Cryptanalysis of anonymous channel protocol for large-scale area in wireless communications

A.M. Barbancho, A. Peinado *

Dept. Ingeniería de Comunicaciones, E.T.S. Ingeniería de Telecomunicación, Universidad de Málaga, Campus de Teatinos, 29071 Málaga, Spain

Received 19 December 2002; received in revised form 1 May 2003; accepted 2 June 2003

Abstract

The authentication and anonymous channel protocol for large-scale area in wireless communications proposed in [Proc. Sixth IEEE Symposium on Computers and Communications (ISCC’01), 3–5 (2001) 36] by Lin–Jan is analyzed, proving that it is not secure. More precisely, fake anonymous channel tickets can be easily generated allowing non-authorized users to be validated by the Visiting Network. Unlike it was claimed in [Proc. Sixth IEEE Symposium on Computers and Communications (ISCC’01), 3–5 (2001) 36], the security of this protocol does not rely on the difficulty of computing discrete logarithms over the finite field GF($p$), $p$ being a prime.

© 2003 Elsevier B.V. All rights reserved.

Keywords: Anonymous channels; Authentication; Cryptanalysis; Wireless Communications

1. Introduction

As it is well known, the security requirements in wireless networks, more extensive that in fixed networks, imply the design of specific security protocols based on strong authentication schemes. Every security service supported by a wireless network depends on this kind of protocols, providing not only the user-network and network-user authentication, but the agreement of the key to be used for encryption as the session key. Hence, these protocols are called authentication and key agreement (AKA) protocols [2]. Global authentication is one of the most difficult requirements to hold by the AKA protocol. More precisely, global authentication is necessary to support roaming of mobile stations with no security breaches in the system. That is, the users want to access and use the mobile system wherever they are, but with the same quality of service as in their own network. Note that the security services provided by the network to the users can be considered as an important differentiating factor in the quality of service. For example, the third generation mobile system UMTS [3–5] provides a new security service: security visibility and configurability, allowing the users to know the security level applied in their communications and to decide on the application of some of these services. In this sense,
global authentication and anonymous channels are growing in interest by the actual and potential mobile users. On one side, the geographical mobility of users is growing, thus requesting better and more efficient authentication methods supporting roaming services. On the other hand, anonymous channels can be considered as a tool to remove or decrease the effect of attacks based on traffic analysis. Furthermore, these channels allow the system to offer prepaid services, which are widely accepted by the users due to the anonymity among other features. For example, electronic voting schemes have to be supported by anonymous channels.

These objectives can be studied considering a model in which the users want to communicate from visiting networks, but they do not want that their location and identification parameters be accessible by the adversary. In the most general sense, the adversary can be considered as any entity different to the user who is communicating to another user. That is, the visiting network V, the home network H, and possible intruders to the system must have no access to the identity and location of the users who are communicating. In the same way, the end-users must have no access to the location parameters of the opposite end-users of the communication. However, practical implementations can reduce these constrains to allow H to trace the users.

Hence, new protocols are being designed to provide mutual (user-network and network-user) authentication from any visiting domain, but protecting all the sensitive information. In other words, the user will operate in the visiting network in an anonymous way, but authenticated remotely by his home network [6–8].

In [1], Lin and Jan propose an authentication and anonymous channel protocol for large-scale area in wireless communications, taking into account computational cost considerations. This protocol has been designed to provide anonymous channels by means of pre-paid tickets. The visiting domain V must verify the authenticity of anonymous tickets using only information on the expiration time $T_{\text{expire}}$. Furthermore, no information must exist allowing V and H to obtain the real identity of users from the messages in the second phase of the protocol. This fact implies that the tickets are distinguishable only on the validity period. Hence, different users will obtain the same ticket provided that $T_{\text{expire}}$ is the same.

This protocol assigns different tickets to different users, except for those that happen to have the same $T_{\text{expire}}$, but any user is able to share his/her ticket to another user, and all of them will gain access anonymously to the system. In any case, the communications established can be considered completely anonymous. The alternative to this situation consists of introducing some additional information relating the user’s real identity within the ticket, thus providing to the system the ability to trace the users.

The tickets issued following the protocol in [1] can be easily forged, as it is shown in Section 3. Section 2 describes the two phases of the original protocol. Sections 3 and 4 presents the security analysis, proving that the original protocol is insecure.

2. The Lin–Jan anonymous channel protocol

In [1], an authentication and anonymous channel protocol is presented to be “easily applied to GSM wireless system” [9], without changing the underlying structure. Actually, the protocol in [1] is designed to be applied over any wireless network providing that a public-key infrastructure exists. This particular scheme can be divided in two phases: the anonymous channel ticket issuing phase and the anonymous channel ticket authentication phase. Next, we introduce the same notation as in [1].

Let us consider a mobile user M, a visiting network V, and a home network H. Let $X \rightarrow Y : Z$ denote the event that a sender X sends a message Z to a receiver Y.

The protocol in [1] is defined considering the existence of secure communications in the system. Usually, a symmetric cryptosystem will be used by H to send messages to mobile users, using a shared $K_{h,i}$. Hence, it is assumed that H uses a distinct key $K_{h,i}$ for each mobile user with identity ID_i. On the other hand, mobile users will send messages to the home network H by means of an asymmetric cryptosystem. Thus, it is necessary to consider that
every user knows H’s public key $e_h$, but only H knows its own private key. It is important to note that no particular cryptosystems are considered. In this way, the protocol in [1] can be applied to any system independently to the specific algorithms employed.

Let \( \{m\}_e \) denote the ciphertext of the message \( m \) encrypted by some public key cryptosystem using the public key \( e_h \). Let \( \{m\}_K \) denote the ciphertext of the message \( m \) encrypted by some symmetric cryptosystem using the shared key \( K \). Let \( K_{h,v} \) be the secret key shared by H and V. Let \( K_{h,i} \) be the secret key shared by H and M. Let \( HD_i \) be the identity of H, and ID, the identity of M.

Besides the previous assumptions, the protocol in [1] defines the following new parameters: a large prime \( P \), with \( Q \) a prime factor of \( P - 1 \), and an element \( g \) of order \( Q \) in \( Z_p^* \). The parameters \( P \) and \( g \) are known by the whole system (H and mobile users). Moreover, a new pair of keys \( (x_h, y_h) \) is defined as \( y_h = g^{x_h} \mod P \), where \( x_h \) is the private key and \( y_h \) the public key of H. Note that this pair of keys and the way in which it is generated are completely independent to the undefined asymmetric cryptosystem existing previously in the system. Hence, H makes use of two different public keys, \( e_h \) to receive messages from mobile users, and \( y_h \) to implement the anonymous channel protocol, and two private keys, \( d_h \) to decipher messages encrypted with \( e_h \), and \( x_h \) to decipher messages encrypted with \( y_h \).

In this way, every mobile user ID\(_i\) has to maintain the following information: his own identification ID\(_i\), the secret key \( K_{h,i} \), shares with the home domain, the public key \( e_h \) of the home domain (corresponding to the previously existing asymmetric cryptosystem), and the parameters of the anonymous protocol, i.e., the integers \( P \) and \( Q \), the public key \( y_h \) and the integer \( g \in Z_p^* \) of order \( Q \).

The anonymous channel protocol can be described as follows. The mobile user M has to obtain a prepaid ticket from his home domain H. Hence, it is necessary for M to communicate with H, in order to authenticate M as a legal and authorized user of the home network. The only entity with the ability to do so is H. This operation is performed across V, in such a way that V may not know the identity of M. Once M is authenticated by H, a ticket is generated to be valid for a period of time \( T_{\text{expire}} \) specified by M. The period length determines the amount of money to be charged immediately to M.

Since no information is provided in [1] about the types of services the mobile users can access to, we consider only one type of service. Otherwise, additional parameters and techniques have to be applied to perform billing tasks and avoid misuses. Note that each service is usually provided with different prices.

H encrypts the ticket and sends it to M across V. Thus, if M wants to use the resources of V, then M has to send the prepaid ticket to V, using a new (anonymous) identity. In this way, V only verifies the validity of the prepaid ticket, i.e., V checks that the expiration time is not exceeded and that the ticket has been issued by H, by means of the relationship between \( x_h \) and \( y_h \).

Next, the details of the protocol are presented.

### 2.1. The anonymous channel ticket issuing phase

When a mobile user M wants to send an anonymous message in the wireless network, M must purchase an anonymous channel ticket from H to be used in the second phase of the protocol. The ticket issued in this first phase is a prepaid ticket. The ticket generation depends on the successful authentication of M by H. The protocol is as follows (see Fig. 1):

**Step 1.** \( M \rightarrow V : HD, N_1, \{ID_i, T, T_{\text{expire}}, \text{Cert}_i\}_{e_h} \), where \( N_1 \) is a random word, \( T \) and \( T_{\text{expire}} \) are timestamps, and \( \text{Cert}_i \) is the authentication information

\[
\text{Cert}_i = (ID_i, T, T_{\text{expire}})_{K_{h,i}}.
\]

In this step, M sends to V the information to be passed to H, in such a way that V cannot access it. That is, M encrypts the information using H’s public key \( e_h \). The only thing V has to do is to re-send this information to H with identity HD.

**Step 2.** \( V \rightarrow H : N_1, \{ID_i, T, T_{\text{expire}}, \text{Cert}_i\}_{e_h} \),

**Step 3.** \( H \rightarrow V : N_1, (C, D, T_{\text{expire}})_{K_{h,i}} \) with

\[
C = g^r \mod P
\]
for a random number \( c \), and
\[
D = x_h + c T_{\text{expire}} \mod (P - 1)
\] (3)

\( x_h \) being the private key of \( H \). The ticket generated \((C, D, T_{\text{expire}})\) is encrypted and sent to \( V \).

**Step 4.** \( V \to M : N_1, (C, D, T_{\text{expire}})_{K_{x_h}} \)
In this case, \( V \) broadcasts this message to every user. \( N_1 \) is used by the legal destination user to identify the correct message.

**Step 5.** \( M \) checks the ticket validity by means of the following equation:
\[
g^D = y_h C^{T_{\text{expire}}} \mod P
\] (4)

since the parameters of any valid ticket satisfy the following relationship:
\[
g^D \mod P = g^{x_h + c T_{\text{expire}}} \mod P
= (g^{y_h})(g^c)^{T_{\text{expire}}} \mod P
= y_h C^{T_{\text{expire}}} \mod P.
\] (5)

If this verification succeeds, the mobile user considers the ticket \((C, D, T_{\text{expire}})\) as a valid one. Note that the term “valid ticket” has to be understood as “ticket generated by \( H \) using its private key \( x_h \) and the parameter \( T_{\text{expire}} \)”. This verification is based on the fact that \( x_h \) and \( c \) are only known by \( H \). To obtain \( x_h \) (resp. \( c \)) from \( y_h \) (resp. \( C \)), discrete logarithms have to be computed turning out the problem computationally infeasible. Hence, the valid ticket can be used in the second phase of this protocol to access to the system.

As one can observe, this phase of the protocol implements a mutual authentication between \( M \) and \( H \). First, \( H \) authenticates \( M \) by means of the identity \( ID_i \), and the shared key \( K_{x_h} \). Next, \( M \) authenticates the originator of the ticket. Moreover, \( M \) verifies that the ticket has been issued to be valid for a period of time bounded by \( T_{\text{expire}} \).

### 2.2. The anonymous channel ticket authentication phase

When a mobile user wants to use the previous ticket \((C, D, T_{\text{expire}})\), then he requests an anonymous channel service call and generates a new ticket containing a new identification \( \text{NewID} \), in order to hide his identity to the visiting network. The protocol is as follows (see Fig. 2):

**Step 1.** \( M \to V : \text{NewID}, T, T_{\text{expire}} \), where \( \text{NewID} = y_h || B || E \), that is, the concatenation of \( y_h \), \( B \) and \( E \), with
\[
B = g^{b} \mod P,
A = g^{a} \mod P,
E = A C \mod P
\] (6)

for random values of \( b \) and \( a \). \( T \) is the current time.

**Step 2.** \( V \to M : r \) where \( r \) is a random challenge.

**Step 3.** \( M \to V : K, L \) with
\[
K = B^k \mod P
\] (7)
for a random value of \( k \), and

\[
L = D + aT_{\text{expire}} + bK + bkrT \mod (P - 1).
\]

(8)

**Step 4.** V checks the ticket validity by means of the following equation:

\[
g^L \equiv y_h E^T_{\text{expire}} B^K K^r T \mod (P)
\]

since the valid parameters satisfy the following relationship:

\[
g^L \equiv g^{D + aT_{\text{expire}} + bK + bkrT} \mod P
\]

\[
= (g^x)^{T_{\text{expire}}} (g^{aT_{\text{expire}}} (g^b)^K (g^{bK})^r T) \mod P
\]

\[
= y_h (AC)^{T_{\text{expire}}} B^K K^r T \mod P
\]

\[
= y_h E^{T_{\text{expire}}} B^K K^r T \mod P.
\]

(10)

If this equation holds, then V authenticates M, that is, V considers M an authorized user of the system. Since V does not know the real identity of M, M can use the resources of V anonymously. Next, M has to agree on a session key with V to communicate securely with each other. However, no indication is presented in [1] about the session key to be used.

3. The Cryptanalysis

We consider two major attacks, consisting on the generation of a fake anonymous ticket, and another two secondary attacks based on minor weaknesses and a simplification of the previous ones. In any case, the attacks succeed in the objective, and the users (or forgers) gain access to the network by means of the fake anonymous tickets. That is, all the attacks concentrate the efforts on the second authentication phase of the Lin–Jan protocol.

3.1. First Attack

We consider the case in which a legal mobile user M (a user with a valid ticket issued by H in the first phase) wants to use his/her ticket far from the validity period bounded by \( T_{\text{expire}} \). Hence, this attack is based on the fact that a valid ticket \((C, D, T_{\text{expire}})\) allows the user to use the anonymous channel up to \( T_{\text{expire}} \), in the way originally determined by the protocol. However, as we prove below, the user M can easily generate a fake ticket \((C', D', T'_{\text{expire}})\) from the knowledge of the valid ticket, allowing him to use the channel in any period of time. The successful attack is as follows:

(a) Fake ticket generation.

(a.1) M generates a new expiration time \( T'_{\text{expire}} > T_{\text{expire}} \) in the following way:

\[
T'_{\text{expire}} = T_{\text{expire}} \cdot \gamma \mod (P - 1)
\]

with \( \gamma \in Z_{p^\prime - 1}, \gamma > 1 \). Note that no explicit indication is stated in [1] about \( T_{\text{expire}} \) format or
data type. However, \( T_{\text{expire}} \) is used directly in modular computations (see Eqs. (3)–(5), (8)–(10)) where the modulus is always \((P - 1)\). Since \( P \) is a big prime with a typical size of 1024 bits, the expiration times \( T_{\text{expire}} \) and \( T'_{\text{expire}} \) will be much less than \((P - 1)\), even if time is expressed in milliseconds from 1/1/1970 as in Unix systems. Hence, the modular computation is not necessary. Anyway, Eq. (11) is defined as modular computation for consistency. On the other hand, it is not recommended to generate \( T'_{\text{expire}} \) much greater than \( T_{\text{expire}} \), in order to make this attack undetectable by \( V \).

Hence, we can define \( T'_{\text{expire}} \) as

\[
T'_{\text{expire}} = T_{\text{expire}} + \Delta \mod (P - 1),
\]

where \( \Delta \in Z_{P-1} \), represents a little increment in expiration time. In this way, we can write

\[
T'_{\text{expire}} = T_{\text{expire}} \cdot \gamma \mod (P - 1),
\]

with

\[
\gamma = (T_{\text{expire}} + \Delta)(T_{\text{expire}})^{-1} \mod (P - 1).
\]

(a.2) \( M \) generates a new value \( C' \), instead of using the ticket component \( C \) issued by \( H \), in the following way:

\[
C' = C'^{-1} \mod P = (g^\gamma)^{-1} \mod P,
\]

where \( \gamma \) is the integer computed from Eq. (13). The computation in Eq. (14) can be easily performed calculating the inverse of the integer \( \gamma \mod (P - 1) \), i.e., \( \beta = \gamma^{-1} \mod (P - 1) \), by means of the extended Euclidean algorithm and then computing \( C' = C^\beta \mod P \).

(a.3) \( M \) generates the fake ticket \((C', D, T'_{\text{expire}})\). Note that the original value of \( D \) is used.

(b) Anonymous channel ticket authentication phase. \( M \) initiates the second phase of the protocol in the usual way. That is,

(b.1) \( M \) sends to \( V \) the message NewID', \( T' \), \( T'_{\text{expire}} \), where NewID' = \( y_h [B'] [E'] \), with

\[
A' = g^{a'} \mod P,
B' = g^{b'} \mod P,
E' = (A' C') \mod P = g^{d' + c' \gamma^{-1}} \mod P
\]

for random values of \( a' \) and \( b' \), as stated in step 1 of the protocol (second phase).

(b.2) \( V \) sends to \( M \) a challenge \( r \) (see step 2 in second phase)

(b.3) \( M \) sends to \( V \) the values \( K' \) and \( L' \),

\[
K' = B'^{k'} \mod P = g^{b'K'} \mod P,
L' = D + c T'_{\text{expire}} + b'K' + b'k'r T' \mod (P - 1),
\]

where \( k' \) is a random value and \( D \) the original ticket component issued by \( H \), i.e.,

\[
D = x_h + cT_{\text{expire}} \mod (P - 1).
\]

Note that the computations of \( K' \) and \( L' \) follow the equations stated in the original protocol.

(b.4) Finally, \( V \) checks Eq. (9) obtaining the following result:

\[
y_h E'_{\text{expire}}^{\gamma} B'^{K'} K'rT' \mod P
= g^{x_h (g^{d' + c' \gamma^{-1}})^{T_{\text{expire}}} g^{b'k'r}} \mod P
= g^{y_h + cT_{\text{expire}} + dT'_{\text{expire}} + b'K' + b'k'r T'} \mod P
= g^{T'} \mod P.
\]

Hence, the user \( M \) gains access illegally to the visiting network. As one can observe, no message modification has been applied to the protocol. The attack relies exclusively on the computation of a fake ticket; more precisely, on the computation of \( T'_{\text{expire}} \) and \( C' \). As a conclusion, the protocol in [I] is not able to control the validity period of the tickets issued by \( H \).

3.2. Second attack

We consider now a mobile user \( M \) with no valid ticket \((C, D, T_{\text{expire}})\), that is, a user not previously authenticated by the first phase of this protocol. The objective, in this case, is to generate a fake ticket allowing any user (previously authorized or not) to use the channel. The successful attack is as follows:

(a) Fake ticket generation.

(a.1) \( M \) generates a new expiration time \( T'_{\text{expire}} > T_{\text{expire}} \).

(a.2) \( M \) generates a new value \( C' \), instead of using the ticket component \( C \) issued by \( H \), in the following way:
\[ C' = g^{c'} (y_h^{-1}) (T_{\text{expire}}')^{-1} \mod P \]
\[ = g^{c' - x_h (T_{\text{expire}}')^{-1}} \mod P. \]  
\[ (18) \]

Unlike the previous attack, parameter \( C' \) does not depend on the valid parameter \( C \), issued by \( H \). This computation can be performed by first calculating the inverse of \( T_{\text{expire}}' \mod (P - 1) \), i.e., \( \beta = (T_{\text{expire}}')^{-1} \mod (P - 1) \), by means of the extended Euclidean algorithm, and then computing \( C' = g^{c'} (y_h^{-1})^\beta \mod P \), for a random value of \( c' \).

(a.3) No value of \( D \) is necessary.
(b) Anonymous channel ticket authentication phase. \( M \) initiates the second phase of the protocol in the usual way. That is, \( (b.1) \) \( M \) sends to \( V \) the message \( \text{NewID}', T', T_{\text{expire}}' \), where \( \text{NewID}' = y_h || B'||E', \) with
\[ A' = g^{d'} \mod P, \]
\[ B' = g^{y'} \mod P, \]
\[ E' = (A'C') \mod P = g^{d'+c'-x_h (T_{\text{expire}}')^{-1}} \mod P \]
\[ (19) \]

for random values of \( d' \) and \( b' \), as stated in the protocol (step 1 in second phase).
(b.2) \( V \) sends to \( M \) a challenge \( r \) (see step 2 in second phase).
(b.3) \( M \) sends to \( V \) the values \( K' \) and \( L' \) (see step 3 in second phase).
\[ K' = B'^{k'} \mod P = g^{b'k'} \mod P, \]
\[ L' = c'T_{\text{expire}}' + d'T_{\text{expire}}' + b'K' \]
\[ + b'k'rT' \mod (P - 1) \]
\[ (20) \]

for random value of \( k' \).
(b.4) Finally, \( V \) checks Eq. (9) obtaining the following result:
\[ y_h E'^{t}_{\text{expire}} B'^{k'} K'^{rT'} \mod P \]
\[ = g^{x_h} (g^{d'+c'-x_h (T_{\text{expire}}')^{-1}}) T_{\text{expire}}' g^{b'k'} g^{b'k'rT'} \mod P \]
\[ = g^{x_h + d'T_{\text{expire}}' + c'T_{\text{expire}}' - x_h + b'K' + b'k'rT'} \mod P \]
\[ = g^{L'} \mod P. \]
\[ (21) \]

Hence, the user \( M \) gains access illegally to the visiting network. Note that, as in the first attack, the user generates a new ticket \( (C', D', T_{\text{expire}}') \), but in this case, these new parameters are not related to a previous valid ticket \( (C, D, T_{\text{expire}}) \). Furthermore, it is not necessary to generate a fake value of \( D \).

Unlike the first attack, in this case the user \( M \) modifies the generation of the parameter \( L \). More precisely, the parameter \( D \) is not included in the computation of \( L \). This is an operation that any user (forger) can perform.

This attack shows that any intruder can be validated by the visiting network using a fake ticket generated easily. Therefore, the protocol is completely insecure.

3.3. Third attack

This attack is only a simplification of the previous one, simplifying conceptually the procedure, in the sense that no relationship exists to the ticket components \( C \) and \( D \). In other words, this is the case in which the forger only knows \( H \)'s public key \( y_h \). Hence, the algorithm is equivalent to the second attack.

(a) No ticket generation phase is necessary.
(b) Anonymous channel ticket authentication phase. \( M \) initiates the second phase of the protocol in the usual way. That is, \( (b.1) \) \( M \) sends to \( V \) the message \( \text{NewID}', T', T_{\text{expire}}' \), where \( \text{NewID}' = y_h || B'||E', \) with
\[ B' = g^{y'} \mod P, \]
\[ E' = g^{c'} (y_h^{-1}) (T_{\text{expire}}')^{-1} \mod P = g^{c'-x_h (T_{\text{expire}}')^{-1}} \mod P \]
\[ (22) \]

for random values of \( b' \) and \( e \). Note that \( B' \) is computed from a random value, as stated in the protocol, but \( A' \) is no longer needed. Furthermore, \( E' \) is computed from a random value \( e \) and a chosen value of \( T_{\text{expire}}' > T_{\text{expire}} \), but not from any value of \( C \).
(b.2) \( V \) sends to \( M \) a challenge \( r \) (see step 2 in second phase)
(b.3) \( M \) sends to \( V \) the values \( K' \) and \( L' \),
\[ K' = B'^{k'} \mod P = g^{b'k'} \mod P, \]
\[ L' = eT_{\text{expire}}' + b'K' + b'k'rT' \mod (P - 1) \]
\[ (23) \]

for random value of \( k' \).
Finally, V checks Eq. (9) obtaining the following result:

\[
y_h B^{rT_0} K_c^{rT_0} \mod P = g^{x_h (g^{e-\bar{x}_h T_{\text{expire}}})^{-1}} g^{b T_{\text{expire}} T_0^{\text{c}}} \mod P
\]

\[
y_h B^{rT_0} K_c^{rT_0} \mod P = g^{x_h + e T_{\text{expire}} - x_h + b K_c^{rT_0}} \mod P
\]

\[
y_h B^{rT_0} K_c^{rT_0} \mod P = g^{\bar{T}_0} \mod P.
\]

\[(24)\]

3.4. Fourth attack

This attack is based on a minor weakness of the system, derived from the fact that no public-key certificate is used to protect the system from public-key owner impersonation. Although it is considered in [1] that there exist secure symmetric and asymmetric (public-key) cryptographic algorithms to communicate the users in the visiting domain V to the home domain H, the utilization of user’s public-key certificates is not explicitly stated in the anonymous communication establishment. In other words, the user previously validated by H in the first phase of the protocol in [1] has to send H’s public-key to V as part of his/her new anonymous identity NewID. No public-key certificate is used in this case. This situation allows the forgers to used non-valid H’s public keys \( y_h \) in order to generate fake parameter \( D \) from the knowledge of \( x_h \).

Taking into account that the number of distinct home domains the users can access anonymously from a given visiting domain is not so large, a simple verification of the valid \( y_h \) values may solve the problem. In any case, a better solution corresponds to the use of public-key certificates.

Anyway, public-key certificates is not enough to make the protocol in [1] secure, as the forger can generate a fake ticket from H’s always-known public key. The forger only needs to know a home domain public key to illegally access the system.

4. Other security considerations

As it is stated in [1], the ticket issued by H is completely anonymous in the sense that V is not able to obtain the real identity of the users. Hence, V may only verify the validity of the ticket, which is the usual anonymous channel protocol objective. But, as can be deduced from the previous attacks, V is not able to distinguish two copies of the same valid ticket. In other words, a legal user may copy his valid ticket to his friends, and all of them may use it to access the system for the same valid period of time. As no consideration is made in [1] about the length of validity periods, this situation must be taken in mind.

Since all the attacks presented focus on the generation of fake tickets, a trivial solution may be adopted consisting on the aggregation of a digital signature to the ticket to provide integrity avoiding the falsification. More precisely, if H digitally signs \( T_{\text{expire}} \), then all the attacks based on the modification of this parameter do not succeed. However, a protocol based uniquely on the integrity protection of this parameter is not enough to avoid the ticket replication.

On the other hand, but related to digital signatures and public key certificates, it is important to note that the mobile user M cannot authenticate the visiting domain V during the second phase of the protocol.

5. Conclusions

Several successful attacks on the authentication and anonymous channel protocol in [1] have been presented, proving that it is completely insecure. Any user previously authenticated by his own home network (in the first phase of the protocol) can always generate a fake ticket from a valid one, allowing him to use the network indefinitely in time, exceeding any timestamp, with no charge in his account. In the second attack, any user, not necessarily authenticated in the first phase, can always generate another fake ticket allowing him to use the network as a legal and validated user with no time limit.

The main weakness of this protocol is the foreign authentication (second) phase, not the anonymity. That is, the visiting network cannot obtain information about the identity of the foreign users accessing the system, but it is possible that any unauthorized user gains access to the network. In
other words, the authentication data used to perform the user authentication reveals enough information to the attacker about the secret parameters but not on the user identity. On the other hand, the first phase of this protocol is secure, performing mutual authentication between M and H.

Acknowledgements

This work have been supported by MICYT-Spain under grant TIC2001-0586, “Gestión del Acceso Seguro a redes abiertas de recursos distribuidos”. The authors thank the anonymous referees for their valuable comments.

References

[9] GSM 02.09, Digital Cellular Telecommunication System (Phase 2+); Security Aspects.

Ana Maria Barbancho was born in Málaga (Spain). She received the Ingeniería de Telecomunicaciones degree from the University of Málaga in 2000. She is currently working on her Ph.D. Thesis. Since 2000, she has been with the Department of Ingeniería de Comunicaciones at the University of Málaga as an Assistant Professor. Her research interests include cryptography, multiset detection and transmission, and musical acoustics.

Alberto Peinado Díaz was born in Málaga (Spain). He received the degree in Telecommunications Engineering from the University of Málaga in 1993, and the Ph.D. degree in computer science from the Polytechnic University of Madrid, Spain, in 1997. From 1995 to 1998, he was with the National Spanish Council for Scientific Research (CSIC), Madrid, Spain, where his research interests were in cryptography and network security. Since 1998, he has been with the Department of Ingeniería de Comunicaciones at the University of Málaga as an Assistant Professor and then as an Associate Professor. His research interests include cryptography, mobile communications, CDMA codes, smart cards and watermarking.