Title: Formal analysis of 3G authentication and key agreement protocol

Abstract: *This contribution presents an analysis of the 3G AKA protocol using an enhanced BAN logic. This enhanced BAN-logic is described in reference [8] of which copies are made available at the meeting for convenience of the delegates. An overview of authentication logics is given in reference [4] which can be downloaded from the web.*

1 Introduction

This paper is on the formal analysis of the authentication and key agreement protocol contained in [1, sect.6.3], called the SEQ-protocol in the sequel. This analysis is made using the authentication logic AUTLOG [7], [8], [5], [6], which is an enhanced BAN-logic [2]. The paper proves that the goals of the SEQ-protocol as they are stated in section 3.3. below are met by the protocol.

Authentication logics are one of the most attractive tools to analyse cryptographic protocols. Since their invention in 1989 [2] a lot of work was done on them, both theoretical research and practical applications. For an overview see [4]. Authentication logics investigate how the beliefs of the participants evolve during the exchange of the messages. A formal analysis consists of four steps:

1. The necessary prerequisites are explicitly stated.
2. The messages are formally described.
3. The protocols goals are explicitly stated.
4. The formal calculus is applied to show how the protocols goals can be derived from the messages and the prerequisites using the rules of the calculus.

Note that this method leads to positive statements like the protocol goal "A believes that K is a good key for communication with B" can be derived. If a protocol goal cannot be derived this may have different reasons, e.g., it could be that some of needed prerequisites are missing, it could also be that there is a failure in the protocol. This method does not explicitly find the failure but it gives the protocol designer or analyser a hint where the failue might be.

In this context we should mention that *all* methods for formal analysing protocols share the feature that none of them is capable to find all mistakes of a protocol, cf. [4]. Each method provides a different view on a given protocol. This means that verifying a protocol with one formal method increases the confidence in a protocol but gives no 100%-guarentee that there is no bug.

The experience with authentication logics is that it is "easy" to apply, at least compared to other formal methods. It helps significantly to understand what a protocol really does because you have to be very precise about the prequisites and the protocol goals. Especially, you should pay attention to the prerequisites and make sure that they really are fulfilled in the scenario where the protocol will be used.

One critique concerning BAN-logic and most of its dialects has been the fact that the calculus itself is inconsistent. Therefore AUTLOG is based on a formal semantics [8]. It is proven in [8] that the AUTLOG-calculus is correct with respect to that formal semantics. Unfortunately, most of the BAN-dialects lack this sort of justification. Another common critique concerning BAN-logics refer to the so-called idealization step. Note that this idealization step is not used within AUTLOG [8].

2 The SEQ Protocol

There are three parties involved in the protocol: The user U represented by his USIM; the home environment HE represented by the authentication centre, and the serving network SN represented by the visitor location register. For the sake of simplicity we make two assumptions: Firstly, we restrict our analysis to the case that HE sends one authentication quintuplet at a time. Secondly, SN stands for the whole set of authorized serving networks. This assumption is reasonable, because the user will not get assurance which SN he is using. He will only know that SN is authorized.

There are three security relevant messages:

Message 1

On request from SN the home environment HE generates an authentication quintuplet. This authentication quintuplet uses the following parameters:

- a random number r
- a key K shared between HE and U
- a sequence number SEQ which is synchronized between HE and U
- an expected response $RES = f2(K, r)$ using a MAC-function $f2$ [1]
- a cipher key $CK = f3(K, r)$ using a one-way function $f3$ suitable for key derivation.
- a integrity key $IK = f4(K, r)$ using a one-way function $f4$ suitable for key derivation.
- an anonymity key $Ka = f5(K, r)$ using a one-way function $f5$ suitable for key derivation.
- authentication token $AUTN = \{SEQ\}_{Ka},\ f1(K, SEQ, r)$ using a MAC-function $f1$

The following message is sent to SN:

$$HE \longrightarrow SN : \quad r, RES, CK, IK, AUTN$$

Message 2

After receipt of this quintuplet SN forwards to U the random number r which serves as a challenge and the authentication token.

$$SN \longrightarrow U : \quad r, AUTN$$

[1] We assume that the parameters $PAR1$,...,$PAR5$ are integrated into the definitions of the functions $f1$,..$f5$, cf. [1, sect.6.3.2, note 4].

Message 3

After receipt of the challenge r the user U computes an expected authentication token $XAUTN$ and compares this with the received $AUTN$. If they are identical U computes the response RES and sends it to SN:

$$U \longrightarrow SN: \quad RES$$

3 Formal Analysis

3.1 Formalisation of the protocol prerequisites

3.1.1 Prerequisites on SN's side

SN believes that HE has jurisdiction concerning keys between U and SN and concerning the freshness of these keys.

$$SN\,believes\,HE\,controls\,(SN \overset{K'}{\leftrightarrow} U \wedge fresh(K')) \tag{1}$$

SN believes that if HE says CK, IK he means that these are good key for communication with U, i.e., HE is regarded as a sort of key server in this case:[2]

$$SN\,believes \quad (HE\,says\,RES \longrightarrow HE\,believes\,(SN \overset{RES}{\leftrightarrow} U \wedge fresh(RES)) \tag{2}$$

$$SN\,believes \quad (HE\,says\,CK \longrightarrow HE\,believes\,(SN \overset{CK}{\leftrightarrow} U \wedge fresh(CK)) \tag{3}$$

$$SN\,believes \quad (HE\,says\,IK \longrightarrow HE\,believes\,(SN \overset{IK}{\leftrightarrow} U \wedge fresh(IK)) \tag{4}$$

It is assumed that the communication path between HE and SN is secure and that SN is able to detect that the message received from HE is a list comprising five items:

$$SN\,believes\,HE\,says\,(r, RES, CK, IK, AUTN) \tag{5}$$

SN is able to identify $f2(K,r)$ with the expected response RES:

$$(f2(K,r))_{SN} \equiv RES \tag{6}$$

SN believes that if a user is able to say RES this user will also have the keys CK and IK. This belief is justified by the fact that HE has connected these items in his message (cf. 5) and SN trusts HE to send him correct authentication quintuplets:[3]

$$SN\,believes \quad (U\,says\,RES \longrightarrow U\,has\,(CK, IK)) \tag{7}$$

SN believes that he has not generated the following message himself:

$$SN\,believes\,\neg SN\,said\,RES \tag{8}$$

[2] Firstly, SN does not know K and thus does not know the inner structure of $RES{=}f2(K,r)$ etc; therefore we simply write RES. Secondly, in this protocol RES has the role of a secret to be shared between U and SN. The notation $SN \overset{RES}{\leftrightarrow} U$ refers both to shared key and to shared secrets.

[3] HE can give the corresponding assurance to SN because U can only say RES if U has K and r. U can then derive CK and IK.

3.1.2 Prerequisites on U's side

U has key K, recognizes it, and believes that it is good key for communication with HE:

$$U\,has\,K \tag{9}$$
$$U\,recognizes\,K \tag{10}$$
$$U\,believes\;HE \overset{K}{\leftrightarrow} U \tag{11}$$
$$U\,believes\;HE\,has\,K \tag{12}$$

U believes that the sequence number SEQ is fresh, i.e. not used in an earlier protocol run. This belief is justified because U is able to check whether SEQ is fresh.

$$U\,believes\,fresh(SEQ) \tag{13}$$

U regards the following messages as atomic messages

$$(X)_U \equiv X \quad \forall X \in \{SEQ, r, K\} \tag{14}$$

U believes that he has not generated the following messages himself:

$$U\,believes\,\neg U\;said\,f1(K,r) \tag{15}$$

U believes that HE has jurisdiction concerning keys between U and SN and U believes that if HE says r he means that the derived keys $CK = f3(K,r)$ and $IK = f4(K,r)$ are good keys for communication with SN:

$$U\,believes\,HE\,controls\,SN \overset{K'}{\leftrightarrow} U \tag{16}$$

$$U\,believes\,(HE\,says\,r \longrightarrow HE\,believes\,SN \overset{fi(K,r)}{\leftrightarrow} U) \quad for\,i = 3,4 \tag{17}$$

U believes that HE has jurisdiction about the freshness of random numbers, and U believes that if HE says r he means that this number is fresh:

$$U\,believes\,HE\,controls\,fresh(r) \tag{18}$$

$$U\,believes\,(HE\,says\,r \longrightarrow HE\,believes\,fresh(r)) \tag{19}$$

3.1.3 Prerequisites on HE's side

HE has a key K and believes that K is a good key for communication with U:

$$HE\,has\,K \tag{20}$$
$$HE\,believes\;HE \overset{K}{\leftrightarrow} U \tag{21}$$

HE believes that the random number r is good for deriving of shared keys (resp. shared secrets):

$$HE\,believes\,good_{fi}(r) \quad for\,i = 2, ..., 5 \tag{22}$$

3.2 Formal Descriptions of the Transactions

$$SN\ sees\quad r, f2(K,r), f3(K,r), f4(K,r), \{SEQ\}_{f5(K,r)}, f1(K,SEQ,r) \tag{23}$$

$$U\ sees\quad r, \{SEQ\}_{f5(K,r)}, f1(K,SEQ,r) \tag{24}$$

$$SN\ sees\quad f2(K,r) \tag{25}$$

3.3 Security goals

The following goals should be achieved after a successful run of the protocol:

1. Entity authentication of U to SN and of HE to U:

   a. $SN\ believes\ U\ says\ RES$

   b. $U\ believes\ HE\ says\ (SEQ, r)$

2. Key agreement between U and SN:

   a. $SN\ has\ CK,\quad SN\ has\ IK$

   b. $U\ has\ f3(K,r),\quad U\ has\ f4(K,r)$

3. Implicit key authentication between U and SN:

   a. $SN\ believes\ SN \overset{CK}{\leftrightarrow} U,\quad SN\ believes\ SN \overset{IK}{\leftrightarrow} U$

   b. $U\ believes\ SN \overset{f3(K,r)}{\leftrightarrow} U,\quad U\ believes\ SN \overset{f4(K,r)}{\leftrightarrow} U$

4. Assurance of key freshness between U and SN:

   a. $SN\ believes\ fresh(CK),\quad SN\ believe\ fresh(IK)$

   b. $U\ believes\ fresh(f3(K,r)),\quad U\ believes\ fresh(f4(K,r))$

5. Key confirmation between U and the network:

   a. $SN\ believes\ U\ has\ (CK, IK)$

   b. $U\ believes\ HE\ has\ (f3(K,r), f4(K,r))$

6. Confidentiality of the user identity related information (i.e. sequence number SEQ) on the air interface: Note that the achievement of confidentiality goals cannot be proven by authentication logics in an explicit manner. The confidentiality follows from the following fact:

   $HE\ believes\ HE \overset{f5(K,r)}{\leftrightarrow} U$

3.4 Proving the security goals

3.4.1 Security goals refering to SN

Concerning the notation: The number in front of the implication arrow shows which formulae lead to the implication, the symbols above the arrow refer to the rule of the calculus [8, sect. 4] which has been used for this implication.Since the rules MP (modus ponens) and K (rationality rule) are used very often we do not always mention it.

Receiving the first message 23 it follows directly by rule H1:

$$23 \xrightarrow{H1} \boxed{SN\, has\, (CK, IK)} \text{ (goal 2.a)} \tag{26}$$

From 5 and prerequisite 2 it follows

$$5,2 \xrightarrow{MP} SN\, believes\, HE\, believes\, (SN \overset{RES}{\leftrightarrow} U \wedge fresh(RES)) \tag{27}$$

$$1,27 \xrightarrow{J} SN\, believes\, (SN \overset{RES}{\leftrightarrow} U \wedge fresh(RES)) \tag{28}$$

Analogously we can prove from 5 and the prerequisites 1, 3, and 4 the goals key agreement, implicit key authentication and assurance on freshness on SN's side:

$$\boxed{SN\, believes\, SN \overset{CK}{\leftrightarrow} U, \quad SN\, believes\, SN \overset{IK}{\leftrightarrow} U} \text{ (goal 3.a)} \tag{29}$$

$$\boxed{SN\, believes\, fresh(CK), \quad SN\, believes\, fresh(IK)} \text{ (goal 4.a)} \tag{30}$$

From the third message SN derives:

$$25,6 \xrightarrow{C} SN\, believes\, SN\ sees\ RES \tag{31}$$

$$31,28,8 \xrightarrow{A1,K} SN\, believes\, U\ said\ RES \tag{32}$$

$$28,32 \xrightarrow{NV,K} \boxed{SN\, believes\, U\ says\ RES} \text{ (goal 1.a)} \tag{33}$$

$$7,33 \xrightarrow{MP,K} \boxed{SN\, believes\, U\ has\, (CK, IK)} \text{ (goal 5.a)} \tag{34}$$

3.4.2 Security goals refering to U

$$24 \xrightarrow{H1} U\, has\, r \tag{35}$$

$$9,35 \xrightarrow{H2} U\, has\, (K, r) \tag{36}$$

$$36 \xrightarrow{H3} \boxed{U\, has\, fi(K, r)\ for\, i = 2, ..., 5} \text{ (goal 2.b)} \tag{37}$$

$$24,37 \xrightarrow{H1,H3} U\, has\, SEQ \tag{38}$$

$$36,38 \xrightarrow{H2,C3} (f1(K, SEQ, r))_U \equiv f1((K, SEQ, r)_U) \tag{39}$$

$$10 \xrightarrow{C1} (K, SEQ, r)_U \equiv (K_U, SEQ_U, r_U) \tag{40}$$

$$14,39,40 \xrightarrow{E2,E3} (f1(K, SEQ, r))_U \equiv f1(K, SEQ, r) \tag{41}$$

$$24, 41 \xrightarrow{C} U\, believes\, U\, sees\ f1(K, SEQ, r) \tag{42}$$

$$42, 11, 15 \xrightarrow{A1} U\, believes\, HE\, said\ \ (SEQ, r) \tag{43}$$

$$13 \xrightarrow{F1} U\, believes\, fresh\,(SEQ, r) \tag{44}$$

$$43, 44 \xrightarrow{NV} \boxed{U\, believes\, HE\, says\ \ (SEQ, r)} \text{ (goal 1.b)} \tag{45}$$

$$12, 45 \xrightarrow{H1,H2} U\, believes\, HE\, has\ \ (K, r) \tag{46}$$

$$46 \xrightarrow{H3} \boxed{U\, believes\, HE\, has\ \ fi(K, r) \quad for\ i = 3, 4} \text{ (goal 5.b)} \tag{47}$$

$$17, 45 \xrightarrow{K} U\, believes\, (HE\, believes\, SN \overset{fi(K,r)}{\leftrightarrow} U) \quad for\ i = 3, 4 \tag{48}$$

$$16, 48 \xrightarrow{J} \boxed{U\, believes\, SN \overset{fi(K,r)}{\leftrightarrow} U \quad for\ i = 3, 4} \text{ (goal 3.b)} \tag{49}$$

$$19 \xrightarrow{MP} U\, believes\, HE\, believes\, fresh(r) \tag{50}$$

$$18, 50 \xrightarrow{J} U\, believes\, fresh(r) \tag{51}$$

$$51 \xrightarrow{F2} \boxed{U\, believes\, fresh(fi(K, r)) \quad for\ i = 3, 4} \text{ (goal 4.b)} \tag{52}$$

3.4.3 Security goals refering to HE

$$21, 22 \xrightarrow{KD} \boxed{HE\, believes\ HE \overset{f5(K,r)}{\leftrightarrow} U} \text{ (goal 6)} \tag{53}$$

4 Comments

Assurance of key's freshness on the user's side: The user U trusts that HE has chosen a fresh random number r together with a fresh SEQ (formula 18). If one does not want to make this reasonable assumption (cf. [3]) then SEQ could be included in the computation of $CK = f3(K, SEQ, r)$ and $IK = f4(K, SEQ, r)$. Then U could convince himself that the derived keys are fresh because he can control whether SEQ is fresh.

References

[1] 3GPP S3.03 VO.1.2 (1999-03) *3G Security Architecture.*

[2] M. Burrows, M. Abadi, R. Needham. *A logic for authentication.* DEC System Research Technical Report No 39, Feb 1989.

[3] ETSI TDoc SMG 10 99C013, "Mutual authentication and key establishment for UMTS Phase 1 based on random challenges and sequence numbers".

[4] Stefanos Gritzalis, Diomidis Spinellis, Paagiotis Georgiadis. *Security Protocols over Open Networks*
and Distributed Systems: Formal Methods for their Analysis, Design, and Verification. Computer Communications 1999, http://kerkis.math.aegean.gr/˜dspin/pubs/jrnl/1997-CompComm-Formal/html/formal.htm.

[5] Volker Kessler, Heike Neumann. *A Sound Logic for Analysing Electronic Commerce Protocols.* Computer Security - ESORICS 98, Springer LNCS 1485, 345-360.

[6] Heike Neumann, Volker Kessler. *Formale Analyse von kryptographischen Protokollen mit BAN-Logik.* Datenschutz und Datensicherheit 2/1999, 90-93.

[7] Gabriele Wedel. *Formale Semantik für Authentifikationslogiken.* Diplomarbeit, RWTH Aachen (1995).

[8] Gabriele Wedel, Volker Kessler. *Formal Semantics for Authentication Logics.* Computer Security - ESORICS 96, Springer LNCS 1146, 218-241.