Deploying new Wireless Standards in Corporate Environments

Florent Bersani, Laurent Butti, Jérôme Razniewski
France Telecom R&D*

April, 2004

Keywords: IEEE 802.11, IEEE 802.11i, WPA, IPsec, security.

Abstract

Deploying IP security (IPsec) protocols for secure wireless access is an efficient short-term solution. Unfortunately, this option has both some technical and economic drawbacks (performance issues, non-IP protocols and multicast are not handled, equipments cost...): an alternative solution is required. In parallel with the Institute of Electrical and Electronics Engineers (IEEE) standardization process, the Wi-Fi Alliance began to specify a new standard, Wi-Fi Protected Access (WPA). This new standard is a subset from [IEEE 802.11i] draft 3.0 that aims at implementing what is stable was stable within IEEE 802.11i at the time WPA was written. It improves drastically authentication, access control, confidentiality and key management. These security features are both robust and flexible: they fulfill most corporate requirements in terms of technical and security constraints. Architectures based on WPA can be deployed now, if technical choices and security processes are rigorous: e.g. mutual certificate-based authentication, robust encryption only, no "backward-compatible" mode, logical segmentation between administration and user data, applied security policy, security audits... Thanks to the lessons learnt from France Telecom R&D experimental deployment we provide some insights on particular issues with deploying new wireless standards such as software installation, re-authentication during handover, certificate revocation list checking...

1 Introduction

[IEEE 802.11] specification was ratified in 1997, and lightly modified in 1999. Since this ratification, lots of wireless networks have been deployed around the world, and particularly in the United States. But, some publications about conceptual issues in IEEE 802.11 security specification appeared in October 2000 [JW00]. Papers about IEEE 802.11 security, and its weaknesses are now numerous and are essentially related to issues with the Wired Equivalent Privacy (WEP) protocol [FMS01]. Some proof-of-concept tools[1] were published and proved that wireless technologies could not be deployed without any upper security layer.

From a corporate point of view, one of the most important requirement is security! If security cannot be achieved, deployments are unacceptable. Authentication must be bullet-proof and confidentiality mechanisms must be resistant as radio diffusion is difficult to master. Today, most corporate wireless deployments are based on IPsec tunneling with certificate-based authentication. This is an effective short-term solution that fulfills most technical constraints and requirements. In parallel, the standardization process evolves quickly and seems to be mature enough now: it shall provide enhanced security at Open Systems Interconnection (OSI) layer 2.

This paper is a guideline for deploying new wireless standards in corporate environments. In the first section, a brief overview of issues with legacy wireless standards will be exposed. Then,

*France Telecom R&D, 38-40 Rue du General Leclerc, 92794 Issy-Les-Moulineaux Cedex 9, France. email: [florent.bersani, laurent.butti, jerome.razniewski] AT francetelecom.com

[1] AirSnort, BSD-airtools, WEPCrack

we will describe the most deployed wireless architecture which is based on IPsec. Next, a state-of-the-art of new wireless standards will be performed in every technical areas (confidentiality, authentication...). After this snapshot, a deployment guideline of most relevant technical choices regarding architecture and security will be exposed, is shall provide the reader with an overview of all corporate deployment constraints, architecture design and technical specifications that must be taken into account for a successful deployment. Lastly, we will present the France Telecom R&D case study where new wireless standards are currently being deployed since late 2003: a complete technical description and experience returns will be emphasized.

2 IEEE 802.11 Issues

This part is short reminder of the dramatic failures of the previous security protocols of IEEE 802.11-1999.

2.1 The dramatic failures of WEP

It is worth having in mind the failures of the previous "security protocol" of 802.11. Basically, this protocol lacked:

- Precise goals;
- Robust authentication;
- Robust data protection;
- Key management.

2.2 No precise goals

It was only stated in IEEE 802.11-1999 that the WEP (Wired Equivalent Privacy) was "intended to provide functionality for the wireless Local Area Networks (LAN) equivalent to that provided by the physical security attributes inherent to a wired medium".

2.3 No robust authentication

The two mechanisms proposed in IEEE 802.11-1999 ("Open system" and "Shared Key") did not provide any security:

- "Open system" was essentially a null authentication that is to say the station (STA) merely asserts its identity and the access point (AP) trusts it without requesting any proof of it;
- "Shared Key" supported authentication of STAs as either a member of those who know a shared key or a member of those who do not. "Shared Key" was proved to be completely flawed.

2.4 No robust data protection

The WEP encapsulation was proved to provide neither confidentiality (with two flavors of attacks: plaintext recovery and key recovery) nor integrity.

2.5 No key management

The standard only specified that the secret key "has been distributed to cooperating STAs by an external management service".

3 Workaround: Upper Security Layer

3.1 Introduction

Wireless networks based on legacy security mechanisms, with all available security features activated (WEP/104[2], Medium Access Control (MAC) address filtering, hidden[3] network name...) are vulnerable to attacks within one day, on both authentication, privacy and access control, enabling the attacker to have full access to internal networks! But wireless is magic, user-friendly and must be deployed! In 2001, when the [FMS01] paper was published, no solution was available to deploy a secure wireless access, but a secure solution was needed. In an obvious way, using an upper security layer for wireless communications represents a serious option. This can be achieved with several technologies: Secure Shell (SSH), Secure Socket Layer (SSL) and IPsec. All these secure protocols are commonly used in IP world, especially for administration purposes, web communications and remote access.

3.2 Secure wireless communications with IPsec

Since 3 or 4 years, IPsec technologies are mastered and often deployed for nomadic access to corporate Intranets. That's why securing wireless access with IPsec technologies is really straightforward, as it is available now! IPsec provides the nomadic users with confidentiality and authenticity. Whatever the kind of physical medium the user has (Public Switched Telephone Network (PSTN), Digital Subscriber Line (DSL), Integrated Services Digital Network (ISDN), 802.11, ...), it is possible for him to connect to the Intranet with IPsec, and to ensure that all communications are both encrypted and authenticated. This solution is deployed at France Telecom R&D since early 2002 and is mostly used in meeting rooms. Of course, this solution represents a short-term solution that fatally has some drawbacks, but it fulfilled most of our requirements at the time of the deployment. In this part, we will describe the IPsec solution as it is deployed at France Telecom R&D.

To summarize all pros and cons for the IPsec solution, two lists are enumerated below. To begin, IPsec solution major advantages are:

- IPsec is independent of OSI lower layers (xDSL, IEEE 802.11, ...);
- IPsec is approved by the scientific community, and proved to be reliable and robust especially from a cryptographic point of view;
- the solution is suitable for all situations whenever remote access to the Intranet is needed: meeting rooms, hot spots, corporate and home;
- the configuration of the user's software is unique despite the multiple possible access networks: only an IPsec client is necessary on the user's computer to face all situations;
- the IPsec box is the unique entrance door to the Intranet, which makes it easier to manage than a distributed solution;
- it is possible to choose the best adapted IPsec box for the company financial capacities.

IPsec solution major drawbacks are:

- there might be some performance issues on the IPsec concentrator that has to handle all the traffic, it is a key factor especially with large deployments;
- the 802.11 access architecture must be carefully designed, as access points, switches, IPsec concentrators and Dynamic Host Configuration Protocol (DHCP) equipments are directly

[2] WEP/104 uses a 104-bit shared secret

[3] the ability to hide any network name advertisement usually present in beacon frames, i.e. these frames are not sent anymore

accessible with an Open[4] IEEE 802.11 authentication: these equipments are open to attacks (like DHCP starvation, protocol flooding, remote exploit on vulnerable applications...) from unknown[5] users as access control is not achieved at layer 2;

- Address Resolution Protocol (ARP) attacks are feasible, leading to trivial denial-of-service attacks;
- the clients' security relies on a proprietary "blocking-mode[6]" feature and filtering functionalities usually implemented in IPsec software that are difficult to master especially if the computer is already compromised;
- non-IP protocols cannot be carried within IPsec tunnels which can be a serious drawback in some environments;
- multicast and broadcast are not handled which can be a serious drawback especially for multimedia services;
- multi-location deployment implies the use of multiple concentrators, or multiple leased lines to a central concentrator which leads to higher costs;
- there are other cost issues for large deployments (as IPsec clients and concentrators are not free!).

3.3 Summary

IPsec is a not an exclusive short-term solution to secure wireless access, it is also possible to use SSH, SSL or any other cryptographic protocol. But IPsec is certainly the most deployed today, and represents a robust solution, where security mechanisms are well reviewed by cryptographic experts even if overall security is not perfect because access control is not performed at layer 2. Man-in-the-middle or passive eavesdropping attacks are impossible when strong[7] authentication and encryption mechanisms are activated. But this solution fails in some specific contexts (non-IP protocols, multicast), and the overall cost of a multiple-location deployment is really huge (client softwares, concentrators, leased lines...): an alternative solution is needed. Also it is important to note that upper layer security solutions must be considered as remote access, which is inherently different from local area network access.

4 New Wireless Standards

These standards should be fully adapted for wireless communications, as they are inherently designed for local area networks! First part briefly describes IEEE 802.11i specification, which is currently being standardized (Draft 8.0, February 2004). The second part is focused on security features implemented in these new standards regarding our wireless deployment with these standards.

4.1 Standards

4.1.1 IEEE 802.11i

IEEE 802.11i tries to address all cited shortcomings, namely, it defines:

[4] it is equivalent to "no authentication"; typically, IPsec deployments do not implement WEP shared secret as it do not provide higher security, and managing an unique shared secret between all clients and access points is not feasible in large deployments

[5] in the sense non-authenticated

[6] this is a specific feature of IPsec client softwares which purpose is to avoid bounce attacks between external connections (typically the Internet) and the Intranet

[7] in the sense certificate-based for authentication, and "well reviewed by cryptographic experts" for both authentication and encryption

- Its goals;
- Robust authentication mechanisms based on IEEE 802.1X and Pre-Shared Key (PSK);
- Robust data protection with Temporal Key Integrity Protocol (TKIP) and Counter Mode CBC-MAC Protocol (CCMP);
- Key management based on IEEE 802.1X;
- A framework to establish a secure association called Robust Security Network Association (RSNA).

Defining one's goals is the mandatory preliminary to robust security. 802.11i essentially aims at providing a secure channel on an insecure link. In 802.11i jargon the secure channel is called a RSNA and the way to maintain the secure channel is referred to as RSNA data privacy protocols.

4.1.2 WPA: Wi-Fi Protected Access

WPA is a standard from the Wi-Fi Alliance[8], and was announced October 31, 2002. It is a subset from [IEEE 802.11i] Draft 3.0 specification, and implements most stable security features at the time of the specification. This standard was designed to provide security in both corporate, residential and hot spot[9] architectures. The idea was to "implement what is stable and bring it to market" now!

WPA is basically:

- authentication mechanisms based on PSK and Internet Engineering Task Force (IETF) Extensible Authentication Protocol (EAP);
- new confidentiality and integrity mechanisms based on TKIP;
- new key management based on IEEE 802.11i's;
- backward-compatible and software upgradeable with legacy technologies.

WPA represents a drastic improvement from a security point of view. Mandatory WPA certification since September, 2003 shall accelerate secure wireless deployments with new wireless security standards.

4.2 Security features

4.2.1 Authentication and access control

Authentication methods are critical, as it could represent the first security breach. Regarding authentication, the user will be accepted or not. That's why, authentication methods must be carefully evaluated and elected regarding the technical context. A balance between security and ease of use should be also performed. This part describes all available authentication methods, and gives some hints about their ability to fit in small, medium or large corporates.

Both 802.11i and WPA provide two authentication methods:

- PSK, which is derived from a shared secret[10] between clients and access points;
- EAP, which is a framework for EAP-based authentication methods.

[8] the Wi-Fi Alliance is a nonprofit international association formed in 1999 to certify interoperability of wireless Local Area Network products based on IEEE 802.11 specification (source: Wi-Fi Alliance)

[9] public Internet access zone with wireless technologies

[10] for user convenience, it is usually an ASCII password

Authentication methods are flexible enough to be deployed in multiple environments where authentication could (or must) be different (login / password, certificate, Subscriber Identity Module (SIM) authentication[11] (cellular operators) card...).

When EAP authentication is used, a back-end authentication server (typically an Authentication Authorization Accounting (AAA) server) is necessary to process user authentication. Obviously, this kind of architecture cannot be easily deployed for a residential gateway. Contrary to this, PSK authentication method does not require a back-end authentication server, so it should be deployed for home users or small corporates.

Different kinds of authentication methods are available:

- PSK: pre-shared secret;
- Transport Layer Security (EAP-TLS): mutual certificate-based authentication;
- EAP-TLS-EAP[12]: server-side certificate-based authentication with an inner client-side EAP authentication (typically a login/password EAP authentication method);
- Tunneled Transport Layer Security (EAP-TTLS): server-side certificate-based authentication with an inner client-side authentication (contrary to PEAP, it is not necessarily an EAP authentication method);
- EAP-[Archie/Shared Key Exchange (SKE)/Pre-Shared Key (PSK)]: mutual shared secret authentication.

Choosing EAP as the authentication framework drastically improved flexibility regarding authentication, which is now one of the best strength of new wireless standards.

Access control is performed at edge (i.e. at access point):

- with PSK authentication, access point and client perform an implicit[13] authentication, upon result, the user will be enabled or not to communicate with the network behind the access point;
- with EAP authentication, client and authentication server perform an EAP authentication, upon result, the user will be enabled or not to communicate with the network behind the access point.

Last point requires attention, as authentication data must go through the access point to the authentication server: this should be the only option for the attacker to compromise the network (e.g. exploiting a buffer overflow with malformed EAP frames...).

4.2.2 Key management

[IEEE 802.1X-2001] is an IEEE standard that enables authentication and key management for IEEE 802 Local Area Networks, including Ethernet. Wireless legacy key management was based on this standard that was specified only for wired networks. As a matter of fact, some weaknesses are inherent to wireless networks, and needed to be addressed in IEEE 802.11i specification: an amendment to IEEE 802.1X-2001 standard is currently being standardized in [IEEE 802.1aa] standard. With this new revision in IEEE 802.11i, it is possible to:

- prove liveness of peers;
- establish fresh pairwise (for unicast traffic) and group (for multicast traffic) key hierarchies;
- avoid man-in-the-middle attacks;

[11] used by Global System for Mobile Communication

[12] a.k.a. PEAP, Protected EAP

[13] in the sense, if client and access point have a different shared secret, they cannot communicate to each other: authentication is not successful

- verify installation of keying material for encryption and integrity.

This enhances overall level of security as key hierarchies will feed confidentiality and integrity protocols with fresh and confident keying material. It is important to note that "backward-compatibility" mode ensures that WPA is fully compatible both with IEEE 802.1X-2001 and IEEE 802.11i key management.

4.2.3 Confidentiality and integrity

Two new confidentiality and integrity mechanisms are defined in IEEE 802.11i specification, TKIP and CCMP. The first one is based on [RC4], and the second one is based on [AES]. Main objectives were to support legacy hardware that do not implement AES which is required for CCMP. As WPA is a subset of IEEE 802.11i Draft 3.0, only TKIP protocol is included in WPA specification. To be more precise about security enhancements, TKIP provides:

- confidentiality thanks to enhanced data encryption based on RC4;
- integrity and authentication thanks to the Message Integrity Check (MIC) and the counter-measures;
- replay protection thanks to a 48-bit sequence number acting as a counter.

It is worth to note that WPA standard specifies an optional encryption mechanism, that can be CCMP. Effectively, some pre-802.11i equipments are WPA compliant with a CCMP implemention.

4.3 Support status

WPA compliant equipments must be available both for authenticator and supplicant, moreover EAP authentication methods must be supported both by supplicants and authentication servers.

A list of current WPA certified products is available at `http://www.wi-fi.org/`: today, WPA compliant equipments are available for most interfaces (PCMCIA, mini-PCI, USB, Compact Flash).

Current WPA support in operating systems:

Operating System	Status
Windows XP	Yes, with SP1
Windows 2000	Yes, with Odyssey WPA
Windows 98/Me	Yes, with Odyssey WPA
Linux	Yes, with HostAP, proprietary drivers, or wrappers

WPA support is very restrictive in terms of operating systems, as third-party softwares are required to support Microsoft 2000/98/Me platforms.

Supported EAP authentication methods in RADIUS software:

RADIUS	TLS	PEAP	TTLS
Microsoft IAS	Yes	Yes	No
Steel Belted 4.5	Yes	Yes	Yes
FreeRADIUS 0.9.3	Yes	Yes	Yes
Secure ACS 3.0	Yes	Yes	No

Supported EAP authentication methods in client software:

Client	TLS	PEAP	TTLS
Windows XP SP1	Yes	Yes	No
Windows 2000 + Patch	Yes	No	No
Odyssey WPA (XP/2000/98/Me)	Yes	Yes	Yes
XSupplicant (*nix)	Yes	Yes	Yes
WPAsupplicant (*nix)	Yes	Yes	No

Most EAP authentication methods are supported in most EAP clients and servers, only shared key EAP authentication methods are not widely available at the moment.

5 Guidelines for a Successful Deployment

In this section, a summary of available technical choices for deploying new wireless standards is firstly described. In the second part, the France Telecom R&D case study will be fully described and explained.

5.1 About standards

5.1.1 Authentication and access control

Obviously, technical choices are tied with technology constraints, especially regarding authentication methods. For example, a certificate-based mutual authentication method is only relevant in a Public Key Infrastructure (PKI) ready corporate. Otherwise, deploying a full PKI only for a wireless network deployment is really disproportionate.

Consequently, each authentication method has its advantages and drawbacks, both in terms of security and management, they are tied with a particular context and must be carefully selected:

- PSK is perfect for home users or small corporates as managing a shared secret in a small and closed environment is feasible;
- EAP-TLS is perfect for PKI-ready corporate as re-using existent PKI architecture can provide both a high level of security and integration (thanks to PKI security policy);
- PEAP and TTLS (with inner login/password authentication method) are perfect for lightweight[14] deployments with existent users databases that are commonly based on login/password (Active Directory,...);
- EAP-[Archie/PSK/SKE] shall provide a good lightweight solution both for small, medium, and large corporates.

To sum up, a "good" EAP authentication method must be the right balance between security, architecture and availability[15] constraints. Password based EAP methods can not be considered as robust as certificate based, because they are vulnerable to dictionary and brute force attacks that are unfortunately emphasized by radio diffusion. As a consequence, when deploying a password based authentication method, the password security policy must be drastic. Another option is to implement One Time Password (OTP) technologies that mitigates these risks, but must be also carefully evaluated regarding user ergonomics if multiple re-authentications are frequently needed. Finally, another important aspect must be underlined, as most EAP authentication methods are still currently being standardized, it certainly has impacts on interoperability, and last but not the least migration procedures toward future standards must be carefully addressed.

5.1.2 Key management

IEEE 802.1X-2001 is known to be weaker than IEEE 802.11i regarding key management. So, to achieve a good level of security, it is mandatory to support only IEEE 802.11i's key management, even if it drops WPA "backward-compatible" mode, i.e. legacy clients (i.e. not WPA compliant) will not inter operate with deployed solution.

5.1.3 Confidentiality and integrity

TKIP seems to meet its entire design goal, which is to provide a tolerable level of security that can be implemented as a software upgrade on legacy hardware. Its design team includes well-known cryptographers, and, unlike WEP, it has received extensive review both by the broader security community for correctness and by the 802.11 hardware vendors for feasibility. It trades off security

[14] in the sense, without large impacts on architecture
[15] in the sense, implementation availability and guaranteed interoperability

to achieve acceptable performance, and it is not the ideal solution. TKIP is an interim solution to support 802.11i on legacy hardware. It is not considered as secure as the AES solution (CCMP) but very much better than WEP.

As WPA is "backward-compatible" with legacy security mechanisms (WEP), it is possible to deploy a mixed solution with TKIP and WEP. This is definitely not recommended if security is a concern: TKIP should be mandatory for confidentiality and integrity.

5.2 Case study: France Telecom R&D

This part describes the France Telecom R&D experimental deployment. Firstly, all technical choices regarding wireless security features and architecture design are described. Then experience returns try to pinpoint all encountered difficulties during the deployment.

5.2.1 Technical choices

France Telecom R&D has deployed a corporate wireless infrastructure with new wireless security standards, with below technical choices. It may be a summary of later chapter for a large corporate:

Robust authentication method: EAP-TLS This method is standardized as a Request For Comments (RFC) standard since 1998. This is definitely a strong advantage in terms of interoperability and perenniality. Certificate based authentication methods are known to be resistant to brute force attacks. EAP-TLS is the best adapted method for PKI ready corporate.

Robust confidentiality and integrity protocol : TKIP This is definitely mandatory to achieve a strong level of confidentiality.

Robust key management: IEEE 802.11i This is definitely mandatory as mixed clients with legacy key management is a potential security breach.

Robust authentication tokens: smartcards This is known to provide a stronger security[16] than disk storage. Moreover, all PKI procedures to create certificates and smartcards are already defined and applied which is very interesting to re-use in a wireless context.

Robust architecture It is necessary to deploy a closed administration network for both authentication and administration traffic with logically segmented architecture between administrative and user Virtual LANs (VLANs). This is critical to enhance architecture security. Most access points have VLAN capabilities, so logical segmentation between different class of users (regarding user authentication) is possible. Moreover, authentication databases (in our case, a PKI related databases) must be interconnected with administrative network which implies some obvious security constraints.

Robust security policy Regarding authentication and smartcards management, the PKI security policy is already defined and applied. But for wireless access with new wireless standards, a classic security policy has to be defined and applied. A secure configuration of all access points and servers was created: minimize open services, secure administration with secure protocols (SSH), centralized administration, unpriviligied processes jailed (especially `radiusd`). Moreover, some periodic wireless security audits were performed to check overall status of the deployment: geographical radio diffusion survey (tune power transmit controls), pen-testing (tests on EAP authentications). Then a log policy was defined regarding centralized logging of EAP authentications (better for management purposes) and analysis of EAP authentications thanks to scripts (statistics of failed and successful authentications, weird events). Lastly, a wireless Intrusion Detection System was deployed, which aims at logging all suspicious wireless events: fake access points, multiple

[16] robustness and reliability

de-authentications and disassociations that are known to be a clear sign of active man-in-the-middle attacks.

Practical choices Equipments were selected with security, features and compliancy in mind:

- Supplicants: Windows XP SP1, and experimental tests with Odyssey Client on Windows 2000;
- Wireless cards (only WPA certified): Cisco, Lynksys, Centrino;
- Authenticator (only WPA certified): Cisco Access Point series;
- Authentication Server: FreeRADIUS;
- Administrative operating systems: GNU/Linux Debian (testing).

Of course, all software and firmware versions are regularly updated according to bug and security fixes.

5.2.2 Experience returns

Handover requires re-authentication: connectivity issues WPA does not support fast handover between access points. It implied connectivity issues when roaming because it is time consuming. It can be reduced (for TLS) by TLS session resumption feature, but it is not implemented in FreeRADIUS. Also, it is worth to note that multiple re-authentication reduces log readability (this issue must be addressed thanks to scripts).

Software: installation issues We encountered some conflicts between several drivers of different cards, especially when upgrading with recent drivers.

Personal Identification Number (PIN) code issues: smartcard locking Issues with the smartcard PIN code interface were encountered leading to smartcard locking (three bad tries maximum).

Certificate Revocation List (CRL): must be checked For a certificate based authentication method, the overall level of security depends on security policy and CRL checking. A CRL must be checked both by the server and client: this implies requirements on softwares (static preconfiguration) and architecture interconnections. Also a CRL can represent several kilobytes, especially with large corporates. So, checking online at every authentication could represent a bad option, because of delays retrieving a large file. We chose to retrieve CRL periodically every hour (any revoked certificate has a maximum window of opportunity of one hour). Another option should be to support Online Certificate Status Protocol (OCSP) both in EAP-TLS supplicant and authentication server. Also, note that it is very difficult to check server certificate revocation if OCSP is not supported: how to check the CRL without any physical access?

Static configuration: difficult to define, apply and accept It is very difficult to define a static configuration for laptop users as they can be used at home, conferences for wireless access with IPsec. For example, a static wireless configuration to connect only with specific security features is impossible to apply if it reduces drastically users ergonomics.

Authenticating with user certificate: authentication issues Certificates are delivered to users, and authentication is performed with users credentials. It is particularly interesting from a nomadic user point of view, but implies some difficulties regarding authentication. As a matter of fact, an user authentication can not occur as a machine authentication. To sum up, a domain log-on should not be possible as the machine is not physically interconnected (authenticated) to the

wireless domain. A specific feature exists in some operating systems: cached credentials that enable an user to connect artificially to its domain without any physical connection. After this "local" authentication, the wireless authentication occurs, providing the user with a full IP connection and accessing to its domain.

Improve authorization: Lightweight Directory Access Protocol (LDAP) integration In order to improve authorization procedures, we implemented a LDAP server containing a tree with a remote access policy control (accept or not, login date) in order to inter operate with FreeRADIUS authorization module. It gives the site administrator with an opportunity to change easily users' remote access policy. At the moment, we integrated this solution with OpenLDAP, and we plan to integrate this solution with an Active Directory server.

Improve automatic configuration: User Principal Name (UPN) checking Windows XP Wireless Zero Configuration retrieves the UPN located in the smartcard for automatic feed with EAP Response Identity (the UPN is also used for client domain authentication with the smartcard logon procedure). For an improved security, we decided to check both UPN present in EAP Response Identity and the UPN present in user certificate sent by EAP-TLS authentication processes. This avoids some malicious actions to authenticate as user1 with an user2 certificate (remember that authorization is performed with EAP Response Identity).

5.2.3 Examples

Architecture deployed:

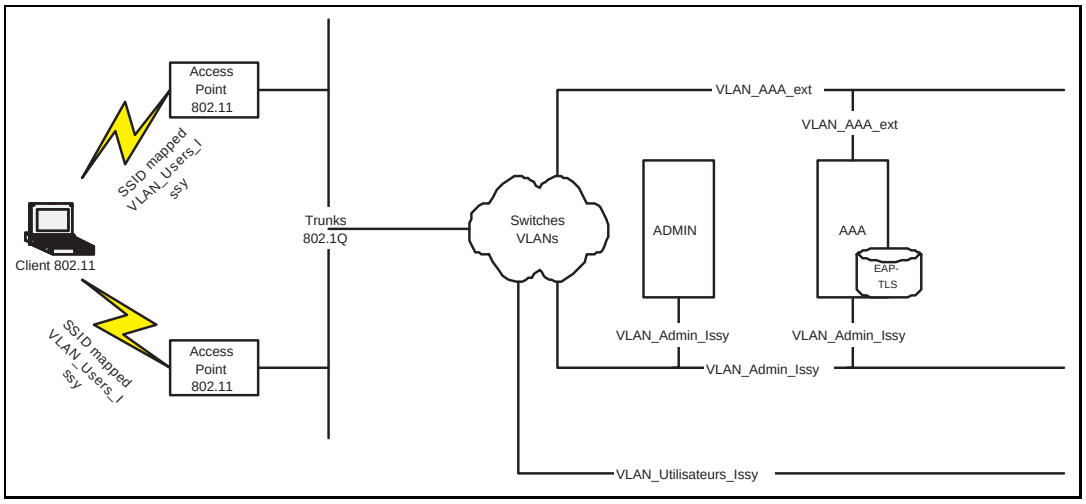

Figure 1: Architecture overview

User certificate example:

```
Certificate:
Data:
Version: 3 (0x2)
Serial Number: 1533 (0x5fd)
Signature Algorithm: sha1WithRSAEncryption
Issuer: C=FR, O=France Telecom, OU=FTRD-Aspic, CN=FTRD AC operationnelle
Validity
     Not Before: May 13 09:30:03 2003 GMT
     Not After : May 12 09:30:03 2006 GMT
```

```
Subject: C=FR, O=France Telecom, OU=FTRD-ASPIC, CN=Laurent BUTTI/
UID=XXXXXXXX/emailAddress=laurent.butti@francetelecom.com
Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (1024 bit)
        Modulus (1024 bit):
            SNIPPED...
        Exponent: 65537 (0x10001)
X509v3 extensions:
    X509v3 Subject Key Identifier:
        95:95:B6:23:E0:54:DB:53:50:42:F7:CD:C7:F9:0B:A0:DD:A1:1C:EA
    X509v3 Authority Key Identifier:
        keyid:A7:87:B8:D0:8B:F4:6F:E3:C1:C0:DA:ED:8E:B4:E0:A7:10:29:FC:D8
    X509v3 CRL Distribution Points:
        URI:http://crl/crl.crl
    X509v3 Key Usage: critical
        Digital Signature, Non Repudiation
    X509v3 Extended Key Usage:
        E-mail Protection, TLS Web Client Authentication,
        Microsoft Smartcardlogin
    Netscape Cert Type:
        SSL Client, S/MIME
    X509v3 Subject Alternative Name:
        othername:<unsupported>, email:laurent.butti@francetelecom.com
    Netscape Comment:
        Certificat de Signature pour Laurent BUTTI
Signature Algorithm: sha1WithRSAEncryption
    SNIPPED...
```

Note that the unsupported "othername" in X509v3 Subject Alternative Name is the UPN, which must be equal to `User-Name` below, i.e. `xyz@realm`.

FreeRADIUS log example:

```
Info: --> User-Name = xyz@realm
Info: --> BUF-Name = Laurent BUTTI
Info: --> subject = /C=FR/O=France Telecom/OU=FTRD-ASPIC/
CN=Laurent BUTTI/UID=XXXXXXXX/emailAddress=laurent.butti@francetelecom.com
Info: --> issuer  = /C=FR/O=France Telecom/OU=FTRD-Aspic/CN=FTRD AC operationnelle
Info: --> verify return:1
Info: undefined: SSL negotiation finished successfully
Info: rlm_eap_tls: Received EAP-TLS ACK message
Auth: Login OK: [xyz@realm/<no User-Password attribute>]
(from client private-network port yyy cli XXXX.XXXX.XXXX)
Info: rlm_eap_tls:  Length Included
Error: TLS_accept:error in SSLv3 read client certificate A
Info: rlm_eap_tls: Received EAP-TLS ACK message
Info: rlm_eap_tls: Received EAP-TLS ACK message
Info: rlm_eap_tls: Received EAP-TLS ACK message
Info: rlm_eap_tls:  Received EAP-TLS First Fragment of the message
Info: error=0
```

Cisco log example:

```
%DOT11-6-ASSOC: Interface Dot11Radio0,
Station    XXXX.XXXX.XXXX Associated KEY_MGMT[WPA]
```

5.2.4 Next steps

Experience returns from this experimental deployment helped us to define a roadmap for new features and architecture, with also the cost constraint in mind which is as usual a strong requirement for a successful architecture. As a consequence, a shared infrastructure between IPsec and WPA seems to be mandatory. It implies migration issues that are critical for a successful operational deployment, and must be taken into account seriously in order to be as soft as possible: a transition period is necessary.

1. IPsec and WPA: wireless access with a shared architecture, i.e. same access points and architecture;
2. IPsec and WPA with dynamic VLANs: same as above, with a dynamic VLAN attribution regarding authentication for WPA users (as an authenticated user belongs to a well known group: marketing, engineering, ...).

Of course, these new deployments have new strengths (in terms of costs and usability), but must be studied carefully as two different class of users are accepted on a same access point: impacts on architecture design and security must be addressed.

6 Conclusions

Deploying new wireless standards in corporate environments is now possible. They provide a large number of possible authentication mechanisms and robust confidentiality and integrity protocols, that fulfills most corporate requirements. To achieve a good level of security, some specific features as "backward-compatible" mode must be deactivated, and a rigorous architecture must be designed. It represents an interesting alternative to IPsec solution that has serious drawbacks both in terms of cost and usability. At the time of writing, one of the major drawback of WPA is related to client-side support, because of limited options (choosing between Windows XP and a third party supplicant that has a cost): this represents a hedge for any WPA deployment. Hope this will certainly get better in the short-term as new offers relying on these new standards will be soon designed and deployed.

7 Acknowledgments

We thank Thierry Baritaud, Olivier Charles, Sylvie Camus and Franck Veysset for their valuable feedback. We also thank Alain Fabre and François Mercier for their support during the experimental deployment. Finally, we thank all the wireless community who motivated us to deploy a secure wireless access with new standards.

References

[JW00] Jesse Walker, *Unsafe at any key size: an analysis of the WEP encapsulation*, `http://grouper.ieee.org/groups/802/11/Documents/DocumentHolder/0-362.zip`, October 2000.

[FMS01] Fluhrer, Mantin, and Shamir, *Weaknesses in the Key Scheduling Algorithm of RC4*, `http://citeseer.nj.nec.com/fluhrer01weaknesses.html`, July 2001.

[OSI] International Organization for Standardization, *Open Systems Interconnection*, `http://www.iso.org`.

[IPsec] IETF, *IP security*, `http://www.ietf.org/html.charters/ipsec-charter.html`.

[WPA] Wi-Fi Alliance, *Wi-Fi Protected Access*, `http://www.wi-fi.org`, 2000-2004.

[IEEE 802.11] IEEE, *Wireless LAN Medium Access Control and Physical Layer Specification*, http://grouper.ieee.org/groups/802/11.

[IEEE 802.11i] IEEE, *Medium Access Control Security Enhancements*, http://grouper.ieee.org/groups/802/11.

[IEEE 802.1X-2001] IEEE, *Port Based Network Access Control*, http://www.ieee802.org/1/pages/802.1x.html, 2001.

[IEEE 802.1aa] IEEE, *Port Based Network Access Control, Amendment 1*, http://www.ieee802.org/1/pages/802.1aa.html.

[EAP] IETF, *Extensible Authentication Protocol*, http://www.ietf.org/html.charters/eap-charter.html.

[RC4] RSA Security, *Rivest Cipher 4*, http://www.rsasecurity.com.

[AES] Joan Daemen, Vincent Rijmen, *Advanced Encryption Standard*, http://csrc.nist.gov/CryptoToolkit/aes/rijndael/.