Enhancing HIPERLAN/2 Security Aspects

Josep L. Ferrer-Gomila, Guillem Femenias, and Magdalena Payeras-Capellà*

Departament de Matemàtiques i Informàtica, Universitat de les Illes Balears
Cra. de Valldemossa km. 7,5, Palma de Mallorca 07122, SPAIN
{dijjfg,guillem.femenias,magdalena.payeras}@clust.uib.es

Abstract. Security services are not contemplated in an appropriate way in the current standards for broadband wireless LANs, namely IEEE 802.11 and HIPERLAN/2. A wrong design of the security architecture, a bad election of cryptographic algorithms and a lack of scalability, are among the criticism that these standards have received. In this paper, the security architecture adopted within the Spanish ICT (Information and Communication Technologies) project DARWIN (Demonstrator of an Adaptive and Reconfigurable Wireless IP Network) is presented. The DARWIN approach, adopting HIPERLAN/2 as a model, incorporates all the basic security services, with a high degree of flexibility and scalability, and correcting some faults of HIPERLAN/2.

1 Introduction

The striking growth of electronic data traffic, the increasing popularity of multimedia applications, and the converging trend of wireless communications and Internet technology, have spurred the evolution from second generation (2G) to third generation (3G) mobile networks and have brought new WLAN standards, like IEEE 802.11 [3] and HIPERLAN/2 [4, 5]. Within the Spanish ICT initiative, project DARWIN is working towards the definition of a flexible broadband WLAN radio access system, based on an IP network platform.

In order to fulfil the requirements on security dictated by higher layers, according to the top down approach adopted within the project, the DARWIN LC (Link Control) layer incorporates some security functions. The principal services that have been considered in the definition of the security architecture are: confidentiality, integrity, access control and authentication (mutual or unidirectional).The security architecture of DARWIN is based on the analysis of the corresponding architecture of HIPERLAN/2, and tries to solve the problems that we have identified in this standard. SSL [1] has been taken as a reference because it's a good security protocol without flaws [2].

First problem to be solved in wireless networks is access control and/or authentication. To achieve mutual authentication, HIPERLAN/2 has two methods: pre-shared key or RSA based authentication. But, it only allows the use of RSA

* This work has been supported in part by the MEC, Spain, and FEDER, under grant TIC2001-0287 and in part by the CAIB under grant PRDIB-2002GC3-18

R. Battiti, M. Conti, and R. Lo Cigno (Eds.): WONS 2004, LNCS 2928, pp. 389–394, 2004.

with three possible key sizes (512, 768 and 1024 bits). This means that if the necessity of using longer keys is observed, HIPERLAN/2 will have to be redefined. We extend the use of RSA to any key size. Besides, HIPERLAN/2 does not foresee the incorporation of the public key infrastructure (PKI) based on digital certificates. We think that in broadband wireless networks, PKI can be deployed in the same way than in wired networks.

A second optional service to be provided is confidentiality. In HIPERLAN/2, this service, when desired, is activated before carrying out the authentication process, and it is not appropriate [6]. The procedure must first begin with the authentication of the parties involved in a communication and then proceed to the key exchange process.

Another problem to be solved in HIPERLAN/2 is integrity/authentication during data transfer phase. If confidentiality service is not activated, data transfer is totally unprotected in HIPERLAN/2. It means that even after a successful authentication phase, the WLAN can be attacked by non authorized users, modifying, altering or inserting data in the wireless network. We add an integrity service, independent of confidentiality service, to solve the described problem.

In this paper we present a proposal that corrects the defects of HIPERLAN/2. DARWIN proposal allows to negotiate the three basic security services: authentication, integrity and confidentiality. The design of the messages, that must be exchanged between the mobile terminal (MT) and the access point (AP), allows to incorporate new algorithms and key sizes without having to redefine the proposal. Anyway, the chosen algorithms are strong enough.

2 Security Architecture in DARWIN

The scope of DARWIN is limited to the lower layers of the OSI reference model: physical and link layers. The link layer distributes its tasks between two sublayers: MAC and LC sublayers. Furthermore, in the LC sublayer we can find a user plane (DLC, Data Link Control) and a control plane (RLC, Radio Link Control). In the control plane three differentiated modules can be found: RRC (Radio Resource Control), AC (Association Control) and DLC Connection Control. In this context, the security functions have been incorporated in the AC module of the RLC.

In order to establish the schedule of incorporation of security services, we have defined five phases: handshake, authentication, key exchange, integrity and confidentiality. Some security functions, like key refresh, security in the handover, etc., will not be described in this paper, even though DARWIN approaches them.

We will use the following notation:

x, y	concatenation of information x and y
$H_f(m)$	hashing of message m with f algorithm
$PR_i(m)$	encryption of message m with the private key of i
$PU_j(m)$	encryption of message m with the public key of j
$E_k(m)$	encryption of message m with the secret key k

3 Handshake

In the establishment stage it is necessary to negotiate which services and algorithms will be used. Related to security services, the MT carries out a proposal and the AP decides which services and algorithms will be used:

1.- MT ← AP: services-mt, alg-list
2.- AP ← MT: services-ap, alg-sel

The argument *services-mt* contains information (one octet) about the desired security services, and must be interpreted as follows (b_0 is the less significant bit):

b_0 value 1 ⇒ MT requests the authentication and integrity services
b_1 value 1 ⇒ MT requests the confidentiality service
b_2 value 1 ⇒ MT has a public key certificate
b_3 value 1 ⇒ MT wants the public key certificate of the AP
$b_4 - b_7$ future use

If the MT demands the authentication service, automatically it demands the integrity service. This way we are not exposed to impersonation attacks during data transfer. On the other hand, if the MT and/or the AP want confidentiality, previously they have to be authenticated. By definition confidentiality means that information only is made available to true (authenticated) users.

The argument *alg-list* is an ordered list of algorithms for authentication/key exchange (RSA or pre-shared key), confidentiality (DES, 3DES, IDEA, AES, RC2 or RC4) and integrity (MD5 or SHA). In the future the number of algorithms for each service can be enlarged, without redefining the protocol messages. This feature provides the scalability property to our proposal. With RSA, parties may have to send a public key certificate. In some cases the encryption will be carried out in stream, while in other cases it will be carried out in chained blocks.

Regarding the response message sent by the AP, the byte *services-ap* contains information about the agreed security services. It must be interpreted as follows:

b_0 value 1 ⇒ the authentication and integrity services are activated
b_1 value 1 ⇒ the confidentiality service is activated
b_2 value 1 ⇒ the MT has to send a public key certificate
b_3 value 1 ⇒ the AP will send its public key certificate
$b_4 - b_7$ future use

The argument *alg-sel* contains the algorithms that have been selected by the AP. If the AP cannot accept any option of *alg-list*, the association should be rejected.

4 Authentication and Secret Exchange

Besides the option of not using authentication, two possible authentication methods can be used in DARWIN: pre-shared key or RSA. The exchange is as follows:

1.- MT $\Rightarrow$ AP: id_type, id, [certificate-mt]
2.- AP $\Rightarrow$ MT: chall$_1$, rand-ap, [certificate-ap]
3.- MT $\Rightarrow$ AP: chall$_2$, rand-mt, response$_1$
4.- AP $\Rightarrow$ MT: response$_2$

In the first message the MT indicates the type of authentication key identifier, and the value of that identifier. The AP can use this identifier to recover the necessary key for this access. Optionally, the MT and the AP have to send public key certificates. The MT should obtain the authentication key of the AP, from the public key certificate of the AP or using the AP identifier sent in the broadcast channels. The arguments *chall*$_1$ and *chall*$_2$ are two random values and they are used by the other part to formulate a response to that challenge. The arguments *rand-mt* and *rand-ap* are also random values, that will be used in the generation of keys and vectors. If the responses to the challenges are correct and, thus, the authentication process ends successfully (parties are authenticated), then the association process can continue. Otherwise, the DLC (Data Link Control) connection should be rejected.

If the pre-shared key mechanism has been agreed, the responses to the challenges are computed using a hashed message authentication code, that is, a hash function with a secret parameter. In DARWIN we use the same function as in HIPERLAN/2:

$$HMAC - MD5_k(m) = H_{MD5}((k \oplus \text{opad}), H_{MD5}((k \oplus \text{ipad}), m))$$

where the input message is m, k is the secret parameter, *opad* is the character 0x5c repeated 64 times and *ipad* is the character 0x36 repeated 64 times. The values of m are as follows:

$$\text{response}_1 = \text{HMAC-MD5}_K(\text{chall}_1, \text{rand-ap}, [\text{PU}_{MT}, \text{PU}_{AP}], \text{alg\_list}, \text{alg\_sel})$$
$$\text{response}_2 = \text{HMAC-MD5}_K(\text{chall}_2, \text{rand-ap}, [\text{PU}_{MT}, \text{PU}_{AP}], \text{alg\_list}, \text{alg\_sel})$$

The optional parameters PU_{MT} and PU_{AP} are the public keys of the MT and the AP. The parameters *alg_list* and *alg_sel* are obtained in the handshake phase. K is the pre-shared secret key between the MT and the AP, with 128 bits at least. The secret exchange based on a pre-shared key, K, is as follows:

$$\text{rand-ap} = E_K(\text{MT}, \text{random})$$
$$\text{rand-mt} = E_K(\text{AP}, \text{random})$$

The AP generates a random value of 48 bytes, *random*, and concatenates it with a MT identifier. The result is encrypted using the key shared with the MT. The MT sends the same value *random* linked with an AP identifier, encrypted with the shared key in order that the AP can verify that it has been received correctly and in a secure way.

With RSA, the responses will be calculated through the computation of a digital signature. DARWIN allows an arbitrary key size (nevertheless, it is recommended that it be between 512 and 2048 bits). The operations are as follows:

$$\text{response}_1 = \text{PR}_{MT}(H_{MD5}(\text{chall}_1, \text{rand-ap}, [\text{PU}_{MT}, \text{PU}_{AP}], \text{alg\_list}, \text{alg\_sel}))$$
$$\text{response}_2 = \text{PR}_{AP}(H_{MD5}(\text{chall}_2, \text{rand-mt}, [\text{PU}_{MT}, \text{PU}_{AP}], \text{alg\_list}, \text{alg\_sel}))$$

The secret exchange with RSA is as follows:

$$\text{rand-ap} = \text{PU}_{MT}(\text{random})$$
$$\text{rand-mt} = \text{PU}_{AP}(\text{random})$$

The AP generates a random value, *random*, and encrypts it with the public key of the MT. Then, the MT sends the same value *random* encrypted with the public key of the AP. In both cases, once the exchange has finished, each user has the necessary material to generate the session keys. The *pre-master secret* is the value *random* (PMS = *random*).

5 Key Generation

Once the MT and the AP have exchanged the *pre-master secret*, each one should generate the session keys for encryption effects (confidentiality service) and/or the keys for the integrity service. DARWIN uses different keys in the AP to MT and the MT to AP directions. So it is necessary to generate two keys and, according to the chosen encryption algorithm, two initialization vectors (IV).

First of all the *master secret*, MS, should be generated using the *pre-master secret*, and the random values, *rand-mt* and *rand-ap*:

$$\begin{aligned}\text{MS} = {} & H_f(\text{PMS}, H_f(\text{'A'}, \text{PMS}, \text{rand-mt}, \text{rand-ap})),\\ & H_f(\text{PMS}, H_f(\text{'BB'}, \text{PMS}, \text{rand-mt}, \text{rand-ap})),\\ & H_f(\text{PMS}, H_f(\text{'CCC'}, \text{PMS}, \text{rand-mt}, \text{rand-ap}))\end{aligned}$$

In the previous (and in the following) expression, f can be MD5 or SHA. Next, the key block, KB, should be computed to obtain the session keys and IVs:

$$\begin{aligned}\text{KB} = {} & H_f(\text{MS}, H_f(\text{'A'}, \text{MS}, \text{rand-ap}, \text{rand-mt})),\\ & H_f(\text{MS}, H_f(\text{'BB'}, \text{MS}, \text{rand-ap}, \text{rand-mt})),\\ & H_f(\text{MS}, H_f(\text{'CCC'}, \text{MS}, \text{rand-ap}, \text{rand-mt})), \ldots\end{aligned}$$

This process has to be repeated until enough output has been generated. Then, this key material, KB, has to be partitioned, as necessary, in the following order: *key-MT*, *key-AP*, *IV-MT*, *IV-AP*, *IC-MT* and *IC-AP*. The extra key material will be discarded. The values *IC-MT* and *IC-AP* will be used to calculate the integrity code. As in HIPERLAN/2, it is possible that some generated key to be a weak key or semi-weak key. If it is the case, it must be discarded and the following block of KB must be used.

6 Integrity and Confidentiality

The encryption allows providing the confidentiality service with respect to the transmitted data, while the keyed-hash functions allow obtaining the integrity service. If one or both services are negotiated during the association or handover phase, this encryption and/or integrity code will be used immediately after the key exchange has been carried out. Messages are encrypted and with integrity protection completely (from the most significant byte, MSB, to the least significant byte, LSB), and individually. The integrity code is generated as:

$$\text{IC} = H_f(\text{IC-sec}, \text{opad}, H_f(\text{IC-sec}, \text{ipad}, \text{seq-num}, \text{info}))$$

In the previous expression, f can be MD5 or SHA (the one that has been agreed in the handshake phase). *IC-sec* was generated from the secret information, and the MT and the AP have their corresponding value (*IC-MT* and *IC-AP*, respectively). The field *seq-num* is the sequence number for this message. The

argument *info* is the information to be protected. Due to the characteristics of the integrity function, it can also be obtained indirectly a second service: the authenticity of the parties involved in the exchange. The encryption is carried out on the whole message, including (if agreed) the calculated integrity code.

7 Some Concluding Remarks

HIPERLAN/2 security aspects can be improved, and here we present some enhancements. We would like to achieve compatibility with HIPERLAN/2, but we think that to carry out key exchange before authentication is a mistake. So, it's very difficult (if not impossible) to achieve compatibility with HIPERLAN/2. In this sense, we see our proposal as a future evolution of HIPERLAN/2. DARWIN incorporates all the basic security services, with a high degree of flexibility, allowing to negotiate services and algorithms to be used. The model that has been adopted in DARWIN allows the scalability of security services. DARWIN can incorporate new algorithms and different key sizes, without having to redefine the proposal of standard.

As a clearly differential element regarding HIPERLAN/2, DARWIN allows the use of public key infrastructure for authentication service. MT and AP can use authentication based on certificates, but sending these certificates is not compulsory (if parties have that information previously). In relation to key exchange, besides pre-shared key, DARWIN establishes an scheme based on RSA, a very used scheme in cryptographic protocols. For confidentiality service we have chosen strong algorithms and secure key generation processes. DARWIN provides stream ciphers and block ciphers, and establishes separated keys for the two directions of the communications (MT to AP, and AP to MT). In fact, we have adopted as a model the established one in SSL, because it is a broadly analyzed protocol and it is well known that it is a good security protocol. Finally, the integrity service was not established in HIPERLAN/2. In DARWIN approach, integrity and confidentiality are independent services. It is very useful in order to detect malicious users once authentication phase has finished (specially if parties do not use the confidentiality service).

References

1. A. Frier, P. Karlton and P. Kocher. The SSL Protocol Version 3.0, http://home.netscape.com/eng/ssl3
2. D. Wagner and B. Schneier. Analysis of the SSL 3.0 Protocol, 2nd USENIX Workshop on Electronic Commerce, 1996.
3. IEEE Std 802.11b-1999. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, IEEE Comp. Soc., 2001.
4. ETSI TS 101 761-1 V1.3.1. Broadband Radio Access Networks; HIPERLAN/2; Data Link Control (DLC) Layer; Part 1: Basic Data Transport Functions, 2001.
5. ETSI TS 101 761-2 V1.3.1. Broadband Radio Access Networks; HIPERLAN/2; Data Link Control (DLC) Layer; Part 2: Radio Link Control (RLC) sublayer, 2002.
6. Kent and Atkinson. Security Architecture for the IP, RFC-2401, 1998.