Smart cards for WLANs
A white paper

Jerome Ajdenbaum
Iteon

Version 2 – February 10th, 2003

The wireless LAN market is currently booming. According to the Yankee group, the WLAN adapter shipments in the US increased by more than 300% to 10 million units in 2002 ! Yet, these figures could have been higher without the lack of security of the first equipments.

The smart card appears to be an interested solution to bring a high level of security without tampering with the ease of use. Operators begin to study the technology and France Telecom, a major European telecom operator, recently announced that it would be using smart cards for the deployment of its WLAN offer.

In this paper, we first come back on a general introduction to wireless LANs, their past security flaws and how these were addressed. Finally we discuss how smart cards can help in terms of security and ease of use, which technologies and standards are available and how they can be deployed.

Wireless LANs : a backgrounder

What is a wireless LAN ?

Close to everybody, in today's business environment has access to a corporate network, plugging some kind of wire in its PC. Basically, wireless networks also known as WLANs offer the same services, without wires. Your PC will connect to the network, through a radio link. There are several ways of communicating between devices on a radio interface : Bluetooth or IEEE 802.15.3 target Wireless Personal Area Networks

6, rue Camille-Desmoulins - 92300 Levallois-Perret - France
Tél. : +33.1.56.76.60.26 - Fax : +33.1.47.59.07.36 - Email : info@iteon.net - Web : www.iteon.net
SARL au capital de 8000 euros - RCS Nanterre B 429 947 161

(WPANs) addressing communication between devices such as PCs, Personal Digital Assistants (PDAs), peripherals, cell phones, pagers, and consumer electronics.

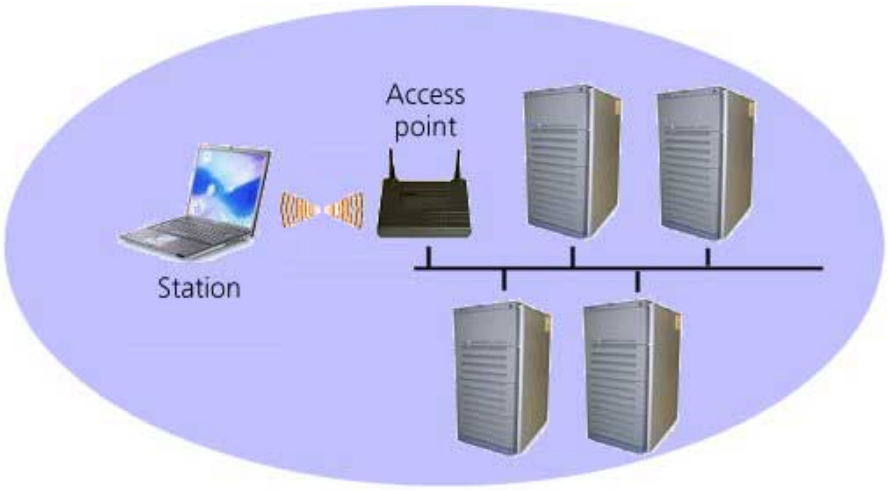
WLAN targets Local Area Networks with higher range, higher transfer rate, and higher price…

Standardisation

WLAN is also known as IEEE 802.11, the name of the standardisation group. This same IEEE 802 group standardised the wired technologies such as Ethernet or Token Ring.

Architecture

Usually a station (e.g. a PC) will connect to the WLAN via an Access Point (AP). The access points make the interface between the wireless environment and the wired world. In order to do that, the station must be equipped with the proper interface, either built in (becoming common for laptops) or as an add-on card.



Windows XP, has built-in support for WLANs providing seamless access to wireless networks.

Roaming WLANs

When a station wants to access an existing WLAN (e.g. for internet access through a WISP – Wireless Internet Service Provider), either after power-up or because it enters an hotspot, it will run a procedure to connect to the best access point. It can passively wait for some information from the access point (a so-called beacon frame) or actively

send data on the radio link (probe request frames) and wait for the answer from the access point (probe response frame).

The next steps are authentication, where the station uses its credentials to be authorised, and association to exchange information about the station and access point respective capabilities.

From that point, data (frames) can be exchanged.

Depending on the result of the authentication procedure (the station is known from the network operator), the user may be asked to buy some airtime in order to enter.

The Wi-Fi Alliance's WISPr (Wireless Internet Service Provider Roaming) committee is aimed at defining a framework for global roaming agreements, allowing an user to seamlessly use its station around the world. It will most likely use the RADIUS protocol (see below).

Security issues with WLANs

Security in computer networks

Today security in local area networks is heavily relying on physical security : intruders do not have a physical access to the network, because the wires are protected by walls, doors, etc.

The way these networks are designed make it be very vulnerable when an intruder finally gains access to the physical media. Today, few companies with a need for high security requirements use VPN techniques to enhance the level of confidentiality on their corporate networks.

Security consists in several functions, including :

- Confidentiality (encryption), preventing attackers from understanding the data,
- authentication, preventing unauthorised access to network resources.

WEP and 802.11 security

When WLANs were specified, much attention was paid to the security aspects, creating a security algorithm to enable wire-equivalent security. Hence, this algorithm was called WEP for Wire Equivalent Privacy.

WEP can be used both for confidentiality and for authentication.

WEP relies on the well know RC4 stream cipher. A stream cipher is a cipher that encrypts flows of data, bit per bit (while block ciphers encrypt blocks). To make things simple, using a secret key, RC4 produces a flow of pseudo-random data that it mixes (XOR) with the plaintext data to be encrypted to obtain the ciphertext. The RC4 key is shared between the

station and the access point allowing one entity to cipher and the other to decipher.

However, a pseudo-random data flow must be used only once. If it is used twice, it becomes evident to recover the plaintext. To prevent that, WEP uses a 24 bit initialisation vector to make each sequence unique.

When a station establishes a session with an access point, it goes through an authentication phase (as mentioned earlier). Two authentication methods are available :

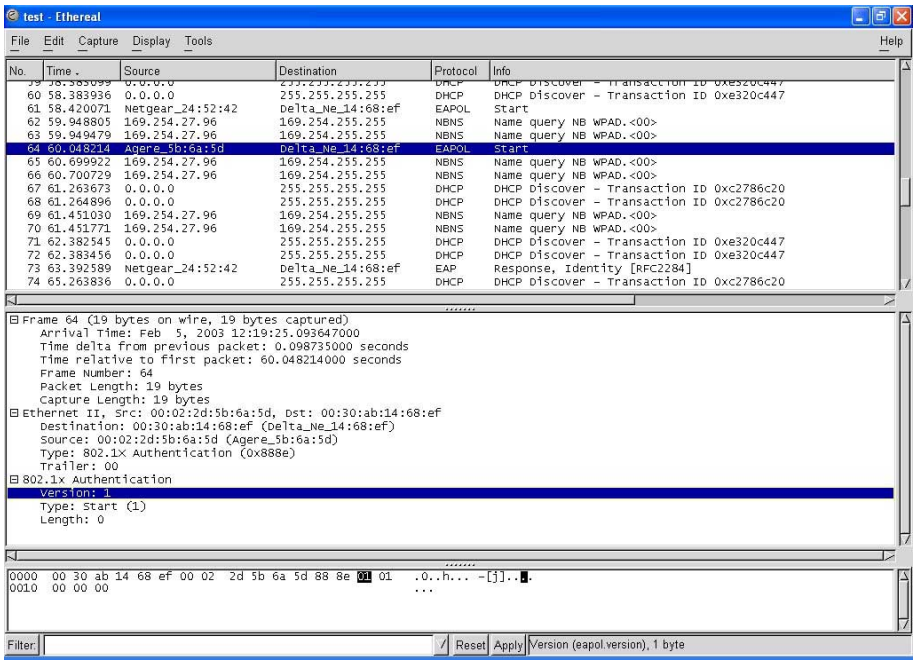
- open authentication, which does not provide security,
- shared-key authentication, that is based on WEP challenge response.

Attacks against WEP

Unfortunately, there has been so many attacks against WEP, both for authentication and for confidentiality that it would be too long to describe them all. These attacks were already widely discussed in many papers on the internet. We will only describe here the main lines.

Most of these problems come from the already mentioned fact that a key stream should not be used twice and from the initialisation vectors. It is worth noting that RC4 itself did not fail.

A paper published in August 2001 by famous cryptographers Fluhrer, Mantin and Shamir showed that a WEP key could be derived by passively recording frames on the radio interface. Many other attacks were described (initialisation vectors replay, bit flipping). Eventually developers implemented these attacks in software that was made available on the internet. AirSnort, for example can recover keys within a few hours on a standard well loaded network using a standard PC. Attackers would just need to park their car nearby a building and wait a few hours to see all the confidential data exchanged (parking lot attack). Below, we show an example of a simple network sniffer widely available on the internet.



Another weakness of WEP is the lack of support of key distribution methods. Static, preshared keys need to be entered on devices.

WEP had proven to be weak, whatever the size of the key.

New security improvements

The failure of WEP happened to be very negative for the WLAN market. Which corporation would want to deploy a network making its secrets available to anyone ?

The security of authentication is now addressed by 802.1X framework, together with EAP protocols while the weaknesses of WEP are closed with TKIP (Temporal Key Integrity Protocol). TKIP can be seen as an (efficient) patch, requiring only software upgrades waiting for the 802.11i protocol based on AES standard encryption algorithm.

802.1X and EAP protocol

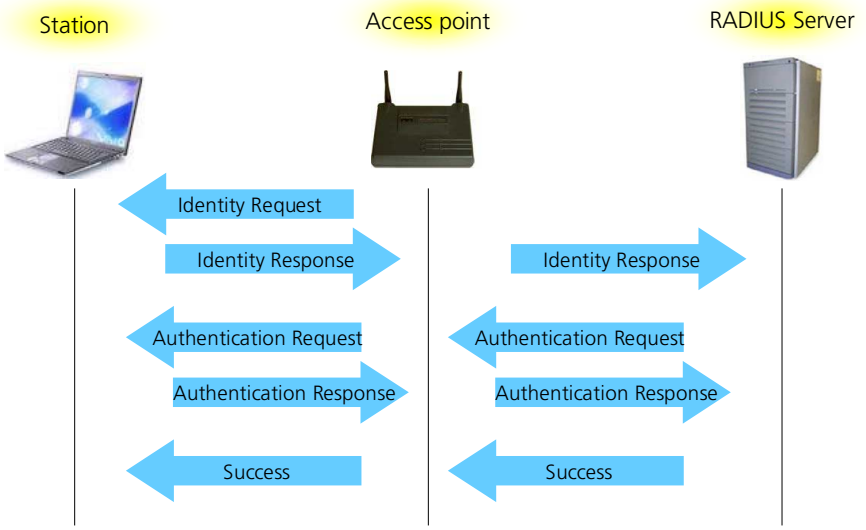
IEEE 802.1X is an authentication framework, residing in the lower layers of the protocol stack. It defines how an entity (supplicant) in the station, will be authenticated by another entity (the authenticator) in the access point, based on a message exchange with a third entity (the authentication server) usually residing in a RADIUS server.

It is based on the well known EAP (Extensible Authentication Protocol).

EAP is base on a threefold dialog.

- First, the access point sends a "EAP Identity Request" message to the station. The station will reply with an "EAP Identity Response"

message containing its identity. The access point will forward this message to the RADIUS server associated with the user's identity.



- Second, the RADIUS server sends an "EAP Authentication Request" to the station, via the access point, the station replies with an "EAP Authentication Response".
- Finally, the RADIUS server verifies if the authentication response is valid and sends an "EAP Success" (or "EAP Failure") message.

EAP methods

EAP is an open protocol : there are several different EAP methods and new methods continue to be added.

Three EAP methods are described in the EAP standard :

- EAP MD5, where the challenge is hashed with a password and transferred, does not provide mutual authentication,
- EAP One Time Password
- EAP Generic Token Card

Other interesting methods include :

- EAP TLS, based on SSL, is an IETF standard (RFC 2716),
- EAP TTLS and PEAP, are hybrid protocols, using TLS to create an encrypted tunnel in which another method is encapsulated. The station authenticates the server using TLS certificates and authenticates itself to the server using another method,
- LEAP, a Cisco method transferring a password in a MD4 hash to ensure confidentiality, is particularly suited for Windows NT environments,

- GSS API EAP, based on the standard Generic Security Service API,
- IAKERB extends Kerberos to enable the station to obtain tickets. Kerberos is a network authentication protocol designed to provide strong authentication for client/server applications, using secret-key cryptography
- EAP SIM, reuses the GSM SIM card to provide mutual authentication. We will discuss EAP SIM in more details below.
- EAP AKA is similar to EAP SIM but based on the USIM,
    - EAP SecurID, based on RSA SecurID tokens, does not provide mutual authentication,

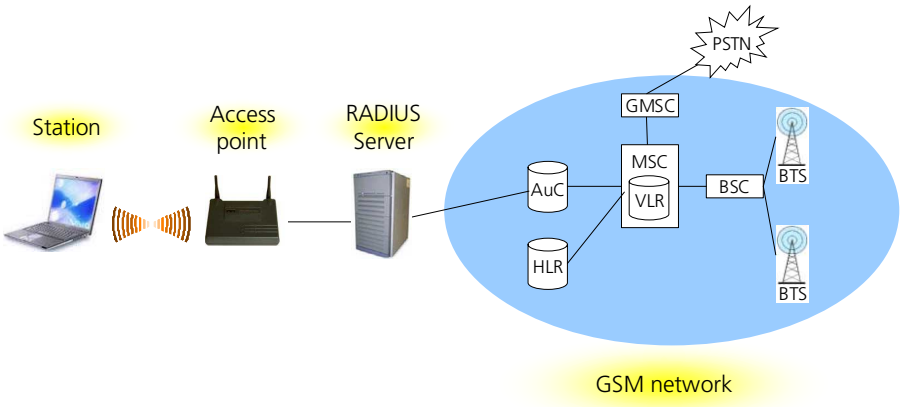
EAP methods can be very easily added in existing products, providing a flexible way to do authentication. On Windows XP, a simple library (DLL) is needed.

RADIUS servers

RADIUS (Remote Authentication Dial-In User Service) is the standard protocol used by Authentication, Authorisation and Accounting (AAA) servers. Therefore, AAA servers are often called RADIUS servers.

In the 802.1X framework, the RADIUS server in dealing with the authentication of the user. Still, if the server is not able to process the authentication itself, it just routes the request to another server.

For example, in the case of a EAP SIM, the RADIUS server will hand the authentication data to the AuC, which is the entity in a GSM network in charge of the authentication of SIM cards.



Using smart cards with WLANs

Why use a smart card ?

For those who know the success of the SIM cards for GSM phones, the idea of adding a smart card to secure WLAN seems natural. Let us detail the pros and cons of this alternative.

Adding smart cards allow to reinforce security – smart cards have no equivalent today in terms of tamperpoofness and resistance to attacks – and to make key distribution simpler – it is much easier to manage tokens rather than to manage preshared keys or complex public key certificates.

The main issue with smart cards of course, is that there are currently no reader on devices. This can easily be solved by adding cards at the SIM format with a reader in the form of a USB token.

EAP TLS : an excellent method for roaming

The Transport Layer Security (TLS) EAP, backed by Microsoft is an internet standard (RFC 2716) based on the well known SSL (TLS) protocol. It is integrated in Windows XP.

It is not the aim of this document to give a training on cryptography, still we would like to introduce a basic notion, and we will restrict the scope to authentication.

There are two types of cryptography : secret key and public key. In secret key infrastructures the authenticator needs to pre-share a secret with the supplicant to authenticate it. For example, in WEP, the station and the access point need to pre-share a key, in a GSM network too. In public key infrastructures, the authenticator does not need to pre-share a secret with the supplicant to authenticate it. The suppliant only needs to hold a certificate. The certificate is like an ID card. It holds information about its owner and is signed by an authority. Using public key mechanisms, the authenticator will be able to check that the supplicant is actually the one it pretends to be, and that this is guaranteed by a trusted authority.

It is very inconvenient to do roaming with secret key infrastructures : for example in GSM, when a user roams to another network, this new network as no way to authenticate him, as they do not share secrets (secrets are only shared between the operator – in a secure server, the AuC – and the user – in its secure SIM card). Therefore, he has to request some authentication material from the original operator, the procedure is quite complex.

With public key, everything becomes very easy, as far as the roaming operator trusts the original one, it can authenticate all of its users.

Public key is therefore very convenient, but it appears to be very complex to manage in particular for the certificate management (registration, distribution, revocation).

If certificates are stored in smart cards, everything becomes much easier : the operators just have to manage tokens. Smart cards holding EAP TLS certificates appear therefore has an excellent solution to roaming issues.

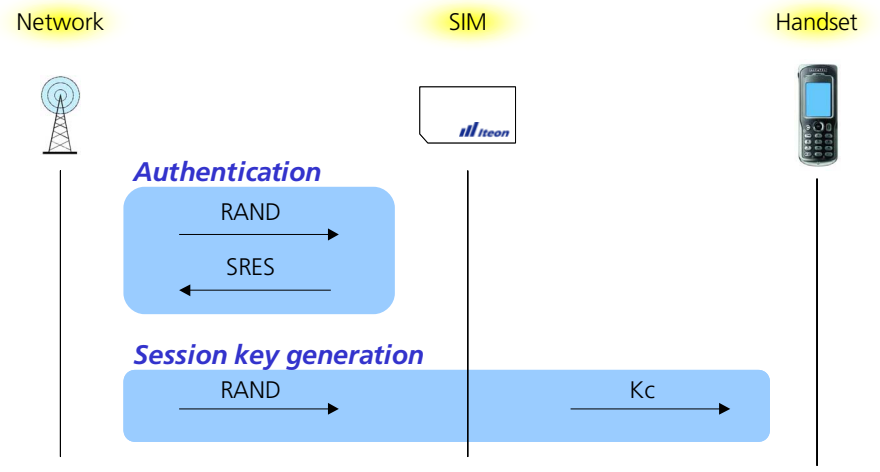
In EAP TLS, the station and the RADIUS server will exchange their certificates, via the access point, in order to authenticate each other (mutual authentication), then they will establish a secure channel (encrypted) by deriving a session key. On this secure channel, the server will then be able to send the WEP key to the station.

EAP SIM : leveraging the GSM infrastructure

The EAP SIM protocol is today a draft RFC (i.e. a draft IETF standard) describing how to use the existing SIM cards to store secrets for EAP authentication. EAP SIM leverages mobile operators' existing infrastructure. The SIM authentication is done, just like today, by the network's authentication centre (AuC).

While the GSM authentication process does not provide mutual authentication, EAP SIM has been designed in order to do so without tampering with compatibility.

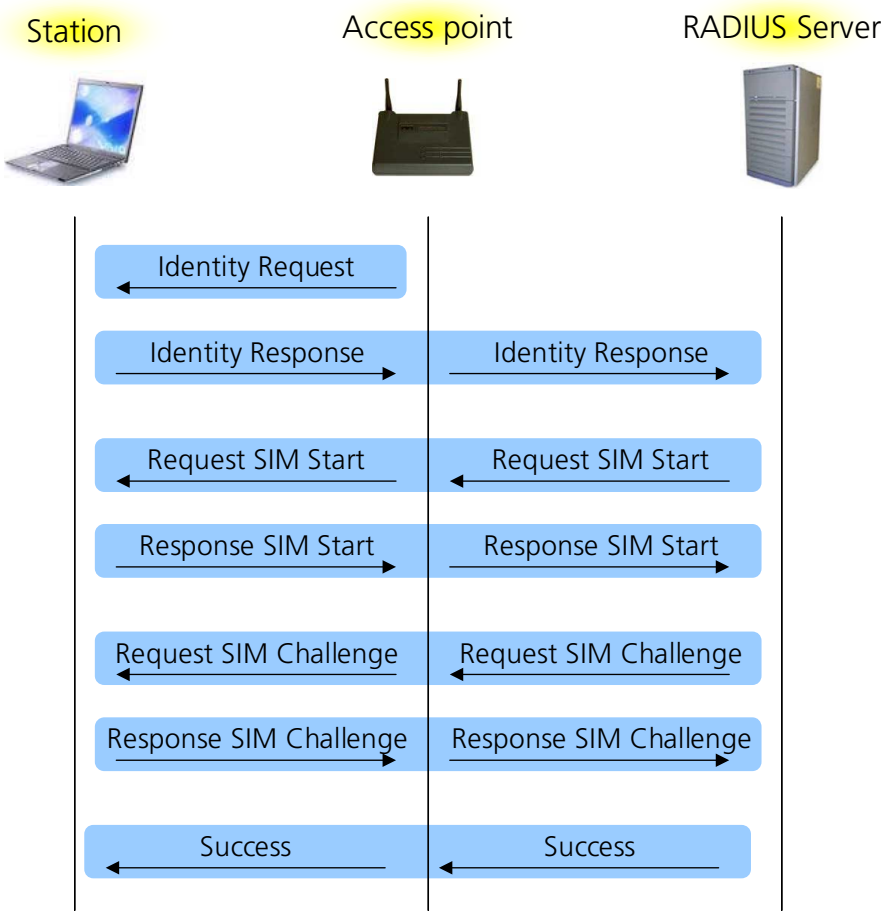
The GSM SIM holds an identity (IMSI) and a secret key (Ki). To authenticate the SIM, the network sends a challenge (RAND), the SIM signs this challenge using its secret key and send the result SRES back to the network. Depending on the result access is granted or denied. To create a session key Kc, the SIM encrypts the RAND challenge.



In the EAP SIM, we have a different mechanism – even if it is reusing the existing SIM and network infrastructure – allowing to provide mutual authentication and generation of key material.

We will give here a simplified description of EAP SIM. The protocol uses three roundtrips.

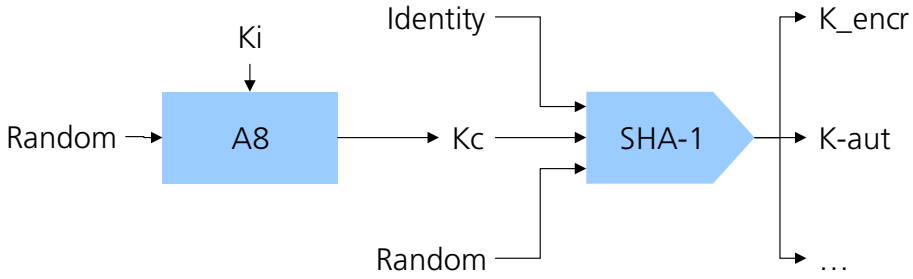
First, the EAP Identity Request / Response messages allow the server to retrieve the user's identity.



The second message exchange EAP Request/SIM/Start and EAP Response/SIM/Start allow the parties to negotiate some parameters. The station sends a random number to the server. Let us call this random number 'challenge 1'.

The server establishes a connection to the GSM authentication centre to get some cryptographic data related to the SIM card of the user. Using this cryptographic material it generates the response to 'challenge 1', a MAC (somehow similar to a signature) and sends it to the user along with a new random number that we will call 'challenge 2'.

The user runs the card's GSM algorithm using 'challenge 2' and gets SRES and Kc, as usual for a SIM card. The station now uses Kc[1] with some other data to generate the cryptographic material : a key for authentication (K-aut), one of encryption (K-encr) and application specific keys.



Using the K-aut key, the station can now verify the response to its 'challenge 1' sent by the server and can therefore authenticate the server.

In turn, the card generates the response to 'challenge 2', and sends it to the server, finishing mutual authentication.

To complete the protocol, the server sends an EAP/Success message to the station (or EAP/Failure if something went wrong).

We saw here that EAP SIM provides mutual authentication and secure session key generation.

Security considerations

It is not always evident to use a card designed for a specific environment in another one. For example, the GSM network does not provide mutual authentication. This is not a major flaw as it is quite complex for an fraudster to operate a fake base station. However, in a WLAN environment it becomes very easy. That is why EAP SIM has been designed to support mutual authentication, in order for the card to be able to authenticate the GSM network.

Still, some attacks exist due to the openness of the WLAN station. For example, an attacker could gain access to cryptographic material (so-called triplets) by passively sniffing the radio interface. An active attack would involve a virus on the station getting triplets from the SIM and sending it to the attacker allowing him then impersonate a valid network.

[1] To be more precise, several randoms are received and several Kc are generated to enhance security.

Integration of smart cards with WLANs

Today, there is no card readers in devices connecting to WLANs. We will explain first how to connect a card to a station, and then what part of the protocol is handled by the card and by the station.

There are several ways to connect a smart card to a station.

The first one involves the connection of a standard reader, which would not be very convenient. Still standard PC/SC readers for cards at the SIM format are already available in the form of a USB token.

© Advanced Card Systems, Ltd.

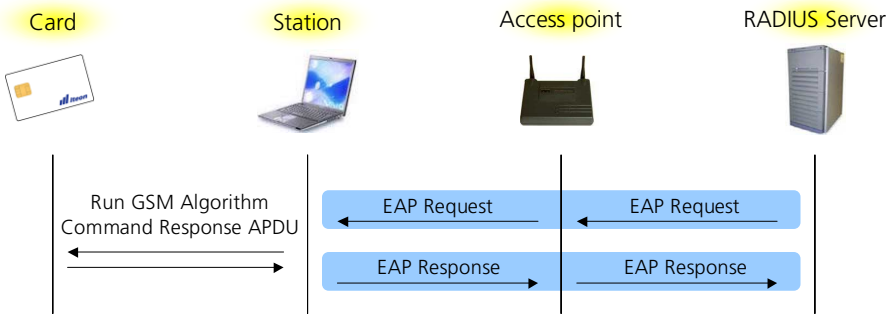
Another way to accept smart cards is directly in the network adaptor. Nokia has already released a PCCARD WLAN adapter, equipped with a smart card reader.

© Nokia.

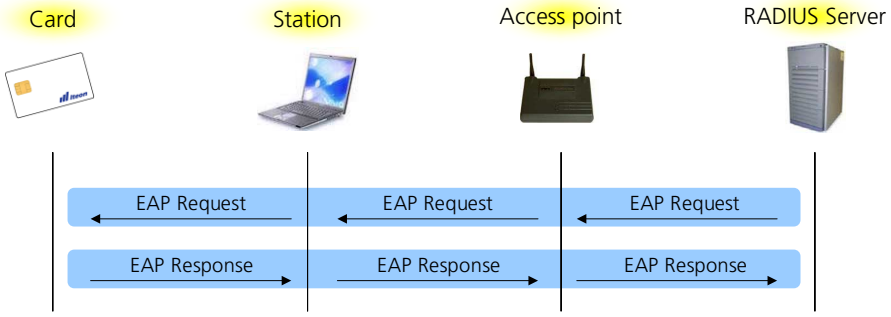
For laptops already integrating a WLAN adapter, the SIM card may just be inserted in a hatch, like in GSM phones. Finally, phones could be WLAN capable and be used as a modem. The link to the station would then be infrared or Bluetooth.

A second aspect to the investigated is which part of the protocol is handled by the card.

In a classic architecture, the EAP protocol would be handled by the station which would only require the card to handle cryptographic operations. For example, in the case of EAP SIM, a piece of software on the station would send some RUN GSM ALGORITHM commands to the card and include the results in response EAP packets.



Another way to proceed is to have the card processing EAP packets itself. This is not a complex task and therefore should not increase the price of the cards. A internet draft already has been published to describe a standard way to do so.



This method is undeniably elegant as it provides end-to-end EAP. All is needed is a piece of software in the PC to map the EAP packets to the smart card which would be able to handle any – one or several – EAP methods.

However an 'EAP engine' must be present on the card. Even if this raises no technical issue, in the case of EAP SIM, the existing SIM cards could not be used as they do not have such an EAP engine. This might be a problem.

What is going on ?

As the smart card industry becomes aware of this opportunity we saw recently several initiatives for the integration of smart cards with WLANs.

Some operators started limited scale pilots to validate the technology, France Telecom will even integrate it in its commercial offer, some companies were incorporated to develop solutions and the industry founded a consortium to "promote WLAN smart card related specifications for wireless LAN mobility management".

Additional services on a WLAN smart card

On a more prospective point of view, once smart cards get integrated with WLANs we could foresee the emergence of new services on the card and the adoption of the card by new kind of devices.

If smart cards are present in WLAN stations such as laptops, we could foresee many new applications. The integration of an EMV application – the standard for smart payment cards – onto such a card would allow users to pay for airtime or for any other services or goods. Payment associations would be able to leverage their existing network, dealing with standard EMV transactions. Other applications could include digital signature

The other path for development would be to integrate a WLAN interface in phones, allowing users to use a single radio infrastructure. Protocol such as Voice other IP (VoIP) could then be used, the WLAN smart card playing the role of a subscriber identity module.

Conclusions

Smart cards appear to be the best solution to secure WLANs. Still, the business model is not well defined. If the interest of WISPs is evident, the added value for a home network is not evident. In between, corporate networks may see in this technology a solution to their current security problems.

Acronyms

- AP Access Point
- DLL Dynamic Link Library
- EAP Extensible Authentication Protocol
- EMV Europay, MasterCard, Visa
- IETF Internet Engineering Task Force
- IMSI International Mobile Subscriber Identity
- LAN Local Area Network
- RADIUS Remote Authentication Dial-In User Service
- RC4 Rivest's Cipher #4, the stream cipher used in WEP
- RFC Request For Comment, name for IETF standards
- SIM Subscriber Identification Module

- TKIP Temporal Key Integrity Protocol
- TLS Transport Layer Security (SSL)
- USB Universal Serial Bus
- USIM Universal Subscriber Identification Module (SIM for 3G)
- VPN Virtual Private Network
- WEP Wireless Equivalent Privacy
- WISP Wireless Internet Service Provider
- WISPr Wireless Internet Service Provider Roaming
- WLAN Wireless Local Area Network
- WPAN Wireless Personal Area Network
- XOR Exclusive OR, a logical function

References

- H. Haverinen, J.Salowey, "EAP SIM Authentication", draft-haverinen-pppext-eap-sim-07.txt, November 2002 (work in progress).
- P.Urien, A.J. Farrugia, G.Pujolle, M.Groot, "EAP support in smartcards", draft-urien-eap-smartcard-00.txt, October 2002 (work in progress).
- WLAN smart card consortium, http://www.wlansmartcard.org.

Contact

Jerome Ajdenbaum

Iteon
6, rue Camille-Desmoulins
92300 Levallois-Perret - France

Phone : +33.1.5676.6026
Fax : +33.1.4759.0736

jerome.ajdenbaum@iteon.net
www.iteon.net

About Iteon

Iteon is an independent smart card consultancy. Since its creation, in 2000, it has been helping organisations to develop new products, offer new services and be successful in their migration projects.

Our fields of experience cover smart cards for the financial sector, telecom and wireless LAN networks, identity. We advise our customers on business and technical strategy, represent them in standardisation bodies, define migration plans, write technical specifications, make product plans, give trainings and develop card software.

In the smart card for WLAN sector, Iteon brings to the industry players marketing and technical support, representation to standardisation bodies and trainings for their marketing, sales and technical staff.