Some Remarks on the Logic of Gong, Needham and Yahalom

A. Mathuria * R. Safavi-Naini * P. Nickolas

Center for Computer Security Research
Department of Computer Science
University of Wollongong
NSW 2522, Australia
email: {g9312439, rei, peter}@cs.uow.edu.au

Abstract

This paper points out instances of unsoundness, incompleteness, and redundancy in the logic of Gong, Needham and Yahalom. Solutions are proposed for each of these problems. The logic is extended to formalize the use of an uncertified key in the Yahalom protocol, enabling the discovery of a previously unreported redundancy in the protocol.

Keywords: formal logic, semantics, protocol verification, cryptographic protocols

1 Introduction

The use of logic to reason about secure cryptographic protocols was proposed in the seminal work of Burrows, Abadi and Needham [1]. The BAN logic initiated a flurry of research into the application of logic for the analysis of secure protocols.

In [2], Gong, Needham and Yahalom propose an extension of the BAN logic. Their extension, known as the GNY logic, offers a number of advantages over the BAN approach. It distinguishes between possessions and beliefs thus enabling reasoning at a lower level than the BAN logic. The logic includes several additional constructs and rules, thereby allowing a wider range of protocols to be analyzed. It makes explicit some of the assumptions made in the BAN approach, and is thus seen to be more general. The GNY approach to protocol analysis also allows infeasible protocol specifications [3] to be detected.

Gong, Needham and Yahalom, like Burrows, Abadi and Needham, provide an "operational" semantics for their logic, but as Syverson [4] points out, this semantics is not independently motivated, as it takes its structure directly from the logical syntax. An argument based on this semantics that the logic is sound is therefore at best problematic. Indeed, examples are presented below of unsound conclusions derivable in the GNY logic. These examples reinforce the need for providing an independently motivated formal semantics for such logics, as has been argued by Syverson [4, 5] and Tuttle [6]. Such a semantics can via soundness and completeness results provide assurance about the correctness and expressiveness of the inference rules.

In this paper we point out several classes of problems which arise in the GNY logic:

1. an unsound rule;

2. the possibility of drawing unsound conclusions by combining rules;

*Support for this work was provided in part by the University of Wollongong Computer Security Technical and Social Issues research program, Australian Research Council (ARC) small grant, and ARC grants A49131885 and A49030136.

3. the incompleteness of the set of rules; and

4. rules with redundant premises

We suggest solutions to these problems, at the syntactic level. A formal justification of these suggested solutions, however, rests ultimately on provision of an independently motivated formal semantics for the logic, which is beyond the scope of this paper.

An interesting outcome of this work is a simplification of the Yahalom protocol [1], which resulted from its analysis by using the GNY logic (with a new rule added). In our analysis of the protocol, we adopt the protocol parser proposed in Gong's logic [7], rather than that of the GNY logic. We find that it may not be possible to apply the inference rules of the logic, as intended by GNY, to a protocol description generated by the GNY parser [2]. The parser given in [7] avoids this problem, and we adopt it in our analysis of the Yahalom protocol. Needless to say, this does not affect the validity of the problems we point out with the GNY logic. In fact, our examples also apply, equally well, to Gong's logic too.

We assume that the reader is familiar with the constructs and the inference rules of the GNY logic. For the sake of convenience, the complete set of inference rules of the logic is given in Appendix A. The paper is organized as follows. In section 2 we point out a flaw in the recognizability rule R6, and propose a possible solution. In section 3 we propose side conditions to several freshness and recognizability rules of the logic, the absence of which leads to surprising results similar to the one shown by Anderson in [8]. In section 4 we show that the logic fails to certify the Yahalom protocol. This motivates us to propose the addition of a new message interpretation rule to the logic. Our analysis of this protocol guides us in discovering a previously unreported redundancy in the protocol. In section 5 we identify redundant premises in the message interpretation rules I2 and I2$'$ of the logic. Finally, in section 6 we conclude the paper.

2 Unsound rule

The recognizability rules of the GNY logic enable principals to advance their beliefs about recognizable formulae. A recognizability rule of the logic is:

$$\text{R6} \quad \frac{P \ni H(X)}{P \mid\equiv \phi(X)}$$

i.e., if principal P possesses formula $H(X)$ then he is entitled to believe that X is recognizable.

Syverson and Oorschot [9] have already argued that R6 is too strong. In fact, R6 is unsound. For example, assume that $P \ni X$. By applying rules P4 and R6, we can then derive the groundless conclusion that $P \mid\equiv \phi(X)$. There is nothing wrong with P4; it just says that a principal is capable of performing a computation on a formula he possesses. The problem lies with R6. Note that P can believe that X is recognizable only if he has certain expectations about the contents of X. However, rule R6 enables us to infer that P's possession of X is sufficient for him to believe that X is recognizable. This rule therefore gives an unsound conclusion.

2.1 Remedy

The rule R6 fails to capture a principal's expectations about the contents of recognizable formulae. To remedy this, we introduce an additional premise in the rule, as follows:

$$\text{R6}' \quad \frac{P \mid\equiv \phi(H(X)),\ P \ni H(X)}{P \mid\equiv \phi(X)}$$

i.e., if P possesses a formula $H(X)$ and believes that it is recognizable then he is entitled to believe that X is recognizable.

3 Unsound conclusions from combination of rules

In [8], Anderson has pointed out that the freshness rules F2 and F7 of the GNY logic, when used together, imply a strange result. Suppose that for principal P all of the following conditions hold: (1) P believes that formula X is recognizable; (2) P possesses a key K; (3) P believes that K is fresh. Then by applying F7 we obtain $P \models \sharp(\{X\}_K)$. By further applying F2 we conclude that $P \models \sharp(X)$. For example, in the analysis of the modified enhanced Needham-Schroeder protocol in [2, p. 242], we can derive the nonsensical conclusion $P \models \sharp(Q)$ in this way.

We note that this problem is not only confined to the freshness rules F2 and F7 used together. There are several other pairs of freshness and recognizability rules which lead to the same strange result, in different ways. We list below each such pair of rules.

1. F7 and F2
2. R2 and F7
3. F8 and F4
4. F9 and F3[1]
5. R3 and F9
6. R4 and F8[1]

To eliminate this problem, we propose side conditions to several of the freshness and recognizability rules of the logic. These side conditions are found to eliminate the derivation of unsound conclusions derivable in their absence.

3.1 Side conditions

To include the side conditions, we first replace each of the rules F2, F7, and R2 by two equivalent rules, as follows:

$$\text{F2}' \quad \frac{P \models \sharp(X),\ P \ni K}{P \models \sharp(\{X\}_K)}$$

$$\text{F2}'' \quad \frac{P \models \sharp(X),\ P \ni K}{P \models \sharp(\{X\}_K^{-1})}$$

$$\text{F7}' \quad \frac{P \models \phi(X),\ P \models \sharp(K),\ P \ni K}{P \models \sharp(\{X\}_K)}$$

$$\text{F7}'' \quad \frac{P \models \phi(X),\ P \models \sharp(K),\ P \ni K}{P \models \sharp(\{X\}_K^{-1})}$$

$$\text{R2}' \quad \frac{P \models \phi(X),\ P \ni K}{P \models \phi(\{X\}_K)}$$

[1] For public-key schemes in which $\{\{X\}_{-K}\}_{+K} = X$ (e.g. RSA [10]).

R2″ $\dfrac{P \models\equiv \phi(X),\ P \ni K}{P \models\equiv \phi(\{X\}_K^{-1})}$

We now propose a side condition $X \neq \{Y\}_K$ to the rule F2″. The rationale behind this side condition is as follows. Let us assume that the statements $P \models\equiv \sharp(\{Y\}_K)$ and $P \ni K$ hold. In the absence of the side condition, we can apply F2″ to obtain the conclusion $P \models\equiv \sharp(Y)$. Now, the only way we could have established $P \models\equiv \sharp(\{Y\}_K)$ is by a prior application of either of the rules F2′ or F7′:

F2′ $\dfrac{P \models\equiv \sharp(Y),\ P \ni K}{P \models\equiv \sharp(\{Y\}_K)}$

F7′ $\dfrac{P \models\equiv \phi(Y),\ P \models\equiv \sharp(K),\ P \ni K}{P \models\equiv \sharp(\{Y\}_K)}$

If F2′ was applied, then $P \models\equiv \sharp(Y)$ must already hold. Hence concluding it later through F2″ is of no use. On the other hand, if F7′ was applied then $P \models\equiv \phi(Y)$ and $P \models\equiv \sharp(K)$ must hold. In this case, the statement $P \models\equiv \sharp(Y)$ may or may not hold. Again, if $P \models\equiv \sharp(Y)$ holds then concluding it through F2″ is of no use. However, if $P \models\equiv \sharp(Y)$ did not hold then concluding so through F2″ is disastrous. Hence, by including the side condition, we have only omitted the possibility of an unsound conclusion, without losing any useful derivations.

We can also argue for similar side conditions to each of the rules F3[2], F4, F7″, F8[2], F9, R2″, R3, and R4. We list below these rules along with the proposed side conditions.

F2″ $\dfrac{P \models\equiv \sharp(X),\ P \ni K}{P \models\equiv \sharp(\{X\}_K^{-1})},\ X \neq \{Y\}_K$

F3 $\dfrac{P \models\equiv \sharp(X),\ P \ni +K}{P \models\equiv \sharp(\{X\}_{+K})},\ X \neq \{Y\}_{-K}$

F4 $\dfrac{P \models\equiv \sharp(X),\ P \ni -K}{P \models\equiv \sharp(\{X\}_{-K})},\ X \neq \{Y\}_{+K}$

F7″ $\dfrac{P \models\equiv \phi(X),\ P \models\equiv \sharp(K),\ P \ni K}{P \models\equiv \sharp(\{X\}_K^{-1})},\ X \neq \{Y\}_K$

F8 $\dfrac{P \models\equiv \phi(X),\ P \models\equiv \sharp(+K),\ P \ni +K}{P \models\equiv \sharp(\{X\}_{+K})},\ X \neq \{Y\}_{-K}$

F9 $\dfrac{P \models\equiv \phi(X),\ P \models\equiv \sharp(-K),\ P \ni -K}{P \models\equiv \sharp(\{X\}_{-K})},\ X \neq \{Y\}_{+K}$

R2″ $\dfrac{P \models\equiv \phi(X),\ P \ni K}{P \models\equiv \phi(\{X\}_K^{-1})},\ X \neq \{Y\}_K$

R3 $\dfrac{P \models\equiv \phi(X),\ P \ni +K}{P \models\equiv \phi(\{X\}_{+K})},\ X \neq \{Y\}_{-K}$

[2]For public-key schemes in which $\{\{X\}_{-K}\}_{+K} = X$ (e.g. RSA [10]).

R4 $\dfrac{P \mid\equiv \phi(X),\ P \ni -K}{P \mid\equiv \phi(\{X\}_{-K})},\ X \neq \{Y\}_{+K}$

Similarly the rules F2′, F7′, and R2′ would also require the side condition $X \neq \{Y\}_K^{-1}$ for conventional cryptosystems in which $\{\{X\}_K^{-1}\}_K = X$ (e.g. DES [11]).

It is obvious that with the side conditions to the above freshness and recognizability rules, the senseless conclusions which can otherwise be drawn from these rules are avoided.

4 Incompleteness of the set of rules

In this section we give an example of a rule which is missing from the set of rules given in [2]. This rule is needed to verify the Yahalom protocol, which was apparently within the scope of the GNY logic [2, p. 243]. Although it has been suggested that in such logics, because of the variety of cryptographic techniques possible, rules may be added when needed [7, p. 18], an independently motivated formal semantics is essential to verify the correctness of the added rules.

The message interpretation rules of the GNY logic enable principals to obtain beliefs about other principals beliefs and possessions. Below we analyze the Yahalom protocol by using the logic. The analysis shows that the logic lacks a message interpretation rule to reason about the use of a shared secret in this protocol. In the analysis given below, we adopt the protocol parsing scheme given by Gong in [7], instead of the one proposed in [2]. First, we clarify our reasons for doing this.

4.1 Protocol parsing

The first step, in analyzing a protocol described in the conventional notation, is to generate a form suitable for manipulation in the logic. In the GNY logic, this task is performed by a protocol parser which inserts explicit information inside protocol message parts, to distinguish whether the recipient of a message conveyed it earlier in the current run of the protocol or not. In the parser output, the presence of a '$*$' before a formula X told to a principal P means that P did not send X in an earlier message in the current run of the protocol.

The only message interpretation rules with a star prefixed to a told formula in a premise are I1, I2, and I3. In each of these rules, the '$*$' (not-originated-here marker) is either prefixed to an encrypted formula (I1, I2) or a hashed formula (I3). This suggests that during protocol parsing, it suffices to consider only encrypted, or hashed, formulas for insertion of the not-originated-here marker, thus simplifying the parsing process. On the other hand, if we choose to consider each complete formula appearing in a line of a protocol description for prefixing with a '$*$', as in [2], then it may not be possible to apply the message interpretation rules to told formulas, as intended by GNY in [2]. For example, in order to apply I3 to the second message of the voting protocol in [2, subsection 5.4], the statement $Q \mid\equiv Q \overset{*S_i}{\leftrightarrow} P_i$ must hold. Presumably, we can obtain this statement from the initial assumption $Q \mid\equiv Q \overset{S_i}{\leftrightarrow} P_i$, but there is nothing in the logic which would enable us to do so. We note that such a problem would not arise if we adopt the modified parsing scheme given in [7].

4.2 Analyzing the Yahalom Protocol

The celebrated Yahalom protocol was first published, and analyzed, in [1]. The goal of the protocol is to distribute an authenticated session key to two principals A and B via a trusted

third party known as the authentication server S. The protocol [1, p. 30] is as follows:

1. $A \rightarrow B : A, N_a$
2. $B \rightarrow S : B, \{A, N_a, N_b\}_{K_{bs}}$
3. $S \rightarrow A : \{B, K_{ab}, N_a, N_b\}_{K_{as}}, \{A, K_{ab}\}_{K_{bs}}$
4. $A \rightarrow B : \{A, K_{ab}\}_{K_{bs}}, \{N_b\}_{K_{ab}}$

The protocol requires the use of an *uncertified key* [3], and as pointed out in [1] "the unusual sequence of messages results in strong guarantees for both A and B with few messages".

We refer to the protocol initiator A as 'Alice' and the other principal B as 'Bob', following standard practice. Initially, Alice and Bob share keys K_{as} and K_{bs} with the authentication server S respectively. Alice initiates the protocol by sending her identity and a nonce[4] N_a to Bob. In the second message, Bob sends to the server his own name and an encrypted part $\{A, N_a, N_b\}_{K_{bs}}$, where N_b is Bob's nonce. In the third message, the server sends to Alice: $\{B, K_{ab}, N_a, N_b\}_{K_{as}}$, $\{A, K_{ab}\}_{K_{bs}}$. The first encrypted part tells Alice that K_{ab} is a good session key for communicating with Bob, and also tells her Bob's nonce. The second encrypted part is intended for Bob. In the fourth message, Alice sends to Bob this encrypted part, along with Bob's nonce encrypted with K_{ab}. Bob decrypts the first encrypted part of this message to get K_{ab}, and uses it to decrypt the second encrypted part. If the latter decryption yields his nonce N_b, then he obtains assurance that K_{ab} is a good session key for communicating with Alice.

The parser produces the following description of the protocol.

1. $B \triangleleft A, N_a$
2. $S \triangleleft B, *\{A, N_a, N_b\}_{K_{bs}}$
3. $A \triangleleft *\{B, K_{ab}, N_a, N_b\}_{K_{as}} \rightsquigarrow S \mid\equiv A \overset{K_{ab}}{\leftrightarrow} B,\ *\{A, K_{ab}\}_{K_{bs}} \rightsquigarrow S \mid\equiv A \overset{K_{ab}}{\leftrightarrow} B$
4. $B \triangleleft *\{A, K_{ab}\}_{K_{bs}} \rightsquigarrow S \mid\equiv A \overset{K_{ab}}{\leftrightarrow} B,\ *\{N_b\} \rightsquigarrow A \mid\equiv A \overset{K_{ab}}{\leftrightarrow} B$

In the parser output, shown above, we have added extensions which describe the beliefs held when the messages are sent. We begin the analysis by listing the initial assumptions:

$A \ni K_{as};\ A \mid\equiv A \overset{K_{as}}{\leftrightarrow} S;\ A \ni N_a;\ A \mid\equiv \sharp(N_a);\ A \mid\equiv \phi(B)$

$B \ni K_{bs};\ B \mid\equiv B \overset{K_{bs}}{\leftrightarrow} S;\ B \ni N_b;\ B \mid\equiv \sharp(N_b);\ B \mid\equiv \phi(N_b);\ B \mid\equiv A \overset{N_b}{\leftrightarrow} B$

$S \ni K_{as};\ S \mid\equiv A \overset{K_{as}}{\leftrightarrow} S;\ S \ni K_{bs};\ S \mid\equiv B \overset{K_{bs}}{\leftrightarrow} S;\ S \ni K_{ab};\ S \mid\equiv A \overset{K_{ab}}{\leftrightarrow} B$

That is, both Alice and Bob possess secret keys for communicating with S. Each possesses a nonce and believes that it is fresh. In addition, Alice believes that the identifier B is recognizable to her, and Bob believes that N_b is recognizable to him. Also, Bob believes that his nonce is a secret shared with Alice. The server possesses secret keys to communicate with Alice and Bob. It also possesses a session key intended for Alice and Bob.

$A \mid\equiv S \mid\Rightarrow S \mid\equiv *;\ A \mid\equiv S \mid\Rightarrow A \overset{K}{\leftrightarrow} B$

$B \mid\equiv S \mid\Rightarrow S \mid\equiv *;\ B \mid\equiv S \mid\Rightarrow A \overset{K}{\leftrightarrow} B;\ B \mid\equiv A \mid\Rightarrow A \mid\equiv *$

Both Alice and Bob believe that the server S is honest. They also trust S to invent a suitable secret key for them. Also, Bob believes that Alice is honest.

[3] A key which is used before its goodness is established [1].

[4] A fresh quantity which has never been used before for its intended purpose [12].

For a run of the protocol, we apply the inference rules to the messages, as follows:

Message 1: Applying P1 we obtain $B \ni (A, N_a)$.

Message 2: Applying T2, and P1 we obtain $S \ni B$.

Applying T2, T1, T3, and P1 we obtain $S \ni (A, N_a, N_b)$.

Message 3: The extension $S \models\equiv A \overset{K_{ab}}{\leftrightarrow} B$ attached to the two encrypted parts is valid because it holds as an assumption. Applying T1, T3, T2, and P1 to the first encrypted part, we obtain $A \ni K_{ab}$ and $A \ni N_b$.

Applying F1, R1, I1, J2, and J3 we obtain $A \models\equiv S \models\equiv A \overset{K_{ab}}{\leftrightarrow} B$.

By further applying J1 we obtain the belief $A \models\equiv A \overset{K_{ab}}{\leftrightarrow} B$. This enables us to include this belief as an extension to the second encrypted part in message 4.

Message 4: By applying T1, T3, T2, and P1 to the first encrypted part we obtain $B \ni K_{ab}$. However, Bob cannot derive any beliefs from this part because he cannot ascertain its timeliness. The protocol leads him to deduce that K_{ab} is good for communicating with Alice if the decryption of the second encrypted part yields his nonce. The only way we can proceed in the logic to reason in this manner is by first establishing that Bob believes the extension attached to the second encrypted part.

However, none of the postulates enable any such beliefs to be derived. The only relevant rule is I1 which cannot be applied, since it requires the recipient of an encrypted message to believe that the key used to encrypt the message is good prior to applying the rule. The logic therefore lacks a rule to reason about the use of a shared secret in the protocol.

4.2.1 Adding a new rule

The blocked derivation of Bob's belief about K_{ab}, in the above protocol, motivates us to propose the addition of the following new rule to the logic:

$$\text{I8} \quad \frac{P \triangleleft *\{X, < S >\}_K,\ P \ni K,\ P \models\equiv P \overset{S}{\leftrightarrow} Q,\ P \models\equiv \phi(X, S),\ P \models\equiv \sharp(X, S, K)}{P \models\equiv Q \mid\sim (X, < S >),\ P \models\equiv Q \mid\sim \{X, < S >\}_K,\ P \models\equiv Q \ni K}$$

Suppose that for principal P all of the following conditions hold: (1) P receives a formula consisting of X concatenated with S, encrypted with key K and marked with a not-originated here mark; (2) P possesses K; (3) P believes S is a suitable secret for himself and Q; (4) P believes that X concatenated with S is recognizable; (5) P believes that at least one of S, X, or K is fresh. Then P is entitled to believe that: (1) Q once conveyed the formula X concatenated with S; (2) Q once conveyed the formula X concatenated with S and encrypted with K; (3) Q possesses K.

A similar rule is needed for "never-originated-here" messages. The new rule I8 enables us to proceed with the derivation of Bob's beliefs in the goodness of K_{ab}, as follows:

Message 4: By applying I8 to the second encrypted part we obtain $B \models\equiv A \ni K_{ab}$, and $B \models\equiv A \mid\sim \{N_b\}_{K_{ab}} \rightsquigarrow A \models\equiv A \overset{K_{ab}}{\leftrightarrow} B$. By further applying J2, and J3 we obtain $B \models\equiv A \models\equiv A \overset{K_{ab}}{\leftrightarrow} B$. We can also attach the belief $A \models\equiv S \models\equiv A \overset{K_{ab}}{\leftrightarrow} B$ as an extension to the second encrypted part, since A derived this belief from message 3. We also need an additional assumption:

$B \mid\equiv A \mid\Rightarrow (S \mid\equiv A \overset{K_{ab}}{\leftrightarrow} B)$, which reflects Bob's trust in Alice to pass on the session key from the server. By applying I8, J2, J3, and J1 we finally obtain $B \mid\equiv A \overset{K_{ab}}{\leftrightarrow} B$.

To conclude our analysis of this protocol, we list the final position attained:

$A \ni K_{ab}$; $A \mid\equiv A \overset{K_{ab}}{\leftrightarrow} B$

$B \ni K_{ab}$; $B \mid\equiv A \overset{K_{ab}}{\leftrightarrow} B$; $B \mid\equiv A \ni K_{ab}$
$B \mid\equiv A \mid\equiv A \overset{K_{ab}}{\leftrightarrow} B$

Both Alice and Bob possess the session key and believe that it is good for communicating with the other. In addition, Bob believes that Alice possesses the session key and believes it to be good for communicating with Bob.

4.2.2 Protocol redundancy

In the analysis given above, we see that Bob does not derive any beliefs about K_{ab} from the encrypted part generated by the server for him, which Alice forwards in message 4. Since he decrypts this encrypted part only to gain possession of K_{ab}, the server need not include Alice's name in it:

$$3'. \quad S \rightarrow A : \{B, K_{ab}, N_a, N_b\}_{K_{as}}, \{K_{ab}\}_{K_{bs}}$$
$$4'. \quad A \rightarrow B : \{K_{ab}\}_{K_{bs}}, \{N_b\}_{K_{ab}}$$

Note that Bob binds the identity claimed by Alice to his nonce, by concatenating them and encrypting with K_{bs} in message 2. Hence, in the last message of the protocol, his nonce not only assures him about the timeliness of the encrypted half sent by Alice, but also guarantees that K_{ab} is meant to be used by him for communicating with Alice. The same final position given before is attained after the above modification to the original protocol.

5 Redundant premises

The message interpretation rule I2 is:

$$\text{I2}\ \frac{P \triangleleft *\{X, < S >\}_{+K},\ P \ni (-K, S),\ P \mid\equiv \overset{+K}{\mapsto} P,\ P \mid\equiv P \overset{S}{\leftrightarrow} Q,\ P \mid\equiv \phi(X, S),\ P \mid\equiv \sharp(X, S, +K)}{P \mid\equiv Q \mid\sim (X, < S >),\ P \mid\equiv Q \mid\sim \{X, < S >\}_{+K},\ P \mid\equiv Q \ni +K}$$

It is obvious that it is unnecessary to include the secret S in the second premise of this rule. Since P is told a message containing S encrypted with his public key (first premise), and he possesses the corresponding private key (second premise), it follows that he possesses S by decrypting this message:

$$\text{T1}\ \frac{P \triangleleft *\{X, < S >\}_{+K}}{P \triangleleft \{X, < S >\}_{+K}}$$

$$\text{T4}\ \frac{P \triangleleft \{X, < S >\}_{+K},\ P \ni -K}{P \triangleleft (X, S)}$$

$$\text{T2}\ \frac{P \triangleleft (X, S)}{P \triangleleft S}$$

$$\text{P1}\ \frac{P \triangleleft S}{P \ni S}$$

The second premise of the message interpretation rule I2$'$ exhibits a similar redundancy.

6 Conclusions

We have pointed out a number of problems with the GNY logic, and suggested possible solutions for them. These solutions are intuitively plausible, but a sound basis for such solutions ultimately requires an independently motivated formal semantics for the logic. We have extended the logic to analyze the Yahalom protocol, and we discovered a redundancy in the protocol.

References

[1] M. Burrows, M. Abadi, and R. Needham, "A Logic of Authentication," Tech. Rep. 39, Systems Research Center, Digital Equipment Corporation, Palo Alto, California, Feb. 1990.

[2] L. Gong, R. Needham, and R. Yahalom, "Reasoning about Belief in Cryptographic Protocols," in *Proc. IEEE Symposium on Security and Privacy*, (Los Alamitos, California), pp. 234–248, IEEE Computer Society Press, 1990.

[3] L. Gong, "Handling Infeasible Specifications of Cryptographic Protocols," in *Proc. of IEEE Symposium on Security and Privacy*, (Los Alamitos, California), pp. 99–102, IEEE Computer Society Press, 1991.

[4] P. F. Syverson, "The Use of Logic in the Analysis of Cryptographic Protocols," in *Proc. IEEE Symposium on Security and Privacy*, pp. 156–170, June 1991.

[5] P. F. Syverson, "The Value of Semantics for the Analysis of Cryptographic Protocols," in *Proc. Computer Security Foundations Workshop IV*, (Los Alamitos, California), pp. 228–229, IEEE Computer Society Press, 1991.

[6] M. R. Tuttle, "Flaming in Franconia: Build Models, not logics." Note on the panel discussion on the Use of Formal Methods in the Analysis of Cryptographic Protocols, Computer Security Foundations Workshop V, June 1992.

[7] L. Gong, *Cryptographic Protocols for Distributed Systems*. PhD thesis, Cambridge University, U.K., 1990.

[8] R. J. Anderson, "UEPS - A Second Generation Electronic Wallet," in *Computer Security - ESORICS 92* (Y. Deswarte, G. Eizenberg, and J.-J. Quisquater, eds.), pp. 411–418, Springer-Verlag, 1992.

[9] P. F. Syverson and P. C. van Oorschot, "On Unifying Some Cryptographic Protocol Logics," in *Proc. IEEE Symposium on Security and Privacy*, may 1994.

[10] R. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-key Cryptosystems," *Communications of the ACM*, vol. 21, pp. 120–126, Feb. 1978.

[11] "National Bureau of Standards. Data Encryption Standard." Federal Information Processing Standards, Pub. 46, Washington, D.C., Jan. 1977.

[12] R. M. Needham and M. D. Schroeder, "Using Encryption for Authentication in Large Networks of Computers," *Communications of the ACM*, vol. 21, pp. 993–999, Dec. 1978.

A GNY logic rules

A.1 Rationality rule

If $\frac{\mathrm{C}_1}{\mathrm{C}_2}$ is a rule, then for any principal P, so is $\frac{\mathrm{P} \mid\equiv \mathrm{C}_1}{\mathrm{P} \mid\equiv \mathrm{C}_2}$.

A.2 Being-Told Rules

T1 $$\frac{P \triangleleft *X}{P \triangleleft X}$$

T2 $$\frac{P \triangleleft (X, Y)}{P \triangleleft X}$$

T3 $$\frac{P \triangleleft \{X\}_K,\ P \ni K}{P \triangleleft X}$$

T4 $$\frac{P \triangleleft \{X\}_{+K},\ P \ni -K}{P \triangleleft X}$$

T5 $$\frac{P \triangleleft F(X, Y),\ P \ni X}{P \triangleleft Y}$$

T6 $$\frac{P \triangleleft \{X\}_{-K},\ P \ni +K}{P \triangleleft X}$$

A.3 Possession Rules

P1 $$\frac{P \triangleleft X}{P \ni X}$$

P2 $$\frac{P \ni X,\ P \ni Y}{P \ni (X, Y),\ P \ni F(X, Y)}$$

P3 $$\frac{P \ni (X, Y)}{P \ni X}$$

P4 $$\frac{P \ni X}{P \ni H(X)}$$

P5 $$\frac{P \ni F(X, Y),\ P \ni X}{P \ni Y}$$

P6 $$\frac{P \ni K,\ P \ni X}{P \ni \{X\}_K,\ P \ni \{X\}_K^{-1}}$$

P7 $$\frac{P \ni +K,\ P \ni X}{P \ni \{X\}_{+K}}$$

P8 $$\frac{P \ni -K,\ P \ni X}{P \ni \{X\}_{-K}}$$

A.4 Freshness Rules

F1 $$\frac{P \models \sharp(X)}{P \models \sharp(X,Y),\ P \models \sharp(F(X))}$$

F2 $$\frac{P \models \sharp(X),\ P \ni K}{P \models \sharp(\{X\}_K),\ P \models \sharp(\{X\}_K^{-1})}$$

F3 $$\frac{P \models \sharp(X),\ P \ni +K}{P \models \sharp(\{X\}_{+K})}$$

F4 $$\frac{P \models \sharp(X),\ P \ni -K}{P \models \sharp(\{X\}_{-K})}$$

F5 $$\frac{P \models \sharp(+K)}{P \models \sharp(-K)}$$

F6 $$\frac{P \models \sharp(-K)}{P \models \sharp(+K)}$$

F7 $$\frac{P \models \phi(X),\ P \models \sharp(K),\ P \ni K}{P \models \sharp(\{X\}_K),\ P \models \sharp(\{X\}_K^{-1})}$$

F8 $$\frac{P \models \phi(X),\ P \models \sharp(+K),\ P \ni +K}{P \models \sharp(\{X\}_{+K})}$$

F9 $$\frac{P \models \phi(X),\ P \models \sharp(-K),\ P \ni -K}{P \models \sharp(\{X\}_{-K})}$$

F10 $$\frac{P \models \sharp(X),\ P \ni X}{P \models \sharp(H(X))}$$

F11 $$\frac{P \models \sharp(H(X)),\ P \ni H(X)}{P \models \sharp(X)}$$

A.5 Recognizability Rules

R1 $$\frac{P \models \phi(X)}{P \models \phi(X,Y),\ P \models \phi(F(X))}$$

R2 $$\frac{P \models \phi(X),\ P \ni K}{P \models \phi(\{X\}_K),\ P \models \phi(\{X\}_K^{-1})}$$

R3 $$\frac{P \models \phi(X),\ P \ni +K}{P \models \phi(\{X\}_{+K})}$$

R4 $$\frac{P \models \phi(X),\ P \ni -K}{P \models \phi(\{X\}_{-K})}$$

R5 $$\frac{P \models \phi(X),\ P \ni X}{P \models \phi(H(X))}$$

R6 $\dfrac{P \ni H(X)}{P \models \phi(X)}$

A.6 Message Interpretation Rules

I1 $\dfrac{P \triangleleft *\{X\}_K,\ P \ni K,\ P \models P \overset{K}{\leftrightarrow} Q,\ P \models \phi(X),\ P \models \sharp(X,K)}{P \models Q \mid\sim X,\ P \models Q \mid\sim \{X\}_K,\ P \models Q \ni K}$

I2 $\dfrac{P \triangleleft *\{X,<S>\}_{+K},\ P \ni (-K,S),\ P \models \overset{+K}{\mapsto} P,\ P \models P \overset{S}{\leftrightarrow} Q,\ P \models \phi(X,S),\ P \models \sharp(X,S,+K)}{P \models Q \mid\sim (X,<S>),\ P \models Q \mid\sim \{X,<S>\}_{+K},\ P \models Q \ni +K}$

I3 $\dfrac{P \triangleleft *H(X,<S>),\ P \ni (X,S),\ P \models P \overset{S}{\leftrightarrow} Q,\ P \models \sharp(X,S)}{P \models Q \mid\sim (X,<S>),\ P \models Q \mid\sim H(X,<S>)}$

I4 $\dfrac{P \triangleleft \{X\}_{-K},\ P \ni +K,\ P \models \overset{+K}{\mapsto} Q,\ P \models \phi(X)}{P \models Q \mid\sim X,\ P \models Q \mid\sim \{X\}_{-K}}$

I5 $\dfrac{P \triangleleft \{X\}_{-K},\ P \ni +K,\ P \models \overset{+K}{\mapsto} Q,\ P \models \phi(X),\ P \models \sharp(X,+K)}{P \models Q \ni (-K,X)}$

I6 $\dfrac{P \models Q \mid\sim X,\ P \models \sharp(X)}{P \models Q \ni X}$

I7 $\dfrac{P \models Q \mid\sim (X,Y)}{P \models Q \mid\sim X}$

A.7 Jurisdiction Rules

J1 $\dfrac{P \models Q \mid\Rightarrow C,\ P \models Q \models C}{P \models C}$

J2 $\dfrac{P \models Q \mid\Rightarrow Q \models *,\ P \models Q \mid\sim (X \rightsquigarrow C),\ P \models \sharp(X)}{P \models Q \models C}$

J3 $\dfrac{P \models Q \mid\Rightarrow Q \models *,\ P \models Q \models Q \models C}{P \models Q \models C}$

A.8 Never-Originated-Here Messages

I1′ $\dfrac{P \triangleleft \{X\}_K,\ P \ni K,\ P \models P \overset{K}{\leftrightarrow} Q,\ P \models \phi(X),\ P \models \otimes(P)}{P \models Q \mid\sim X,\ P \models Q \mid\sim \{X\}_K}$

I2′ $\dfrac{P \triangleleft \{X,<S>\}_{+K},\ P \ni (S,-K),\ P \models \overset{+K}{\mapsto} P,\ P \models P \overset{S}{\leftrightarrow} Q,\ P \models \phi(X,S),\ P \models \otimes(P)}{P \models Q \mid\sim (X,<S>),\ P \models Q \mid\sim \{X,<S>\}_{+K}}$

I3′ $\dfrac{P \triangleleft H(X,<S>),\ P \ni (X,S),\ P \models P \overset{S}{\leftrightarrow} Q,\ P \models \phi(X,S),\ P \models \otimes(P)}{P \models Q \mid\sim (X,<S>),\ P \models Q \mid\sim H(X,<S>)}$