A Note on an Authentication Technique Based on Distributed Security Management for the Global Mobility Network*

Levente Buttyán and Constant Gbaguidi
Swiss Federal Institute of Technology
Institute for computer Communications and Applications (ICA)
EPFL-DI-ICA, CH-1015 Lausanne, Switzerland
{Levente.Buttyan, Constant.Gbaguidi}@epfl.ch

Sebastian Staamann and Uwe Wilhelm
Swiss Federal Institute of Technology
Operating Systems Laboratory
EPFL-DI-LSE, CH-1015 Lausanne, Switzerland
{Sebastian.Staamann, Uwe.Wilhelm}@epfl.ch

7 April 1998

Abstract

In this paper, we analyse the authentication protocol that has been proposed for the so called global mobility network in the October issue of the IEEE Journal on Selected Areas in Communications. Using a simple logic of authentication, we show that the protocol has flaws, and we present three different attacks that exploit these. We correct the protocol using a simple design tool that we have developed.

1 Introduction

In a recent issue of the IEEE Journal on Selected Areas of Communications, an authentication technique has been proposed for use in the so called global mobility network (GLOMONET), which provides a personal communication user with global roaming service [SN97]. The proposed authentication technique consists of two phases:

- *the roaming-service-setup phase*, in which authentication to set up the roaming-service environment is performed by the visited (roamed) network, the home network, and the roamer, and
- *the roaming-service-provision phase*, in which authentication to provide the roaming service within the visited network is performed only by the visited network and the roamer.

The latter is based on a secret key, which is shared by the temporal security manager in the visited network and the roamer. This key is generated and distributed in the roaming-service-setup phase using the following authentication protocol[1]:

1. $U \to V : Request$
2. $V \to H : rnd_1$
3. $H \to V : K_n F(rnd_1),\ rnd_2$
4. $V \to H : K_n F(rnd_2),\ K_n F(K_t F(K_v))$
5. $H \to V : K_{uh} F(K_t F(K_v))$
6. $V \to U : rnd_3,\ K_t,\ K_{uh} F(K_t F(K_v))$
7. $U \to V : K_v F(rnd_3)$
8. $V \to U : K_v F(K_v F(rnd_3))$

where U, V, and H denote the user, the visited network, and the home network, respectively; rnd_1, rnd_2, and rnd_3 are random numbers; K_n is a secret key shared between V and H; K_{uh} is a secret key shared between U and H; K_t and K_v are keys generated by V; $KF(x)$ denotes x encrypted with the key K; and $A \to B : M$ means that A sends the message M to B.

The protocol works in the following way:

1. The roaming user U sends a *Request* to the visited network V.
2. V sends the random number rnd_1 to authenticate the home network of the user H.
3. H responds V's random challenge with the calculated value $K_n F(rnd_1)$, and sends the random number rnd_2 to authenticate V.
4. V verifies if it received back its random number rnd_1 encrypted with the key K_n. If so, then V believes that H has been authenticated, since the key K_n is known only by H and V, and so V believes that H sent the message. V generates the user authentication key K_v and the temporary cipher key K_t to encrypt K_v. Then, V responds H's random challenge with $K_n F(rnd_2)$, and sends $K_n F(K_t F(K_v))$.
5. H verifies if it received back its random number rnd_2. If so, then H believes that V has been authenticated. H decrypts $K_n F(K_t F(K_v))$ and re-encrypts the result $K_t F(K_v)$ with the key K_{uh}. H sends $K_{uh} F(K_t F(K_v))$ to V.
6. V forwards $K_{uh} F(K_t F(K_v))$ to U along with the key K_t and the random number rnd_3 to authenticate U.
7. U uses the key K_{uh} that it shares with H, and the key K_t that it has just received to obtain the authentication key K_v. Then, U responds V's random challenge with $K_v F(rnd_3)$.

[1] We denote the key that is shared between the user and the home network by K_{uh}, instead of the original K_h notation in [SN97].

8. V verifies if it received back its random number rnd_3. If so, then V believes that U has been authenticated. V sends the calculated value $K_vF(K_vF(rnd_3))$ to U. U verifies if it received back $K_vF(rnd_3)$ encrypted with K_v. If so, then U believes that V has been authenticated.

The authors in [SN97] claim that after the successful execution of the protocol the key K_v is a shared secret between the roaming user U and the visited network V, and thus, it can be used later in the roaming-service-provision phase to authenticate U and V. However, the protocol has serious flaws. These flaws can be exploited by various attacks. In this note, we present three of them. The first two attacks enable an intruder (who can be an outsider or a legitimate, but malicious user) to obtain the authentication key K_v. In this way, it can impersonate an unsuspicious roaming user or the visited network to this user. The third attack allows the intruder to feed the roaming user with a compromised old authentication key, and thus, to masquerade as the visited network to the roaming user.

The rest of the paper is organised as follows. In Section 2, we analyse the protocol with a simple logic of authentication. Our analysis points out the weaknesses in the protocol. In Section 3, we present three different attacks that exploit the revealed weaknesses. In Section 4, we redesign the protocol with a design tool that has been developed from the logic mentioned.

2 Analysis

In this section, we analyse the protocol that was described in the previous section. As a tool for this analysis, we use a simple logic for authentication [BSW98]. We do not describe the logic in detail here (a brief description of it can be found in the Appendix), we rather concentrate on the analysis itself.

The first step of the analysis is to identify the initial assumptions and the goals of the protocol. Then, we translate the protocol description given in the previous section into the language of our logic. Finally, we try to generate a witnessing deduction, which is a derivation of the goals from the assumptions and the protocol itself, using the inference rules of the logic. The lack of such a deduction indicates that the protocol may not be correct. The analysis process often reveals the weaknesses, and helps us to construct attack scenarios more easily. This is the program that we follow in the sequel.

We have identified the following assumptions about channels (keys), random numbers, and trust between parties in the analysed protocol:

(A1) $V \in r(C_n)$, $V \in w(C_n)$, $H \in r(C_n)$, $H \in w(C_n)$
V and H can read and write from/to the channel C_n, which is provided by the encryption with the key K_n. This is based on the assumption that V and H know the key K_n.

(A2) $V \models (w(C_n) = r(C_n) = \{V, H\})$
V believes that the channel C_n can be used only by V and H (i.e., it is a conventional secret channel between V and H). This is based on the assumption that K_n is a shared secret between V and H, thus, it is not known to other parties. For similar reasons:

(A3) $H \models (w(C_n) = r(C_n) = \{V, H\})$
H believes that the channel C_n is a conventional secret channel between V and H.

(A4) $U \in r(C_{uh})$, $U \in w(C_{uh})$, $H \in r(C_{uh})$, $H \in w(C_{uh})$
U and H can read and write from/to the channel C_{uh}, which is provided by the encryption with the key K_{uh}. This is based on the assumption that U and H know the key K_{uh}.

(A5) $U \models (w(C_{uh}) = r(C_{uh}) = \{U, H\})$
U believes that the channel C_{uh} is a conventional secret channel between U and H. This is based on the assumption that K_{uh} is a shared secret between U and H, thus, it is not known to other parties. For similar reasons:

(A6) $H \models (w(C_{uh}) = r(C_{uh}) = \{U, H\})$
H believes that the channel C_{uh} is a conventional secret channel between U and H.

(A7) $V \in r(C_v)$, $V \in w(C_v)$
V can read and write from/to the channel C_v, which is provided by the encryption with the key K_v. This is based on the assumption that V generates the key K_v, so it possesses it.

(A8) $V \models \sharp(K_v)$
V believes that the key K_v is fresh. This is based on the assumption that V generates this key and it believes that it generates fresh keys.

(A9) $V \models (w(C_v) = \{U, V\})$
V believes that the writer set of the freshly established channel C_v is $\{U, V\}$, therefore, it can be used to authenticate U. This is a dangerous assumption, because it is based on V's belief that the protocol does not reveal the key K_v to untrusted parties.

(A10) $U \models ((V \mid\!\sim \sharp(K_v)) \rightarrow \sharp(K_v))$
U does not directly believe that the key K_v is fresh. However, if V says that K_v is fresh in a recent message, then U believes this. This is based on the assumption that U believes that V is honest and competent in generating and distributing fresh keys.

(A11) $U \models ((V \mid\!\sim (w(C_v) = \{U, V\})) \rightarrow (w(C_v) = \{U, V\}))$
If V says (in a recent message) that the channel C_v can be used for authentication purposes, then U believes this. This is based on the assumption that U believes that V is honest and competent in generating and distributing good authentication keys, and the protocol does not reveal the key K_v.

(A12) $U \models ((H \mid\!\sim (V \mid\sim X)) \rightarrow (V \mid\sim X))$
U believes that H is honest and competent in deciding if V said something. This is based on the assumption that U knows that V and H have a conventional secret channel between them, and U considers its own home network H to be honest.

(A13) $V \models \sharp(rnd_1)$
V believes that the random number rnd_1 is fresh (i.e., it has not been used before the current run of the protocol). This is based on the assumption that rnd_1 is generated by V and it is random, so it has a very low probability that rnd_1 is equal to a previously

generated random number (assuming that the size of rnd_1 is sufficiently big). For similar reasons:

(A14) $H \models \sharp(rnd_2)$

(A15) $V \models \sharp(rnd_3)$

It is not always clear what the goals of an authentication protocol should be [Syv91]. Some authentication protocols convince the parties that they are talking to each other, while others also establish session keys between the parties that they can use for authentication or secret communication later on. Although, the authors in [SN97] do not explicitly state the goals of their protocol, they give some requirements (r1)-(r8) that they want it to satisfy. Based on these requirements and the protocol itself, we have identified the following goals:

(G1) $V \models (H \mid\!\sim rnd_1)$
V believes that H has recently said the random number rnd_1 (i.e., V believes that H answered V's random challenge). Similarly:

(G2) $H \models (V \mid\!\sim rnd_2)$
H believes that V has recently said the random number rnd_2 (i.e., H believes that V answered H's random challenge).

(G3) $U \models (w(C_v) = \{U, V\})$
U believes that the writer set of the channel C_v, which is provided by the encryption with the key K_v, is the set $\{U, V\}$. This means that if U receives a message via this channel, then it believes that the message was sent by V. Thus, the channel C_v can be used to authenticate V.

(G4) $U \triangleleft K_v$
To use the channel C_v, U must possess the key K_v. Therefore, U must receive a message that contains K_v.

(G5) $V \models (U \mid\!\sim rnd_3)$
V believes that U has recently said the random number rnd_3 (i.e., V believes that U answered V's random challenge). Similarly:

(G6) $U \models (V \mid\!\sim K_v F(rnd_3))$
U believes that V answered U's challenge.

The last two steps (step 7 and 8) of the protocol are similar to the last two steps of some well-known authentication protocols (e.g., the Needham-Schroeder symmetric key authentication protocol [NS78]). In these protocols, the goal of the last two steps is to obtain the second order beliefs [BAN90]:

$$V \models (U \models (w(C_v) = \{U, V\}))$$
$$U \models (V \models (w(C_v) = \{U, V\}))$$

It is not clear whether the authors wanted their protocol to reach these goals or not, so we do not consider these to be goals.

The next step is to translate the original protocol description into the language of our logic. This is almost straightforward:

1. $V \triangleleft Request$
2. $H \triangleleft rnd_1$
3. $V \triangleleft (C_n(rnd_1),\ rnd_2)$
4. $H \triangleleft (C_n(rnd_2),\ C_n(C_t(K_v,\ \sharp(K_v),\ w(C_v) = \{U, V\})))$
5. $V \triangleleft C_{uh}(C_t(K_v,\ \sharp(K_v),\ w(C_v) = \{U, V\}))$
6. $U \triangleleft (rnd_3,\ K_t,\ C_{uh}(C_t(K_v,\ \sharp(K_v),\ w(C_v) = \{U, V\})))$
7. $V \triangleleft C_v(rnd_3)$
8. $U \triangleleft C_v(C_v(rnd_3))$

In step 4, 5 and 6, we inserted two additional elements ($\sharp(K_v)$ and $w(C_v) = \{U, V\}$) in the messages that are not present in the original protocol description. These additional elements capture V's implicit intention, namely, that V not only wants to send the key K_v to U (via H), but V also wants to convey the fact that K_v is fresh and good for authentication for U and V. This is the only way to convince U of the key K_v.

To derive the goal (G1), we start the analysis with step 3. First using inference rule (S2) of our logic, then applying rule (S1) and assumption (A1), we get:

$$V \models (V \triangleleft rnd_1 \mid C_n)$$

Using rule (I1) and assumption (A2), we obtain:

$$V \models ((V \triangleleft X \mid C_n) \to (H \mid\sim X))$$

From these results, using rule (R1), we get:

$$V \models (H \mid\sim rnd_1)$$

From this, using rule (F1) and assumption (A13), we can derive the goal (G1). In a similar way, we can derive the goals (G2) and (G5). To derive the goal (G4), we start the analysis with step 6. First using rule (S2), then applying rule (S1) and assumption (A4), we obtain

$$U \triangleleft C_t(K_v,\ \sharp(K_v),\ w(c_v) = \{U, V\})$$

Since U received K_t, $U \in r(C_t)$ holds, and we can use rule (S1) and (S2) again to reach the goal (G4). The remaining two goals (G3) and (G6) cannot be derived. In particular, we cannot derive (G3), which would be necessary to derive (G6). Although, we can derive that

U sees the key K_v, U does not believe anything about it (i.e., U does not believe that K_v is fresh and good for authentication for U and V). The problem is that U cannot conclude that V sent the key K_v, because K_v is received via the channel C_t, which can be written by everybody (since K_t is sent in clear in step 6). Even if U believed that V had sent K_v, it would not believe that V has sent it recently, since there is nothing fresh for U in the messages that it receives. Therefore, we can conclude that the protocol has at least two weaknesses:

1. K_t is sent in clear, so it is known to everybody.
2. U does not receive any fresh messages in the protocol.

3 Attacks

In this section, we present three attacks that exploit the weaknesses identified in the previous section. The first attack is based on eavesdropping of messages, the second attack is based on modification of messages, while the third attack is based on replay of old messages. Assuming that an intruder can eavesdrop, modify, and replay messages is not unrealistic. The authors in [SN97] are aware of this ability of the intruder, since they consider the following threats related to authentication procedures to be possible regarding the GLOMONET[2]:

2) Threats on interworking between terminal and visited network:

...

- signal eavesdropping between a terminal and a network;
- signal modification between a terminal and a network.

4) Threats on interworking between networks:

...

- signal modification between networks;
- signal eavesdropping between networks.

However, later, they exclude signal modification from the scope of their paper by noting that "anonymous interference with signals (such as jamming) is difficult to prevent by authentication procedures". This statement is true, but this does not justify to exclude the signal modification threat from the analysis. We believe that the goal of an authentication protocol is not to prevent such interferences, but their consequences. Thus, it might be possible that the authentication of a legitimate user fails due to an attack based on signal modification (we rather consider this a denial of service attack), but a well designed authentication protocol should never assign false identities to principals as a consequence of an attack (even if the attack is based on signal modification). Therefore, we consider signal modification to be possible in the sequel.

[2]We number the items according to [SN97].

Attack 1:

In this attack, the intruder I and the home network H collaborate in order to obtain the authentication key K_v of the roaming user U and the visited network V. Let us assume that U started the protocol. In step 4, H stores $K_tF(K_v)$. In step 6, I eavesdrops K_t and sends it to H. Using K_t, H decrypts the previously stored message $K_tF(K_v)$, and obtains the key K_v. Then, H sends K_v to I, who, by possessing the authentication key that is supposed to be a shared secret between U and V, can impersonate U and/or V.

This attack is based on the assumption that the home network is not trustworthy, and it collaborates with intruders. This assumption seems to be unusual (we discuss this issue in Section 4.1), but we note that the authors in [SN97] considered that "it is possible that the entities concerned take illegal action in roaming-service provision. Therefore, it is desirable not to leak the authentication keys needed for their authentication to the other networks". It is clear that this desire is not satisfied by the protocol.

Attack 2:

In this attack, the intruder I obtains the authentication key K_v of the roaming user U and the visited network V without any collaboration with the home network H. We assume that I is a legitimate, but malicious user with the same home network H as the roaming user U. The attack scenario is the following:

1. $U \to V : Request(U, H)$
2. $V \to H : rnd_1$
3. $H \to V : K_nF(rnd_1),\ rnd_2$
4. $V \to H : K_nF(rnd_2),\ K_nF(K_tF(K_v))$
5. $H \to V : K_{uh}F(K_tF(K_v))$
6. $V \to U : rnd_3,\ K_t,\ K_{uh}F(K_tF(K_v))$
7. $U \to V : K_vF(rnd_3)$
8. $V \to U : K_vF(K_vF(rnd_3))$
    1. $I \to V : Request(I, H)$
    2. $V \to H : rnd'_1$
    3. $H \to V : K_nF(rnd'_1),\ rnd'_2$
    4. $V \to I(H) : K_nF(rnd'_2),\ K_nF(K'_tF(K'_v))$
    4. $I(V) \to H : K_nF(rnd'_2),\ K_nF(K_tF(K_v))$
    5. $H \to V : K_{ih}F(K_tF(K_v))$
    6. $V \to I : rnd'_3,\ K'_t,\ K_{ih}F(K_tF(K_v))$

where $V \to I(H) : M$ means that the message M that was sent by V to H is intercepted by I; and $I(V) \to H : M$ means that I sends the message M to H in the name of V.

Let us assume that U, V, and H successfully run the protocol. In step 4 and in step 6, I

eavesdrops $K_nF(K_tF(K_v))$ and K_t, respectively. Then, I starts the protocol with V. Since I is a legitimate user, it can do that. I lets the protocol run until step 4. In step 4, I exchanges the second part of the message $K_nF(K_t'F(K_v'))$ to $K_nF(K_tF(K_v))$. H accepts the modified message, since the first part $K_nF(rnd_2')$, which is the only part of the message for which freshness can be checked, is correct. H decrypts $K_nF(K_tF(K_v))$, and re-encrypts the result $K_tF(K_v)$ with K_{ih}. When I receives message 6 from V, it obtains K_v, since it knows both K_{ih} and K_t. Later, I can use K_v to impersonate U and/or V in the roaming-service-provision phase.

Attack 3:

This attack exploits the fact that U does not receive any fresh message in the protocol. We assume that K_v^* is a compromised old authentication key of U with V, and that the intruder I recorded the protocol that established K_v^*. Thus, I possesses the old authentication key K_v^*, the corresponding temporary cipher key K_t^*, and the cipher $K_{uh}F(K_t^*F(K_v^*))$. The attack scenario is the following:

1. $U \rightarrow I(V) : Request$
6. $I(V) \rightarrow U : rnd_3',\ K_t^*,\ K_{uh}F(K_t^*F(K_v^*))$
7. $U \rightarrow I(V) : K_v^*F(rnd_3')$
8. $I(V) \rightarrow U : K_v^*F(K_v^*F(rnd_3'))$

When U starts a new instance of the protocol with the *Request* message, I replays back message 6 from the old protocol (I may change the random number rnd_3 to rnd_3'). U thinks that the authentication key is K_v^*, so it sends $K_v^*F(rnd_3')$ to V. This messages is intercepted by I. I generates the last message $K_v^*F(K_v^*F(rnd_3'))$ (it knows K_v^*). In this way, I can impersonate the visited network V.

4 Correction

In this section, we correct the protocol using a simple design tool [BSW98], which is based on synthetic rules that can be used to generate authentication protocols from their goals in a systematic way. The list of the synthetic rules used in this section can be found in the Appendix.

As we have shown in Section 2, the goals (G3) and (G6) cannot be derived from the initial assumptions and the protocol description. Indeed, if we could derive (G3), then we would be able to derive (G6). Thus, the crucial point is the goal (G3). In the following, we generate the protocol steps that are required to reach the goal (G3). Then we construct the corrected protocol.

We start the synthesis with rule (Syn10):

$$U \models (w(C_v) = \{U, V\})$$
$$\hookrightarrow \qquad U \models (V \mid\!\sim (w(C_v) = \{U, V\}))$$

$$\hookrightarrow \quad U \models ((V \mid\!\sim (w(C_v) = \{U,V\})) \rightarrow (w(C_v) = \{U,V\}))$$

The second new goal is assumption (A11). We continue with the first new goal. Using (Syn5):

$$\begin{aligned} & U \models (V \mid\!\sim (w(C_v) = \{U,V\})) \\ & \qquad \hookrightarrow \quad U \models (V \mid\!\sim (w(C_v) = \{U,V\},\ rnd_0)) \end{aligned}$$

The new goal can be reached by using (Syn6):

$$\begin{aligned} & U \models (V \mid\!\sim (w(C_v) = \{U,V\},\ rnd_0)) \\ & \qquad \hookrightarrow \quad U \models (V \mid\!\sim (w(C_v) = \{U,V\},\ rnd_0)) \\ & \qquad \hookrightarrow \quad U \models \sharp(w(C_v) = \{U,V\},\ rnd_0) \end{aligned}$$

The second new goal can be reached by using (Syn8):

$$\begin{aligned} & U \models \sharp(w(C_v) = \{U,V\},\ rnd_0) \\ & \qquad \hookrightarrow \quad U \models \sharp(rnd_0) \end{aligned}$$

if rnd_0 is some fresh data for U. We continue with the first new goal $U \models (V \mid\!\sim (w(C_v) = \{U,V\},\ rnd_0))$. Using (Syn10):

$$\begin{aligned} & U \models (V \mid\!\sim (w(C_v) = \{U,V\},\ rnd_0)) \\ & \qquad \hookrightarrow \quad U \models (H \mid\!\sim (V \mid\!\sim (w(C_v) = \{U,V\},\ rnd_0))) \\ & \qquad \hookrightarrow \quad U \models ((H \mid\!\sim (V \mid\!\sim (w(C_v) = \{U,V\},\ rnd_0))) \rightarrow \\ & \qquad\qquad \rightarrow (V \mid\!\sim (w(C_v) = \{U,V\},\ rnd_0))) \end{aligned}$$

The second new goal is assumption (A12). We continue with the first new goal. Using (Syn7):

$$\begin{aligned} & U \models (H \mid\!\sim (V \mid\!\sim (w(C_v) = \{U,V\},\ rnd_0))) \\ & \qquad \hookrightarrow \quad U \lhd C_{uh}(V \mid\!\sim (w(C_v) = \{U,V\},\ rnd_0)) \\ & \qquad \hookrightarrow \quad U \in r(C_{uh}) \\ & \qquad \hookrightarrow \quad U \models (w(C_{uh}) = \{U,H\}) \\ & \qquad \hookrightarrow \quad U \models \sharp(V \mid\!\sim (w(C_v) = \{U,V\},\ rnd_0)) \\ & \qquad \hookrightarrow \quad H \models (V \mid\!\sim (w(C_v) = \{U,V\},\ rnd_0)) \end{aligned}$$

The first new goal is a protocol message. The second and the third new goals are assumptions (A4) and (A5), respectively. The fourth new goal can be reached by using (Syn8) and considering that rnd_0 is fresh for U. We continue with the last new goal. Using (Syn4):

$$H \models (V \mid\sim (w(C_v) = \{U, V\},\ rnd_0))$$

$$\hookrightarrow \quad H \lhd C_n(w(C_v) = \{U, V\}, rnd_0)$$

$$\hookrightarrow \quad H \in r(C_n)$$

$$\hookrightarrow \quad H \models (w(C_n) = \{V, H\})$$

$$\hookrightarrow \quad V \lhd (w(C_v) = \{U, V\},\ rnd_0)$$

The first new goal is a protocol message. The second and the third new goals are assumptions (A1) and (A3). The last new goal is partially reached by default, since V generates K_v. To fully reach the last new goal, V must see rnd_0. This is a protocol message. Thus, we obtained the following protocol:

$$V \lhd rnd_0$$

$$H \lhd C_n(w(C_v) = \{U, V\},\ rnd_0)$$

$$U \lhd C_{uh}(V \mid\sim (w(C_v) = \{U, V\},\ rnd_0))$$

Using this result and considering the other goals (G1), (G2), and (G4)-(G6) as well, we construct the corrected protocol in the following way:

1. $U \rightarrow V : U, H, rnd_0$
2. $V \rightarrow H : rnd_1$
3. $H \rightarrow V : K_n F(rnd_1),\ rnd_2$
4. $V \rightarrow H : K_n F(rnd_2,\ rnd_0,\ U,\ K_v)$
5. $H \rightarrow V : K_{uh} F(rnd_0,\ V,\ K_v)$
6. $V \rightarrow U : rnd_3,\ K_{uh} F(rnd_0,\ V,\ K_v)$
7. $U \rightarrow V : K_v F(rnd_3)$
8. $V \rightarrow U : K_v F(K_v F(rnd_3))$

4.1 Discussion

We note that the correctness of this correction depends on the trustworthiness of the home network. Since the home network H sees the authentication key K_v, assumption (A9) holds and goal (G3) is reached only if the home network does not reveal the key K_v and it does not use it for encrypting messages. If the home network is trustworthy then the corrected protocol reaches all the identified goals (G1)-(G6). Furthermore, it also enables the roaming user U and the visited network V to obtain the second order beliefs in the established authentication key K_v.

However, this means that the correction does not satisfy the original requirement (r8) in [SN97] (confidentiality of the user authentication key in the key generating network to the other networks). We believe that this requirement cannot be satisfied in the given situation. Introducing other parties and assuming other pre-established channels (and modifying the protocol) can help us to solve this problem. Nevertheless, this is out of the scope of this note.

Our correction of the authentication protocol proposed in [SN97] shows that flaws in this protocol can be eliminated by making the home network know the key used in the authentication process. In other words, the home network must keep some control over - at least some knowledge of - the authentication process, which is deliberately left exclusively to the responsibility of the visited network in [SN97]. We can also justify this from a practical point of view. The user may not want to exchange secret keys with a third party only (i.e., a network that it does not have an agreement with); otherwise, it could not verifiably lodge a complaint to its exclusive contract partner, the home network provider, if any damage to its service occurred (e.g., use of its service profile by another user). Since the authentication procedure is left to the visited network, this operator would not be able to trace back the problem either. To prevent this undesirable situation, the GSM specification [GSM], for instance, recommends that the home network has some control over the authentication process. There, the visited network forwards the authentication information to the home network, which actually makes the decision of accepting or refusing the call request. It seems to be questionable whether the effort to avoid the necessity to contact the home network each time the user authenticates to the visited network is really practical.

Finally, we note, that our aim was to correct the protocol proposed in [SN97], and not to design a new one. Therefore, it might be possible that our correction is not the "optimal" protocol for the given purposes. This means that other protocols may use less messages and/or encryption operations, and, at the same time, they may reach the same goals.

5 Conclusion

We analysed the authentication protocol that has been proposed for the global mobility network in a recent issue of the IEEE Journal on Selected Areas in Communications. Our analysis was based on a simple logic of authentication. We revealed two serious weaknesses in the protocol, and we demonstrated three attacks that exploit these weaknesses. We corrected the protocol using a simple design tool. The corrected version of the protocol satisfies all the original requirements but one. The consequence of this is the need for the assumption that the home network does not leak and does not use authentication keys.

References

[BAN90] M. Burrows, M. Abadi, and R. Needham. A logic of authentication. *ACM Transactions on Computer Systems*, 8(1):18–36, February 1990.

[BSW98] L. Buttyán, S. Staamann, and U. Wilhelm. A simple logic for authentication protocol design. In *Proceedings of the 11th IEEE Computer Security Foundations Workshop*, 1998. (to appear)

[GSM] ETSI. Security Aspects. GSM 02.09 version 4.4.1, ETS 300 506, 2nd ed., 1998.

[NS78] R. Needham and M. Schroeder. Using encryption for authentication in large networks of computers. *Communications of the ACM*, 21(12):993–999, 1978.

[SN97] S. Suzuki and K. Nakada. An authentication technique based on distributed security management for the global mobility network. *IEEE Journal on Selected Areas in Communications*, 15(8):1608–1617, 1997.

[Syv91] P. Syverson. The use of logic in the analysis of cryptographic protocols. In *Proceedings of the IEEE CS Symposium on Research in Security and Privacy*, pages 156–170, 1991.

Appendix

Language

Hereafter we will use the following notations: P and Q range over principals; C is a channel; X represents a message, which can be data or formulae or both; $C(X)$ denotes message X on channel C; ϕ will be used to denote a formula.

The basic formulae are the following:

$P \lhd C(X)$: P sees $C(X)$, where $C(X)$ is message X sent via channel C. If P cannot read channel C, then P cannot recognise and understand this message (i.e., P cannot determine which channel was used and what was the message).

$P \lhd X \mid C$: P sees X via C. P received message X via channel C. This is possible only if someone has sent this message, and P can read this channel.

$P \lhd X$: P sees X. Someone has sent a message containing X via a channel that P can read.

$\sharp(X)$: X is fresh. X has never been said before the current run of the protocol. This is usually true for nonces.

$P \mid\!\sim X$: P once said X. P at some time sent a message that contained X. We do not know exactly when the message was sent.

$P \parallel\!\sim X$: P has recently said X. This means that P uttered X in the current run of the protocol.

If ϕ is a formula, then the following is also a formula:

$P \models \phi$: P believes ϕ. P believes that ϕ is true. This does not mean that ϕ is really true, but P acts as though.

Further formulae can be derived by using the conventional logical operators from propositional logic. If ϕ_1 and ϕ_2 are formulae, then the following are also formulae:

$\phi_1 \wedge \phi_2$: ϕ_1 and ϕ_2.

$\phi_1 \vee \phi_2$: ϕ_1 or ϕ_2.

$\phi_1 \rightarrow \phi_2$**:** ϕ_1 implies ϕ_2.

We also use notations from set theory. The meaning of these notations is straightforward in our language (e.g. $P \in \mathcal{A}$, where $\mathcal{A}$ is a set of principals, is a formula, which means that principal P is an element of the set $\mathcal{A}$).

Inference Rules

(S1) If a principal P receives a message X via a channel C, and P can read this channel, then P recognises that the message has arrived on C and P can see the message.

$$\frac{P \lhd C(X), P \in r(C)}{P \models (P \lhd X \mid C), P \lhd X}$$

(S2) If a principal P sees a compound message (X, Y), then it sees also parts of the message (i.e., X and Y).

$$\frac{P \lhd (X, Y)}{P \lhd X, P \lhd Y}$$

(I1) If a principal P believes that a channel C can be written only by a set of principals $\mathcal{W}$, then P believes that if it receives a message via C, then someone from the set $\mathcal{W}$ except P itself ($\mathcal{W} \setminus \{P\}$) said X.

$$\frac{P \models (w(C) = \mathcal{W})}{P \models ((P \lhd X \mid C) \rightarrow \bigvee_{\forall Q_i \in \mathcal{W} \setminus \{P\}} (Q_i \mid\sim X))}$$

(I2) If a principal P believes that another principal Q has said a compound message (X, Y), then it believes that Q has said parts of the message as well (i.e., X and Y).

$$\frac{P \models (Q \mid\sim (X, Y))}{P \models (Q \mid\sim X), P \models (Q \mid\sim Y)}$$

(I3) If a principal P believes that another principal Q has recently said a compound message (X, Y), then it believes that Q has recently said parts of the message as well (i.e., X and Y).

$$\frac{P \models (Q \parallel\!\sim (X, Y))}{P \models (Q \parallel\!\sim X), P \models (Q \parallel\!\sim Y)}$$

(F1) If a principal P believes that another principal Q said a message X and P also believes that X is fresh, then P believes that Q has recently said X.

$$\frac{P \models (Q \mid\sim X), P \models \sharp(X)}{P \models (Q \parallel\!\sim X)}$$

(F2) If a principal P believes that part of a compound message X is fresh, then it believes that the whole message (X, Y) is fresh.

$$\frac{P \models \sharp(X)}{P \models \sharp(X, Y)}$$

(F3) If a principal P believes that a key K is fresh, then it believes that the encryption of a message X with the key K is fresh.

$$\frac{P \models \sharp(K)}{P \models \sharp(K(X))}$$

(R1) If a principal P believes that ϕ_1 implies ϕ_2 and the principal believes that ϕ_1 is true, then it believes that ϕ_2 is also true.

$$\frac{P \models (\phi_1 \rightarrow \phi_2), P \models \phi_1}{P \models \phi_2}$$

Synthetic rules

(Syn1) To recognise that a message X arrived via a channel C, it is sufficient for a principal P to receive $C(X)$ and to be able to read C.

$$\begin{array}{lll} P \models (P \lhd X \mid C) & & \\ & \hookrightarrow & P \lhd C(X) \\ & \hookrightarrow & P \in r(C) \end{array}$$

(Syn2) To see a message X, it is sufficient for a principal P to see a message (X, Y) that contains X or to receive X via a channel C.

$$\begin{array}{lll} P \lhd X & & \\ & \hookrightarrow & P \lhd (X, Y) \ \ / \ \ P \models (P \lhd X \mid C) \end{array}$$

(Syn3) To believe that a principal Q said X, it is sufficient for a principal P to believe that Q said a message (X, Y) that contains X.

$$\begin{array}{lll} P \models (Q \mid\sim X) & & \\ & \hookrightarrow & P \models (Q \mid\sim (X, Y)) \end{array}$$

(Syn4) To believe that a principal Q said X, it is sufficient for a principal P to receive X via a channel C that it can read and that it believes can be written only by Q, or P and Q. Furthermore, Q needs to see X.

$$\begin{array}{lll} P \models (Q \mid\sim X) & & \\ & \hookrightarrow & P \lhd C(X) \\ & \hookrightarrow & P \in r(C) \\ & \hookrightarrow & P \models (w(C) = \{Q\}) \;\; / \;\; P \models (w(C) = \{P, Q\}) \\ & \hookrightarrow & Q \lhd X \end{array}$$

(Syn5) To believe that a principal Q has recently said X, it is sufficient for a principal P to believe that Q has recently said a message (X, Y) that contains X.

$$\begin{array}{lll} P \models (Q \mid\!\mid\sim X) & & \\ & \hookrightarrow & P \models (Q \mid\!\mid\sim (X, Y)) \end{array}$$

(Syn6) To believe that a principal Q has recently said X, it is sufficient for a principal P to believe that Q said X and X is fresh.

$$\begin{array}{lll} P \models (Q \mid\!\mid\sim X) & & \\ & \hookrightarrow & P \models (Q \mid\sim X) \\ & \hookrightarrow & P \models \sharp(X) \end{array}$$

(Syn7) If X is a formula and P believes that Q is honest (i.e., $P \models ((Q \mid\!\mid\sim \phi) \rightarrow (Q \models \phi))$), then to believe that Q has recently said X, it is sufficient for P to receive X via a channel C that it can read and that it believes can be written only by Q, or P and Q. Furthermore, P needs to believe that X is fresh and Q needs to believe X.

$$\begin{array}{lll} P \models (Q \mid\!\mid\sim X) & & \\ & \hookrightarrow & P \lhd C(X) \\ & \hookrightarrow & P \in r(C) \\ & \hookrightarrow & P \models (w(C) = \{Q\}) \;\; / \;\; P \models (w(C) = \{P, Q\}) \\ & \hookrightarrow & P \models \sharp(X) \\ & \hookrightarrow & Q \models X \end{array}$$

(Syn8) To believe that a message X is fresh, it is sufficient for a principal P to believe that some part X' of X is fresh.

$$\begin{array}{lll} P \models \sharp(X) & & \\ & \hookrightarrow & P \models \sharp(X') \end{array}$$

(Syn9) To believe that a principal Q believes a formula ϕ, it is sufficient for a principal P to believe that Q is honest and that Q has recently said ϕ.

$$
\begin{aligned}
& P \models (Q \models \phi) \\
& \qquad \hookrightarrow \qquad P \models (Q \mid\sim \phi) \\
& \qquad \hookrightarrow \qquad P \models ((Q \mid\sim \phi) \rightarrow (Q \models \phi))
\end{aligned}
$$

(Syn10) To believe a formula ϕ, it is sufficient for a principal P to believe that a principal Q is honest and competent, and that Q has recently said ϕ.

$$
\begin{aligned}
& P \models \phi \\
& \qquad \hookrightarrow \qquad P \models (Q \mid\sim \phi) \\
& \qquad \hookrightarrow \qquad P \models ((Q \mid\sim \phi) \rightarrow \phi)
\end{aligned}
$$

(Syn11) To believe a formula ϕ, it is sufficient for a principal P to believe a formula ϕ' and the implication $\phi' \rightarrow \phi$.

$$
\begin{aligned}
& P \models \phi \\
& \qquad \hookrightarrow \qquad P \models \phi' \\
& \qquad \hookrightarrow \qquad P \models (\phi' \rightarrow \phi)
\end{aligned}
$$