides its credentials via a secure channel to its home authentication server, so that a Uni-Fy node never manages the private information od a user. There are no limits about the protocol used to exchange information between the authentication system and authentication server, as long as the appropriate firewalling rules are set in the Uni-Fy gateway.

3.1.3 Authentication procedure: Captive portal

When a client connects to a WLAN managed by Uni-Fy gate, it receives an IP address following its DHCP request. With this procedure, the client enters the WLAN but its status is still “unauthorized”, so it cannot access the external LAN. Moving the status to “authenticated” is the purpose of the subsequent packet exchange. In order to obtain an authorization, the client contacts a trusted remote authentication server and exchanges information about his identity.

Related to the authentication procedure, the exchange of information for authorization includes login and password, cryptographic challenges, secure connection or other techniques. Because of the end-to-end characteristic of these procedures, the Uni-Fy gate does not manage private information of the users: it is transparent to the authentication procedures. The system allows unauthorized users to contact external trusted authentication servers, but it is also able to limit the traffic to avoid flooding attacks.

Renewal procedures can be based on stateful protocol and they may require specialized software running on the client, or can be based on standard application (e.g. “captive portal” approach described below).

The first authentication procedure supported by Uni-Fy is a web-based solution, called captive portal. When an unauthorized user wants to access an external network, he needs to open a browser and request a web-page. The Gatekeeper component intercepts the query and redirects the user’s browser to a local page where the user can choose one of the trusted authentication providers. The choice of an authentication provider establishes a secure HTTP connection between the client and the remote authentication server to exchange personal information aimed at user’s authentication.

A successful authorization procedure generates an update of client list in the Uni-Fy system and forces the opening of a pop-up window in the client. The pop-up window must be kept alive along the whole session because renewal is based on its periodic refresh.

3.2 Extension of the authentication procedure

In this section we will see a practical demonstration of the feasibility of the integration within the Uni-Fy gate of other authentication mechanisms. In particular, we will see a secure authentication scheme based on Session Initiation Protocol (SIP) [12] and related to the scheme that is used in 3GPP/IMS security framework [11].

The basic idea is that SIP based authentication mechanism can interact with the authentication system improving the authentication capacities: devices like Wi-Fi phone or devices without display for web-browsing will be able to access to remote resources. The SIP based mechanism will coexist with the captive portal mechanism.

The mechanism we propose is a mixture of captive portal solution and the SIP authentication procedure [13] combined with AKA mechanism (to originate the Digest-AKA authentication scheme [11]). The underlying idea is to realize a collection of trusted-ISPs that is based on the same signaling platform used for multimedia real-time service and in 3G mobile networks. Now we will show a short overview about the authentication mechanism used in this work.

In SIP-based network the digest authentication involves handshake of messages based on shared secret keys. The entities act in such scenario are user terminals with capability of initiating or receiving a call based on SIP signaling. The devices are called User Agents (UA). An UA is an endpoint of a communication and it can acts as server (UAS) if it receives a call, or as client (UAC) if it initiates a call. Usually the authentication request is asked by a UAS to provide identity of UAC before processing of its request, but in some case also UAC can start an authentication procedure. In this last case a mutual authentication is provided.

The Authentication and Key Agreement (AKA) procedure is the authentication mechanism that is used in 3G network and is an extension of the framework for authentication developed by Third Generation Partnership Project (3GPP) in order to extend interoperability of SIP with 3G network. AKA is a challenge/response mechanism that provides mutual authentication between user and network and roaming facilities. In this case the authentication procedure is based on keys that are stored both in user’s device and in the authentication provider.

A mix between the two previous authentication procedure originates Digest-AKA authentication scheme [11]. With this mechanism a mutual authentication between user and network is provided.

3.2.1 Implementation in UniWireless framework

Now we will describe how an authentication procedure based on Digest-AKA mechanism acts and how it can be implemented in the Uni-Fy gate system.

In a inter-ISP roaming scheme, the ISP can provides access to the network (it acts as Access Provider), authentication functionalities (it acts as Authentication Provider) or both. When a user interacts with an Authentication Provider and an Access Provider that are administrated separately, trust relationship is expected.

When a mobile user roams into a new visited network it tries to register with his own SIP registrar server . This SIP registrar server acts as home registrar or Home Authentication Provider. The register procedure is intercepted by the Uni-Fy gate that manages the visited network and the authentication system redirects the request to the Home Authentication Provider appropriately modified with ISP-to-ISP authentication and authorization capabilities, according to the architecture described in the previous section.

In order to assure ISP-to-ISP authentication and correct authorization information retrieval from the Home Authentication Provider (i.e. the remote SIP registrar server), an extension of the standard UAC-to-UAS SIP authentication procedure is proposed and has beenimplemented.

Two new header fields allowing authentication between two intermediate SIP entities are here defined:

- Proxy-To-Proxy-Authenticate header
  (shortly *pp-authenticate* header) is used to carry authentication request information;

- Proxy-To-Proxy-Authorization header

(shortly *pp-authorization* header) is used to carry authentication response information.

The pp-authenticate header is used by a generic intermediate proxy to authenticate a next-hop proxy or next-hop UAS, in order to correctly trust information sent as response from such next hop entity. The pp-authenticate header is inserted by the proxy within a proxing SIP request message, while the *pp-authorization* is inserted in a SIP response message by the next hop entity in response to the pp-authenticate request.

The authentication method used with the pp-authenticate and pp-authorization can be anyone of the SIP authentication methods, without any restriction, and is selected by the intermediate node that starts the proxy-to-proxy authentication procedure.

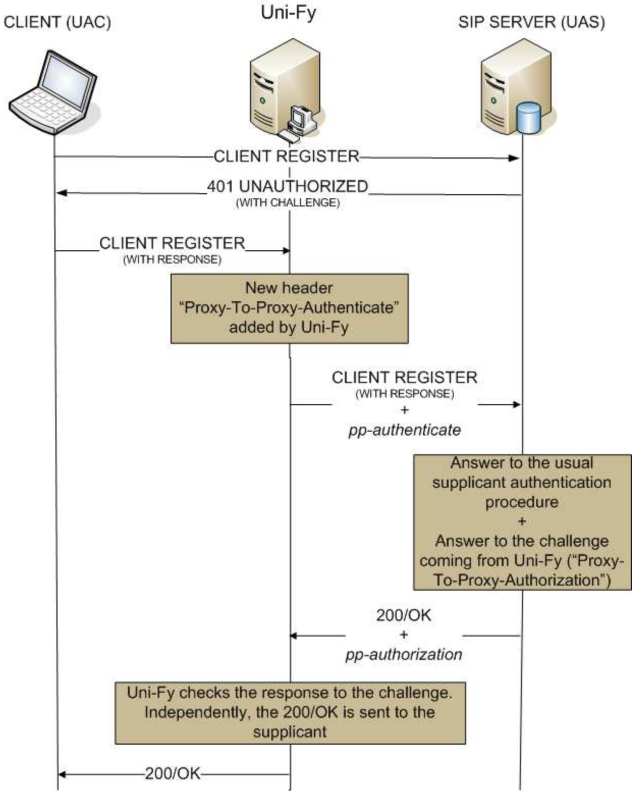
CLIENT (UAC)
Uni-Fy
SIP SERVER (UAS)
CLIENT REGISTER
401 UNAUTHORIZED
(WITH CHALLENGE)
CLIENT REGISTER
(WITH RESPONSE)
New header "Proxy-To-Proxy-Authenticate" added by Uni-Fy
CLIENT REGISTER
(WITH RESPONSE)
+
pp-authenticate
Answer to the usual supplicant authentication procedure + Answer to the challenge coming from Uni-Fy ("Proxy-To-Proxy-Authorization")
200/OK
+
pp-authorization
Uni-Fy checks the response to the challenge. Independently, the 200/OK is sent to the supplicant
200/OK

Figure 2: Proposed Authentication Scheme

The complete registration and authentication procedure exchanged between the user and the Access Provider and between the Access Provider and the Authentication Provider is shown in Fig. 2.

When a user starts an authentication procedure, it sends a register request without authentication header field. The packet is intercepted by the Uni-Fy gate and it is forwarded to the registrar server. UAS starts standard UAC-to-UAS authentication procedure, by sending a 401 Unauthorized response message containing a WWW-Authenticate header with the authentication method and the challenge, as described in [12] and [11]. The message is transparently forwarded to the UAC.

With the reception of this response the UAC sends a new register request with an Authorization header with the proper authentication challenge response. When intercepting this authenticated register request, the Uni-Fy gate (or better the Gatekeeper component) starts a new proxy-to-proxy authentication procedure attempting to challenge the remote registrar. In the register request a new pp-authenticate header field is added with the security parameters according to the selected authentication method used for the proxy-to-proxy authentication. Any authentication method can be used for this purpose, but in the rest of the section we describe the procedure using Digest authentication mechanism.

The receiving registrar server (UAS), according to this procedure processes both the Authorization and the pp-authentication header fields for user authentication and for proxy-to-proxy authentication, respectively.

For the latter, a new pp-authorization header field is added into the registration response generated after the user authentication has been performed and a 200/OK response is sent if the authentication process succeeded. This pp-authorization header field should include, at least, the computed response to the challenge sent, together with the other parameters sent with the pp-authenticate header field.

When the Gatekeeper receives such message with the pp-authorization header, it checks if the new response match with expected result that is locally calculated based on the secret shared between the Access Provider and the Authentication Provider. If the check succeeds and if the response code sent to the UAC from the UAS is a 200/OK code, the Gatekeeper updates its authorization table changing the status of the user to "AUTHORIZED", otherwise if the check fails, the status of the user changes to "FORBIDDEN".

The authentication and authorization scenario that we described has been implemented in the nation-wide test bed UniWireless. In particular a new plugin that manages SIP-based authentication is added to the Gatekeeper component. The new module has been developed in C++ and it is based on the reSIProcate C++ SIP stack library [24].

Besides, we provide the implementation of the registrar server. The UAS has been developed in Java and it is based on the mjsip SIP stack library [25]. The server is appropriately extended to support proxy-to-proxy authentication mechanisms.

4. UniWireless IMPLEMENTATION

The UniWireless framework is a collection of hotspots providing network connectivity in several places. All the universities joining the TWELVE project installed a Uni-Fy gate and some of them also act as authentication provider. Each university has decided autonomously how to install the authentication software related to its previous network configuration and architecture. In Figure 3 an overview of the topology of the system is shown.

The implementation of the Uni-Fy gate can be done with Gateway and Gatekeeper running on a single machine or in two separate computers. The chosen implementation does not influence the performance of the other authentication system in the UniWireless framework: among Uni-Fy gates there are no interactions. Each system works separately and only manages users in the private LAN that it controls.

The interactions in the system are among the Uni-Fy gate and the remote authentication servers. In the setup phase of the Uni-Fy gate a list of remote authentication servers must be inserted. A remote authentication server is defined by IP address, domain and information on how to reach authentication procedure.

The authentication server must be trusted, so prior agreements must be subscribed among connectivity and authentication providers.

After a correct authentication procedure the user receives an acknowledgment from the remote authentication server and has rights to access remote resources. The remote authenticator must send also information to the Uni-Fy node that manages the LAN where the user is, in order to confirm the change of the user state from unauthorized to authorized.

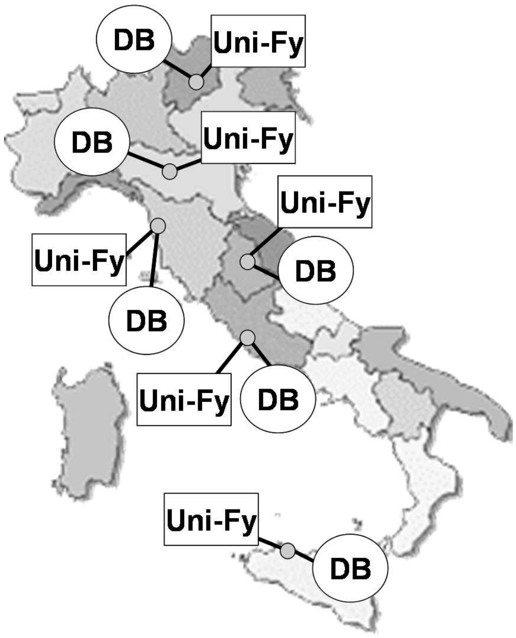

Figure 3: Overview of the UniWireless framework

Besides user authentication and wireless access, the framework has been used to test new algorithms, authentication procedures and protocols without impacts on the other authenticators. Obviously if the new version of Uni-Fy gate that provides SIP-based authentication is implemented only in a hotspot, users relying on that new form of authentication will not be able to use it anywhere else. For this new authentication procedure to be supported by all the entities involved in the framework, an update of all Uni-Fy systems is required.

It is important to underline that updating the authentication system only requires re-compiling the system and (in some case) adding new configuration parameters. It does not force to install new servers that support locally the new authentication procedure. With updating of Uni-Fy gate a nomadic user can access from everywhere using his own credential provided by a remote authenticator.

5. CONCLUSIONS

In this paper we have described the structure of an extensible AAA system targeted at wireless hotspots. This system, called Uni-Fy, is based on the Open Access Network philosophy. It is used for access management and accounting in WLANs, but it can also be used for LANs where the users access with wired connections. Uni-Fy manages the authentication by interacting with remote authentication servers that may use different authentication protocols (LDAP, RADIUS, ...).

Futhermore we presented also extension of procedures for client authentication with a new mechanism. It is based on SIP protocol and it is related to scheme that is used in 3GPP/IMS security framework.

Acknowledgments

The development of the UniWireless framework would have been impossible without the contributions of prof. Giuseppe Bianchi, prof. Renato Lo Cigno and all the people that are working in the TWELVE project to extend and improve the features of this hotspot management system.

We also wish to thank prof. Roberto Battiti, coordinator of the WILMA project where the Uni-Fy gateway originated from and dott. Alessandro Villani, for the technical support in the development of the authentication system and the deployment of the system.

6. REFERENCES

[1] IEEE Std 802.1X: Standard for Local and metropolitan area network – Port-Based Network Access Control. IEEE, 2001 (Revision 2004).

[2] IEEE Std 802.11i: Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks. IEEE, 2004.

[3] R. Battiti, R. Lo Cigno, M. Sabel, F. Orava, and B. Pehrson. Wireless LANs: from warchalking to open access networks. *Mobile Networks and Applications*, Vol. 10:275–287, 2005.

[4] M. Brunato, D. Severina. WilmaGate: a New Open Access Gateway for Hotspot Management. *Proceedings of WMASH2005*, 56–64, 2005.

[5] Rob Flickenger. Wireless Hack. O'Reilly, 2003, Chapter 7.

[6] Rob Flickenger. Builiding Wireless Community Networks. O'Reilly, 2003.

[7] R. Lo Cigno, V. Ammirata, M. Brunato, D. Di Sorte, M. Femminella, R.G. Garroppo, D. Giustiniano, A. Ordine, G. Reali, S. Salsano, D. Severina, I. Tinnirello, and L. Veltri. TWELVE Test Bed and Demonstration Planning. *Network Workshop 2006*, Courmayeur, 11-13 January, 2006.

[8] M. Mellia, R. Lo Cigno, F. Neri, "Measuring IP and TCP behavior on edge nodes with Tstat," *Computer Networks*, Vol. 47, No. 1, pp. 1–21, Jan. 2005, Elsevier Science

[9] B. Pehrson, K. Lundgren, and L. Ramfelt. Open.Net - open operator neutral access network. In *12-th IEEE workshop on Local and Metropolitan Area Networks*, Stockholm, SE, 2002.

[10] E. Pelletta, F. Lilieblad, M. Hedenfalk, and B. Pehrson. The design and implementation of an operator neutral open wireless access network at the Kista IT-university. *12-th IEEE Workshop on Local and Metropolitan Area Networks*, 2002.

[11] S. Salsano, G. Martinello, and L. Veltri. Wireless LAN-3G Integration: Unified Mechanisms for Secure Authentication based on SIP. *IEEE international Conference on Communications - ICC 2006*, Instambul, 11-15 June, 2006.

[12] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks M. Handley, and E. Schooler SIP: Session Initiation Protocol *IETF RFC 3261*, June 2002.

[13] J. Franks, P. Hallam-Baker, J. Hostetler, S. Lawrence, P. Leach, A. Luotonen and L. Stewart HTTP authentication: Basic and Digest Access Authentication *IETF RFC 2617*, June 1999.

[14] Athens. `http://www.athensams.net/`

[15] Eduroam: Education Roaming. `http://www.eduroam.org/`

[16] IRAP: International Roaming Access Protocol. `http://www.irap.nl/`

[17] NoCat Network. `http://nocat.net/`

[18] Shibboleth.
`http://shibboleth.internet2.edu/`

[19] StockholmOpen Project.
`http://www.stockholmopen.net/`

[20] TWELVE Project.
`http://twelve.unitn.it/`

[21] Wifidog.
`http://dev.wifidog.org/`

[22] WILMA Project.
`http://www.wilmaproject.org/`

[23] WilmaGate download page.
`http://netmob.unitn.it/wilmagate.html`

[24] SIPfoundry reSIProcate: an rfc3261 sip stack.
`http://www.sipfoundry.org/reSIProcate/`

[25] MjSIP - GPL open source SIP stack Java implementation.
`http://www.mjsip.org`