SETIT 2007
4rth International Conference: **S**ciences of **E**lectronic, **T**echnologies of **I**nformation and **T**elecommunications
March 25-29, 2007 – TUNISIA

An Incremental Authentication Study using SIM-IP Cards for IEEE 802.11 Wireless LANs

Bachar Zouari[1] Myriam Kallel[2] Ana Cavalli[1]

[1] GET/INT - LOR Department, SAMOVAR CNRS-Unit, Institut National de Télécommunication

9 rue Charles Fourrier – 91011 Evry Cedex – France

{Bachar.Zouari, Ana.Cavalli}@int-evry.fr

[2] ReDCAD Research Unit, Ecole Nationale d'Ingénieurs de Sfax, BP W 3038 Sfax, Tunisie

Myriam.Kallel@yahoo.fr

Abstract: In this paper, we focus on one of the most critical security issues - authentication. Authentication within wireless networks is reviewed. Wi-Fi security weaknesses are illustrated. These drawbacks involve the necessity of designing a new generation of secure wireless systems. In fact, self-control, flexibility, adaptability, autonomy and distribution are the main features to be addressed in a suitable architecture that fulfills modern requirements. In this context, we propose an incremental approach to the final solution which features secure access control with roaming using SIM-IP Cards. An acceptable management and installation price are expected. Intermediate steps are discussed in detail. Security goals and system architecture guidelines are outlined.
Key words: Authentication, Wi-Fi, 802.1X, EAP, TLS, key management, SIM-IP

INTRODUCTION

Wi-Fi networks provide specific mechanisms to ensure authentication and encryption based on using the Wired Equivalent Privacy (WEP) protocol [1]. However, these mechanisms are not secure enough. Many IEEE working task groups (802.11e, 802.11i, 802.1X) are working on related security framework to secure Wi-Fi networks and allow vendors to differentiate their products based on specific algorithms and key handling techniques.

Indeed, we note the diversity of the Wi-Fi vulnerabilities, the suggested solutions to alleviate its weaknesses and the difficulty in concluding on the predominance of a specific mechanism. Lastly, let us notice that no standard is thus established and the issue remains not completely resolved.

In this paper, we focus on one critical issue in WLAN security, more precisely on the authentication and access control procedures. In this context, we propose various authentication methods which can be seen as suitable candidates to make a balance between security requirements and system flexibility and adaptability in the case of the interconnection of remote Wi-Fi networks according to the security level. The aim of our work is to provide different mechanisms in order to fulfill security requirements and to offer security robustness with the regard to the mobility.

The rest of the paper is organized as follows. Section II points out the main security flaws that can occur in a Wi-Fi network and states the current most used solutions. A brief presentation is given in Section III, to fix the context of the work carried out in this paper concerning the interconnection of remote Wi-Fi networks. A detailed description of the proposed security evolution is given in section IV. Finally, section V provides concluding remarks and highlights our future work.

1. Proposed Solutions to secure Wi-Fi

This section is devoted to an overview of security mechanisms applied in a Wi-Fi network and shows the flaws depicted by the weaknesses of the used techniques. In this work, we are interested by authentication mechanisms to set up in BSS infrastructures. Actually, wireless clients must establish an association with APs before any data exchange. Management frames called 'beacon management frames' allow the establishment of the association. An identifier, called SSID, is given to a network controlled by an AP. AP may have a list of many SSIDs. Clients and AP then perform a mutual authentication.

To provide a secure Wi-Fi network, we can classically apply a subset of the following means:

• DSSS technology authentication based on using direct spreading of sequences,

• WEP and its authentication modes, [2][3][4][5]

• Access Control Lists (ACLs),

• SSIDs

• Key and AP management.

WEP is vulnerable and does not specify key distribution mechanisms. Only few vendors have implemented some related procedures. WEP relies on an external mechanism to set-up a globally-shared array of 4 keys [6][7]. An AP can decrypt packets enciphered with any of the four keys. Each message contains a key identifier field specifying the index in the array of the keys being used. The standard also allows for an array that associates a unique key with each wireless client. In practice, a single key is used for an entire network. The reuse of a single key makes attacks more practicable since it increases IV collision chances (24 bit). Moreover, changing a key requires every single user to manually reconfigure its wireless network adapter. Enforcing a reasonable key validity period remains a problem as the keys can only be changed manually.

APs usually provide a network management interface for configuration purposes. An intruder can read/write confidential information via used protocol (in the most cases HTTP, SNMP, telnet or a combination of those).

There are various solutions which can probably be combined to enhance the security of a Wi-Fi system and reduce the viability of the attacks. Among these possibilities, we can find:

- minimal precautions (limit radio coverage, enable WEP, …)
- SSID: modify default SSID, remove SSID diffusion from management messages, change SSID frequently
- MAC addresses limitation and filtering
- improved WEP: use of 104-bit keys, frequent key change, usage of one key per wireless unit and a mechanism to disallow the reuse of IV value for different packets as long as possible
- change session keys frequently
- improve data integrity via strong keyed message authentication code (MAC) such as SHA1-HMAC
- use of IEEE 802.1X for port based authentication (EAPoW, RADIUS)
- use of packet filtering and firewalls for the WLAN to LAN integration
- usage of higher security protocols (IPsec, etc.)

We can conclude that many solutions are proposed to ensure the respect of security constraints. Relevant enhancements are merely expected by recommending applying a combination of these mechanisms to enforce the overall system security. Nevertheless, WLANs systems still have some vulnerabilities which can be exploited by unauthorized users and permit them to gain access to sensitive data. Therefore, on-going standardization work in 802.11 Task group I, studying the convergence between IEEE 802.11 and IEEE 802.1X, made the following recommendations [8] in order to improve security functionalities: mandatory mutual authentication and usage of ciphers providing per-packet authentication and encryption: new key management protocol Temporal Key Integrity Protocol (TKIP), AES instead of RC4.

2. Our proposal context

The goal of this paper is to show the different issues cited above through a real case study and to describe three phases by which we pass in order to set-up a secure infrastructure and enhance the security. Our goal is to check some current solutions and to analyze their scope. A prototype with a huge number of participants will make it possible to carry out a demonstration of feasibility of security-based implementations.

The viability of the obtained solution will be assessed within the framework of real-time interactive services and advanced data applications.

2.1. Security goals

In the context of the interconnection of three remote WLAN sites, we address authentication and confidentiality goals. Firstly, distributed user management is investigated through designing distributed mechanisms of key management and user authentication. Secondly, user authorization levels are clearly defined. For intra-domain authentication, we study some incremental authentication models in order to gradually increase the authentication functionality through different OSI layers (2, 3, etc.)

2.2. Design guidelines

To design our solution we make many assumptions on system configurations such as usage of networks based on 802.11b technology, usage of Internet Protocol (IP), possibility for administration contracts between the domains and, finally, the availability of a common backbone for all participating networks, like e.g. the Internet. Explicitly, trust requirements are clearly defined; we assume that trust relationship with a foreign domain is unidirectional and takes place between two entities. Domain intercommunication is effectively based on a public backbone. We consider the backbone to be mistrusted.

3. Various scenarios

As depicted in section II, a short-term solution is to use a robust key management system for WEP

using IEEE 802.1X [9] architecture. This architecture is a network port authentication system which helps to dynamically derive the keys for WEP. It describes a framework for centralized authentication, access control and key exchange, without fixing a particular security mechanism to achieve this goal. It integrates with open standards for Authentication/ Authorization/ Accounting (AAA) protocols [10], centralizing the authentication decisions at the central AAA-server. This facilitates user and key management and additionally provides for accounting. The most famous representative of the AAA protocol family is the Remote Access Dial-In User Service (RADIUS) [11] protocol. The APs use RADIUS to contact the authentication server. The peers use the Extended Authentication Protocol (EAP) [12] to request access at the APs. Several proposals and Internet standards for suitable authentication are based on EAP. Among those are EAP-MD5 ([12]) and EAP-TLS (Transport Layer Security in EAP) [13]. A lot of other EAP based authentication methods are currently work in progress at the Internet Engineering Task Force (IETF) like EAP-GSS (Kerberos over EAP), EAP-AKA (3G authentication in EAP) and EAP-TTLS (Tunneled Transport Layer Security). The APs act as AAA-clients blocking all the incoming traffic from every network port, except for EAP frames. The EAP frames are analyzed and resent to the AAA-server using EAP-in-RADIUS attributes [14]. The port blockade persists till the arrival of the AAA-server's positive response message. The AP then grants access to the port where the EAP message came from. In the WLAN case, the ports are in fact logically assigned after the physical association.

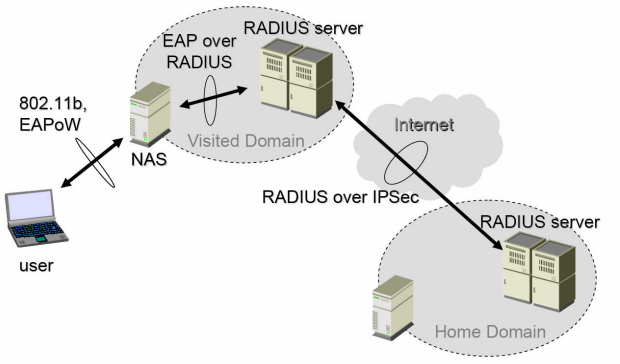


Figure 1. General IEEE 802.1X architecture with roaming

The more complicated case of the non-local user access is carried out by proxying means defined in the RADIUS protocol [11].

Some vulnerabilities of 802.1X have already been discovered [15], notably leading to session hi-jacking attacks or Denial of Service (DoS) type attacks.

The difference between the proposed solutions concerns the force of the used authentication mechanisms and/or the possibilities regarding the user management and the user access levels. In this section, we present different approaches that have been installed and tested in the context of this study.

Since the necessary infrastructure basically remains the same in all scenarios, we will try to describe a practical way from an Open Shared Authentication to our final proposal over functional steps. First of all, we have to assure the security infrastructure exists. It consists of the installation of an AAA server which is always a RADIUS server in our case as the standardization process of Diameter protocol [16] hasn't yet been finished. The underlying Wi-Fi physical layer dictates the usage of appropriate access points acting as authenticators. Those must be IEEE 802.1X enabled, i.e. EAP and RADIUS capable.

In the following section, we will shortly describe the used architectures, the impacts on the security, user management and administration efforts. We begin with the rather typical scenario widely used today and describe its evolution to the stronger schemes. Finally, we will present the solution which we would like to have at the end of the project.

3.1. Scenario 1

Description - This architecture basically follows the 802.1X rules. In its classical set-up it corresponds to the PPP/CHAP equivalent of the dial-in networks, using Point-to-Point (PPP) as transport protocol for the authentication frames. In our case of a local network we could have used PPP over LAN and its authentication schemes (PAP/CHAP). However, this set-up is pretty well-known on one hand and not native to the LANs on the other hand. Besides, we believe that it's already been used for long time, so it's of low interest as a case study. The usage of PPPoL with EAP is possible since EAP was originally designed for use with PPP. Yet, it would be way too complicated since EAP-frames can be now transported directly within the Ethernet-frames using their appropriate form (EAPoL, EAPoW, etc. [9])

Moreover, due to the nomination of the EAP protocol as the transporting frame for the IEEE 802.1X architecture and because of the availability of new EAP-enabled products on the market and in the free software world, some practical study seems to be urgently necessary. Basically, this authentication form is based upon the secrets pre-shared between the RADIUS server and the user. The authenticator system represented by the EAP- and RADIUS-enabled Wi-Fi access point acts as a pass-through device, translating the values in the EAPoW-frames into EAP-in-RADIUS attributes. The server presents to the user an unpredictable random number (challenge), to which the user has to reply by the MD5 hash of the challenge concatenated with the pre-shared secret. According to the properties of the MD5 algorithm, it is hard to generate a matching hash value without knowing the clear-text password. What is more, provided that the challenge won't be used again, the potential attacker sniffing on the wire can't re-use this value for a subsequent authentication. Having verified the correctness of the reply, the server sends an Accept-Response message to the access point, which then opens the related port.

Our case is more complicated, since we have to provide a roaming service for foreign users. Because of the shared secret, the effective authentication work can not be done in the visited network. In the most general case, the RADIUS server has to proxy the request to the user's home network. Thus, the proper user naming scheme is very important in this context. We adopt a format which directly corresponds to the email-address of the user, i.e. the complete user name is the same as user's usual email-address. This format is user@realm where:

- user: the user identifier, treated by the responsible RADIUS server; in our case it is the user's usual ID.
- realm: the identifier of the user's home network; in our case it is the mail-address-domain part of the respective organization.

Every RADIUS server not being configured as responsible for a requested realm has to find the server responsible for this realm according to its configuration. Then, it resends the request acting as a RADIUS client.

According to the RADIUS protocol, data communication between the server and the client doesn't transport any passwords (in particular the "User-Password" attribute) in clear. But, RADIUS dictates the usage of MD5-based method for hiding the password value. There are some serious known security issues, e.g. described at [17], showing the possibility for successful attacks against the used method in particular. Thus, the RADIUS client-server security considered weak, we conclude that the RADIUS traffic is not sufficiently secured to be transported "as is" over public networks, like e.g. over the Internet. However, this is exactly what will happen in the most general case of roaming. So, in order to secure the server interconnections we strongly encourage the usage of IPSec on the underlying network layer. (TLS can not be used because RADIUS is a UDP based protocol). The total number i of server interconnections for a configuration with N domains is: $i = N(N-1)/2$, which results in exactly 3 interconnections in the current (N=3). With this low number, we use IPSec in the following modes:

- Shared secret mode, hence the total of *i* shared secrets. The re-usage of network internal RADIUS client-server shared secrets is categorically discouraged.
- Transport mode, given that no tunneling is to be done and the transport mode is much more efficient.

Analysis - Beginning with the analysis of the theoretical security, we note that this type of authentication can not be considered being high-level-security. The derivate of the CHAP protocol in its EAP form (EAP/MD5) has never been proven to be secure. The password of the user is never transported in clear over the network which should definitely be mentioned as an advantage. But there are some weaknesses directly or indirectly related to this protocol:

- Reported weaknesses of the MD5 algorithm [18] could provide collision attacks delivering a matching value. This can be considered to be a side-effect and a related minor security issue.
- The security of this protocol directly depends on the quality of the pseudo random number generator (PRNG) used for challenge creation. The created numbers should be unpredictable and must not be repeated. A repetition of the same challenge means a successful authentication for an attacker eavesdropping on the medium.
- RADIUS server has to possess the clear text password in order to be able to verify the password correctness. There is no efficient way to generate the same value without having the clear-text-password at the moment of the MD5 procession. Supposing that the server manages a data base for thousands of users (which is not rare) we should doubt this security concept as such. Is it more secure to store thousands of clear-text passwords on one server or to transmit clear-text passwords over some link? Ideally, the passwords should always be encrypted or hidden. Here, the answer depends on the used infrastructure. In our case of a wireless network it is not possible to transmit the passwords in clear. So, we have to use password privacy on the medium at the cost of making the server an appreciated target for attacks. This should be considered a major security issue. The security of the RADIUS server should be considered very sensitive in this architecture.
- Due to the security problems in the RADIUS client-server traffic RADIUS-specific attacks can be applied as described in [17] and at [19]. As already mentioned, RADIUS traffic should be thus additionally protected by security protocols like IPSec. Such protection is absolutely necessary when using inter-domain proxying but can be sometimes omitted within the corporate networks depending on the trust requirements and the WLAN integration scheme.

Some precautions should be met when using this authentication scheme:

- Different shared secrets should be used for each server/client combination. This secret should use non-alpha characters

and be more than 16 characters long [17]. Altering RADIUS passwords frequently should be considered.

- User passwords with as much entropy as possible have to be used. Never should dictionary words be used.

The RADIUS server should be protected by limiting access to it with all possible measures. If possible, IPSec-capable clients should be used and any other traffic on the server-side should be rejected. Additionally, the unprotected passwords should be stored in a protected data-base. It is probably a good idea to use some other host as password depository and limit its connections to the RADIUS server only. Application level firewalls can be used to assure that only correct RADIUS packet can pass through and only from known clients.

3.2. Scenario 2

Description - This architecture directly sets up on the infrastructure obtained in the first phase. Basically, it replaces EAP/MD5 by much more secure EAP/TLS [13]. The latter provides a full TLS exchange within EAP frames. The security of EAP/TLS thus depends on the security of TLS, a well-known, widely used and well-analyzed cryptographic protocol suite as defined by RFC 2246. EAP/TLS introduces fragmentation for EAP and provides strong mutual authentication plus dynamic session key exchange based on public key cryptography. Derived keys can then be obtained from the EAP method to be used in the encryption in the following way: at the authenticated peer side the keys are provided by the EAP-method-API and given to the card driver by the operating system (OS). At the network's side, the keys are derived by the RADIUS server's EAP-method and delivered to the appropriate NAS within a RADIUS protocol attribute. The access point and the peer use this key for WEP encryption on the wireless link.

Compared to the Scenario 1, no changes are required to the APs since, according to the concept, they act as pass-through devices. In the same manner, since the proxying RADIUS server acts as an AAA-client, the proxying of EAP/TLS is possible. However, since the full authentication plus key exchange need a minimum of 9 messages (the actual number depends on whether certificates and fragmentation are used) to be sent, it is better to use the given advantage of public key cryptography. Provided that all participating sites use the same public key infrastructure (PKI) this allows local identity verification without contacting the other side. The used CA itself does not have to be online to the verification time. Basically, if the conditions are fulfilled, the AAA server interconnections can be shut down in this scenario. However, the participators should agree upon the accounting information exchange and billing. In the case of the educational context of the project this is not an issue. The accounting information is gathered only for statistics.

Analysis - First of all, since the MD5 algorithm in general and the dubious MD5-based encryption in particular are not used anymore, all security issues regarding MD5 can be dropped. The usage of EAP/TLS can be considered being a distinct improvement since, for the first time, it introduces a strong cryptographic suite on the stage of network access. Simultaneously, the problem with the clear text passwords on the server disappears. The AAA-server interconnections are not necessary anymore which results in some advantages: first, it significantly decreases the overall authentication delay; second, it provides an even better security; and finally it significantly reduces the maintenance expenditures. Nonetheless, the RADIUS server still has to be protected as it is the central part of the network access control obtaining logged in user statistics.

Generally, this authentication scheme naturally inherits problems of the related cryptographic concepts, i.e. TLS and 802.1X system. These problems include all known attacks against TLS and the conceptual problems of the port authentication in the wireless environment: once the port is authenticated, every packet sent to this port is forwarded into the network. In fact, if the attacker succeeds in overtaking the existing logical port, he can use the authenticated link. This is possible, because the so-called association (physical adapter binding to the radio network) is not covered by the authentication proposed in 802.1X. So, every adapter is allowed to be associated with the AP. What it then has to do, is to replace its MAC address preventing that the authenticated state of the link is changed. That can be used in order to mount hijacking or denial of service (DoS) attacks. However, this problem is a general problem in IEEE 802.1X standard and is not explicitly related to EAP/TLS [15].

3.3. Scenario 3

Description - With Scenario 2, we set up a WLAN-security solution with roaming support. However, the provided public key cryptography is clearly more difficult to handle. The particular problems are the certificate deployment and the reactivity of the system regarding the user management. During the certificate deployment is only an initial step the user management is an important task which remains important during the whole system lifetime. Reactivity is the speed with which the requested user record changes (personal data changes, certificate changes, authorization level changes, temporary access denial, permanent ban, user deletion) propagate through the whole system. In the case of a pure certificate based system as presented in Scenario 2, these changes can only be noticed in the visited network by maintaining a certificate repository which features a certificate revocation list (CRL) and which is synchronized between all the participating domains. During the immediate synchronization could be probably achieved by respective transactions, domain interconnections become necessary again and the maintenance efforts extensively increase. On the

other hand, it is difficult to maintain a common user data base between a lot of basically independent sites. Additionally, in the context of the project one of the aims was to provide roaming access by system i.e. without having to interconnect administrative and organizational institutions of the three sites.

For this purpose, we propose a mixed solution which is based on Scenario 2 regarding the authentication process in the local domain. However, even if the identity verification is done locally, the user validity, user existence and authorization levels are verified by re-using the AAA-server interconnections introduced in scenario 1. The AAA-server in the visited network receives the first message (Response Identity) forwarded to it by an AP. The AAA-server then requests authorization access for the user in the "User-Name" attribute. It forwards the request according to its proxy configuration if this user is not member of his domain. It removes, however, the "EAP-Message" attribute. The AAA-server in user's home domain responds with the list of user's authorization levels. A diagram of a basic message exchange is presented in Figure 2.

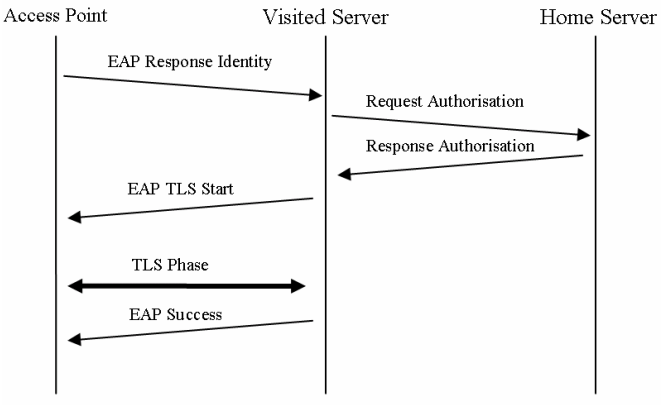


Figure 2. Basic idea of our solution

We are currently discussing the appropriate attributes, formats and message types, in which this information can be sent in a best way, regarding security, efficiency and protocol compliance. In the moment, the authorization information is sent in a new vendor-type attribute within an Accept Response message. For security reasons, the server does not accept Request messages which do not include the EAP-Message attribute from the ordinary APs.

Once the authorization levels are verified and the user has the needed rights to access this particular network the AAA-server in the visited domain proceeds with the EAP/TLS process with the peer. If the peer authenticates successfully (i.e. presented certificate is valid and the User-Name attribute value corresponds to the identity in the certificate), the server issues the Accept Response message. The accounting information is currently kept locally, but it could be forwarded to the home server.

To perform a robust authentication with this proposal, we pursue the strategy of pushing the control elements further towards the network edge. In fact, we install a smartcard in the user terminal which acts as a network edge device. This smartcard is responsible for different control and network layer tasks. However, our network plane is completely IP-oriented and different control layer tasks can be IP-based. The smartcard thus has to be accessible over IP since otherwise the used mechanisms and protocols have to be adapted.

TCP/IP-enabled smartcards like the SIM-IP card have recently gained popularity in the industry. Different manufacturers are planning to propose smartcards integrating a TCP/IP stack. We think that this trend will gain momentum with the proliferation of IP technology. Furthermore, the smartcard development process produces faster and more powerful devices every year. In this work, we use the SIM-IP card as an example because it is the first card to propose an integrated TCP/IP stack.

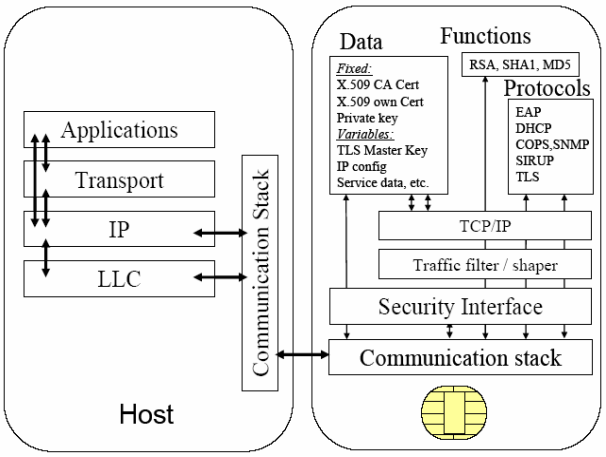


Figure 3. SIM-IP card

This SIM-IP card is an IP-capable Java-based intelligent subscriber's identity module (SIM) with the possibility to integrate services (see Figure 3). Similarly to the GSM/3G USIM cards, it provides a mechanism for user authentication and accounting. Additionally, it includes TCP/IP functionality and can, on one hand, complete terminals that do not support IP natively and, on the other hand, provide IP-based services itself. The card carries a set of security associations (user credentials, authentication procedures, algorithms, etc). It stores data in protected XML files. It can execute Java applets in a protected environment. In particular, it integrates a highly trusted web server and supports various protocols like HTTP, LDAP, COPS/SNMP, EAP, etc.

Additionally to that trusted and tamper-resistant computing environment, the SIM-IP card offers three main advantages:

- Abstraction from the technology-bound secure access mechanisms of the used access network technology
- TCP/IP stack independent from the associated terminal
- An opportunity to include service end points on the card

We use these SIM-IP features to provide users with a computing environment independent of the serving network. For that purpose, we introduce a novel Services-on- Card (SoC) concept. Since we install classically network-internal components on the card, each SIM-IP remains the property of the issuing provider. It is pre-configured by the latter and seen as a trusted network node after it has successfully established the link. This is illustrated in Figure 4. Using trust transitivity, this can be easily extended by an additional visited network. Note that the SIM-IP card does not implement any radio access specific functions.

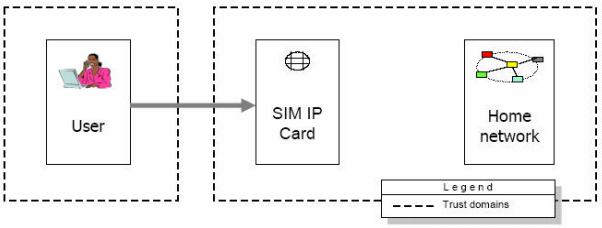


Figure 4. Main actors and trust with the SIM-IP card

We distinguish four *network access phases*. In the first phase, the card connects to all available SPNs using contained credentials and algorithms over terminal's network interfaces. In the second phase, the card collects the data necessary for the network selection decision. In the third phase, the card verifies the user credentials, presents to the user the available services and their properties and grants service access to users. Herein, the user verification is very simple since it can be processed internally by some proprietary algorithm (typically, smartcards use PINs or passwords). Even the mere possession of the card might suffice in some cases.

Finally in the last phase, after a successful network access, the card classifies and manages user traffic and makes necessary reservations. A QoS-aware traffic filter can be installed on the SIM-IP card. It classifies the passing IP packets according to the used protocol/application. Different traffic classes can be defined describing diverse criteria (throughput, latency, jitter,…). Each class is given a priority level.

SIM-IP card stores the necessary security associations and implements the protocols and algorithms necessary for authentication, key management, etc. of every used technology The link layer security mechanisms like e.g. link encryption are carried out by the terminal interface itself. In the authentication phase, the SIM-IP card thus establishes the necessary key material. It then derives appropriate keys and delivers these to the selected terminal interface.

Analysis - This scenario represents a compromise between the first and the second scenarios trying to pull together the advantages of the both. The domain interconnection is obviously indispensable for roaming purposes: even if in the second scenario it can be shut down, we must not forget that it in fact results in a partly common inter domain user management which would still need interconnections for synchronization purposes. In this scenario, those repositories are not necessary since no common CRLs have to be maintained. This reduces the complexity of the system (no repository element) and the maintenance and administration expenditures. The identity is verified using the root CA certificate installed on every AAA server and client. The validity is verified by directly contacting the responsible site. Hence, this solution uses an efficient mid-way between the minimal authentication delay (i.e. no proxying at all) and the completely local authentication (i.e. full-proxying). Moreover, it needs exactly 2 messages to be exchanged on the backbone instead of the minimum of 4 messages in the first and about 10 messages in the second scenarios, thus becoming more efficient. Consequently, it can guarantee the full system-wide reactivity to the remote user data base changes.

Furthermore, the local security of this solution directly corresponds to the security of the second scenario, which was discussed above. Thus, the security is drastically improved compared to the first scenario. Discussing the security of the inter domain connections we should notice that the only sensitive information exchanged in these messages are the user name and user's authorization levels. Even if this information was sniffed and decrypted, no successful login would be possible. In our case, the messages exchanged over the backbone still pass through the secured IPSec channel since it has already been established in the first scenario. With this approach and recalling the relatively insensitivity of the exchanged information, this can be considered being sufficiently secure.

This scenario, with the introducing of SIM-IP Card, provides the higher security of the second approach, shorter authentication delays and high reactivity of the user management of the first scenario combined with more secure and more efficient inter domain link at reduced maintenance and administration costs. It provides also a method to store session keys used in authentication phase.

4. Conclusion and future work

In this paper, we highlight major security flaws in the WEP protocol and recommend several standard and non-standard based solutions to take into account in order to enhance network security. Then, we focus particularly on authentication and the network access since it is the main point of the study undertaken in this work. In the context of a case study that consists of an interconnection of remote Wi-Fi wireless LANs, we deeply discuss the deployment of a global security solution. Three different scenarios are proposed as a solution and are anchored on using various well-known protocols (EAP/TLS, RADIUS, IPSec), strong cryptographic procedures, certificate deployment and user management. A detailed analysis of each scenario is provided. We also highlight the main features to be fulfilled in order to achieve higher security and more

flexible and reactive user management.

Our future work will consequently consist in demonstrating the feasibility of applying these features within a real experimentation platform. Obviously, we will consider a large class of security attacks and a high density of users to analyze the behavior the used security mechanisms.

REFERENCES

[01] Geiger, J., "Wireless LANs", Edition Wiley, 2000.

[02] L.M.S.C of the IEEE Computer Society, "Wireless LAN medium access control (MAC) and physical layer (PHY) specifications", IEEE standard 802.11, Editions, 2003.

[03] Fluhrer, S., Martin, I., and Shamir, A., "Weaknesses in the Key Scheduling Algorithm of RC4", Proc. of the 8th Annual Workshop on Selected Areas in Cryptography, August 01.

[04] D.Doligez, SSL challenge virtual press conference, 1995 http://pauillac.inria.fr/~doligez/ssl/press-conf.html

[05] Walker, J., "Unsafe at any Key Size: an Analysis of the WEP encapsulation", IEEE Document 802.11-00/362, October 2006.

[06] Arbaugh, W.A., Shankar, N., and Wang, J., "Your 802.11 Network has no Clothes", Proc. of the first IEEE International Conference on Wireless Local Area Networks and Home Networks, December 2001. http://www.cs.umd.edu/~waa/wireless.pdf

[07] Borisov, N., Goldberg, I., and Wagner, D., "Intercepting Mobile Communications: the Insecurity of 802.11", Proc. Of the 7th ACM International Conference on Mobile Computing and Networking, Rome, July 2006.

[08] M. Casole, "WLAN security – Status, Problems and Perspective", in Proceedings of European Wireless 2002, Florence Italy, February 2002.

[09] L.M.S.C of the IEEE Computer Society, "Port-Based Network Access Control", IEEE Standard 802.1X, June 2004.

[10] Internet Engineering Task Force, AAA Working Group, http://www.ietf.org/html.charters/aaa-charter.html

[11] Rigney, C., Willens, S., Rubens, A., Simpson W., "Remote Authentication Dial-In User Service (RADIUS)", RFC 2865, IETF, June 2005.

[12] Blunk, L., Vollbrecht, J., "PPP Extensible Authentication Protocol", RFC 2284, IETF, March 2004.

[13] Aboba, B., Simon, D., "PPP EAP/TLS Authentication Protocol", RFC 2716, IETF, October 2005.

[14] Rigney, C., Willats, W., Calhoun, P., "RADIUS Extensions", RFC 2869, IETF, June 2002.

[15] Mishra, A., Arbaugh, W. A., "An Initial Analysis of the IEEE 802.1X Standard", University of Maryland, February 2004.

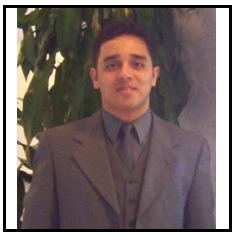
[16] Calhoun, P. et al., "Diameter Base Protocol", IETF AAA Working Group, Work in progress, <draft-ietf-aaa-diameter-10.txt>.

[17] Hill, J., "An Analysis of the RADIUS "Remote authentication dial in user service" Protocol", November 2001, http://www.untruth.org/~josh/security/radius/radius-auth.html

[18] Dobbertin, H., "The Status of MD5 After a Recent Attack", RSA Laboratories' CryptoBytes, Vol. 2, N°2, 1999, ftp://ftp.rsasecurity.com/pub/cryptobytes/crypto2n2.pdf

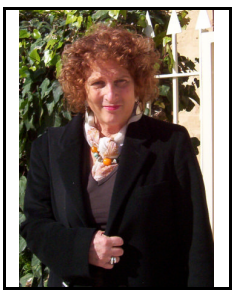
[19] Aboba, B., "The Unofficial 802.11 Security Web Page", http://www.drizzle.com/~aboba/IEEE

BIOGRAPHY



> Name: Bachar Zouari
Address: 9, rue Charles Fourier, 91011 Evry France
Education & Work experience: Researcher: IEEE 802.11 Networks' Security
Tel: +216 21 460 330
E-mail: Bachar.Zouari@int-evry.fr
Bachar.Zouari@zouari.net

> Name: Myriam Kallel
Address: ReDCAD Unit, ENIS BP W 3038 Sfax, Tunisie
Education & Work experience: Researcher: IEEE 802.11 Networks' Mobility
Tel: +216 23 200 085
E-mail: Myriam.Kallel@yahoo.fr



> Name: Ana Cavalli
Address: 9, rue Charles Fourier, 91011 Evry France
Education & Work experience: GET/INT-Evry Professor & LOR Department Director
Tel: +33 160764027
E-mail: Ana.Cavalli@int-evry.fr