# THE VERIFIABILITY OF TWO-PARTY PROTOCOLS

Ronald V. Book[1] and Friedrich Otto[2]

[1]Department of Mathematics,
University of California,
Santa Barbara, CA 93106 / USA

[2]Fachbereich Informatik,
Universität Kaiserslautern,
6750 Kaiserslautern / West Germany

Public key encryption as used in network communication has been investigated extensively. The main advantage of the techniques developed in this area is the potential for secure communication. However, while public key systems are often effective in preventing a passive saboteur from deciphering an intercepted message, protocols must be designed to be secure when dealing with saboteurs who can impersonate users or send copies of intercepted messages on the public channel. Dolev and Yao [3] have shown how informal arguments about protocols can lead to erroneous conclusions, and they have developed formal models of two-party protocols, both cascade protocols and name-stamp protocols. Recall that a protocol is a set of rules that specify what operators a pair of users, the sender and the receiver, need to apply in an exchange of messages for the purpose of transmitting a given plaintext message from the sender to the receiver. In terms of their models, Dolev and Yao developed an elegant characterization of cascade protocols that are secure, a characterization with conditions that can be checked by inspection.

The problem that is studied in this paper is that of message authentication in the sense of Diffie and Hellman [2]. How can a user determine whether the messages received are the correct messages that comply with the rules of the protocol used ? The security of a protocol limits the ability to authenticate messages as shown by Dolev and Yao [3]. Our goal is to develop a method for message authentication that allows a user to determine whether the messages he receives actually comply with the protocol and, in this sense, are free of error. This method should be based on properties of the protocol itself, not on

F. Pichler (Ed.): Advances in Cryptology - EUROCRYPT '85, LNCS 219, pp. 254-260, 1986.

the messages exchanged or on the users. Further, the property of security should be retained whenever possible.

We call a protocol sender-verifiable if the sender is able to check whether the reply messages he receives actually comply with the protocol. Thus, if a protocol is sender-verifiable, then the sender can detect whether a saboteur has injected improper messages into the system. Similarly, a protocol is receiver-verifiable if the receiver can check whether the reply messages received comply with the protocol.

The notion of verifiability may also be used as an additional requirement for security. Recall that the power of a potential saboteur (as described by Dolev and Yao [3]) depends on the fact that in an exchange both the sender and the receiver follow the rules of the protocol and apply the specified operators to the messages they receive without checking that the received message itself complies with the protocol. If the user can check whether the messages received comply with the protocol before continuing with the exchange, then he can end the exchange as soon as he detects a message not complying with the protocol, thus restricting the power of a saboteur.

The main results of this paper are simple characterization theorems for two-party protocols that are sender-verifiable (resp., receiver-verifiable). These characterization theorems yield fast algorithms to determine whether a protocol is sender-verifiable or receiver-verifiable.

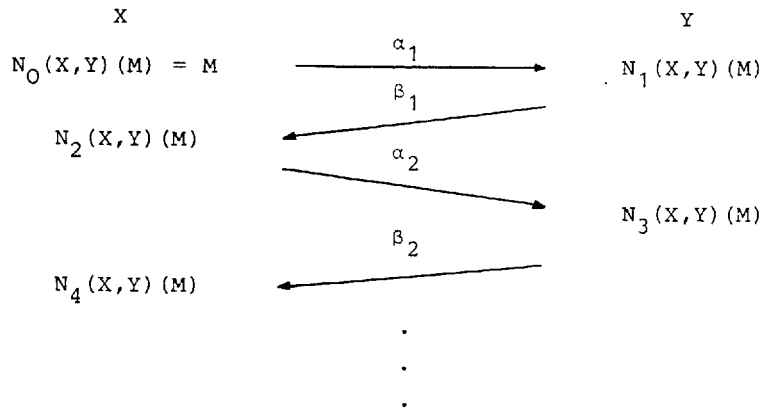
Our notation is based on that of Dolev and Yao [3].

A cascade protocol has a set of cancellation rules $\{D_X E_X = 1, E_X D_X = 1 \mid X \text{ is a user}\}$. For every operator word $\gamma$, let $\bar{\gamma}$ be the result of applying all possible cancellation rules until there is nothing left to cancel; operator words of the latter type are called irreducible. It turns out that for every operator word $\gamma$ there is a unique irreducible word $\bar{\gamma}$ such that for every plaintext message M, $\gamma(M) = \bar{\gamma}(M)$. Further, any two operator words $\gamma_1$ and $\gamma_2$ are considered to be equivalent if for all plaintext messages M, $\gamma_1(M) = \gamma_2(M)$. Hence, $\gamma_1$ and $\gamma_2$ are equivalent if and only if $\bar{\gamma}_1 = \bar{\gamma}_2$.

Let $P = \{\tilde{\alpha}_i, \tilde{\beta}_j \mid 1 \leq i \leq t, 1 \leq j \leq t'\}$ be a two-party cascade protocol where $t' = t$ or $t' = t-1$. For any two distinct users X and Y, let $N_1(X,Y) = \alpha_1(X,Y)$, $N_{2j}(X,Y) = \beta_j(X,Y)N_{2j-1}(X,Y)$, $1 \leq j \leq t'$, and $N_{2i+1}(X,Y) = \alpha_{i+1}(X,Y)N_{2i}(X,Y)$, $1 \leq i \leq t-1$.

If user X initiates an exchange with user Y to transmit plaintext message M, the messages exchanged are $N_1(X,Y)(M), N_2(X,Y)(M), \ldots,$

$N_{t+t'}(X,Y)(M)$. We illustrate this exchange as follows:




The sender X would like to verify that the receiver Y actually receives the correct message at each stage. Also, the receiver Y would like to verify that the sender X receives the correct replies. If both of these things can be done, then the message authentication problem (in the sense of Diffie and Hellman [2]) can be solved. The definition of verifiability is vague. Clearly, some notion of effective process is desired. Therefore, we restrict our attention to the following simpler notions.

A sequence of pairs $(u_j,v_j)$, $1 \leq j \leq t'$, with $u_j$, $v_j \in \{E_X,E_Y,D_X\}^*$ is a sender-verification sequence for P if for each j, $1 \leq j \leq t'$, $\overline{u_j N_{2(j-1)}(X,Y)} = \overline{v_j N_{2j}(X,Y)}$. (Here, $N_0(X,Y)$ is the identity function).

A sequence of pairs $(u_i,v_i)$, $1 \leq i < t$, with $u_i$, $v_i \in \{E_X,E_Y,D_Y\}^*$ is a receiver-verification sequence for P if for each i, $1 \leq i < t$, $\overline{u_i N_{2i-1}(X,Y)} = \overline{v_i N_{2i+1}(X,Y)}$.

The first result can be stated in the following way.

Theorem 1. Let $P = \{\tilde{\alpha}_i,\tilde{\beta}_j\}$ be a two-party cascade protocol.

(a) If P has a sender-verification sequence, then P is sender-verifiable.

(b) If P has a receiver-verification sequence, then P is receiver-verifiable.

Let us sketch a proof of part (a). Consider the situation where user X initiates an exchange with user Y in order to transmit the plaintext message M. For each $j \geq 1$, X wishes to know if the reply message received is the unique reply that complies with the protocol. It is assumed that the sender X always remembers the last message

$N_{2j-2}(X,Y)(M)$ received. When a new reply message M' is received, X tries to determine whether M' is in fact the message $N_{2j}(X,Y)(M)$ that is expected. If the protocol has a sender-verification sequence, then there exist $u_j$ and $v_j$ in $\{D_X,E_X,E_Y\}^*$ such that $\overline{u_jN_{2j-2}(X,Y)} = \overline{v_jN_{2j}(X,Y)}$ and so $u_jN_{2j-2}(X,Y)(M) = v_jN_{2j}(X,Y)(M)$. If the received message is M', then X can apply $v_j$ to M' and compare $v_j(M')$ with $u_jN_{2j-2}(X,Y)(M)$. Now these two bit streams agree if and only if M' is in fact equal to $N_{2j}(X,Y)(M)$, since the equation $\overline{u_jN_{2j-2}(X,Y)} = \overline{v_jw}$ has the unique irreducible solution $w = \overline{N_{2j}(X,Y)}$. Thus, X can determine whether the reply message M' received at this stage of the exchange is in fact the unique reply that complies with the protocol.

Thus, we see that in the case of two-party cascade protocols, the existence of verification sequences allow both sender and receiver to determine whether the reply messages received actually comply with the protocol. Now the question of whether or not such sequences exist depends on the protocol itself, not on the choice of users, and so this concept is uniform in the same sense that Dolev and Yao's definition of the protocol is uniform.

We have characterized those two-party cascade protocols that have sender-verification (resp., receiver-verification) sequences. These characterizations are similar to the characterization of security given by Dolev and Yao in the sense that the conditions involve properties of each $\tilde{\alpha}_i$ and $\tilde{\beta}_j$ that can be checked by inspection. We combine the conditions that characterize security with those that characterize the existence of such sequences.

Theorem 2. Let $P = \{\tilde{\alpha}_i,\tilde{\beta}_j \mid 1 \leq i \leq t,\ 1 \leq j \leq t'\}$ be a two-party cascade protocol. Then the following are equivalent:

(a) P is secure and has both a receiver-verification sequence and a sender-verification sequence;

(b) for any two user names X and Y, the following hold:

(i) $E_X$ or $E_Y$ occurs in the word $\alpha_1(X,Y)$;

(ii) for every $i \geq 2$, $\alpha_i(X,Y) \in \{E_X,E_Y\}^*$ or $\alpha_i(X,Y) = w_1E_Xw_2w_3$ with $w_1, w_3 \in \{E_Y,D_X\}^*$, $w_2 \in \{E_X,E_Y\}^*$, and $w_3^{-1}$ is a prefix of $\beta_{i-1}(X,Y)$;

(iii) for every $j \geq 1$, $\beta_j(X,Y) \in \{E_X,E_Y\}^*$ or $\beta_j(X,Y) = w_1E_Yw_2w_3$ with $w_1, w_3 \in \{E_X,D_Y\}^*$, $w_2 \in \{E_X,E_Y\}^*$, and $w_3^{-1}$ is a prefix of $\alpha_j(X,Y)$.

This development is completely constructive. That is, knowing the existence of a sender-verification sequence for a protocol P allows us to construct such a sequence.

Theorem 3. There is a linear time algorithm that on input a two-party cascade protocol P will halt and output a sender-verification sequence (resp., receiver-verification sequence) for P if such a sequence exists and will halt with output "NO" if such a sequence does not exist.

Now we turn to the study of name-stamp protocols. Let $D = \{D_X \mid X \text{ is a user}\}$ and $E = \{E_X \mid X \text{ is a user}\}$. For each $\gamma \in (D \cup E)^*$, there is a unique irreducible $\gamma^{-1}$ such that $\gamma\gamma^{-1} = \gamma^{-1}\gamma = 1$. In the case of name-stamp protocols, there exist other types of functions, the name-appending, and name-matching functions (see [3]). Let $I = \{i_X \mid X \text{ is a user}\}$, where each $i_X$ is the name-appending function associated with X, and let $J = \{d_X \mid X \text{ is a user}\}$, where each $d_X$ is the name-matching function associated with X. Then every operator word in $(I \cup D \cup E)^*$ has a left inverse and every operator word in $(J \cup D \cup E)^*$ has a right inverse. No nontrivial operator word in $I^*$ has a right inverse and no nontrivial operator word in $J^*$ has a left inverse. These facts lead to certain difficulties when we consider the question of verifiability of name-stamp protocols.

The first problem comes when one tries to extend Theorem 1 to name-stamp protocols. The definition of a verification sequence changes in the sense that for a sender-verification sequence, each $u_j$, $v_j$ is taken from the set $\Gamma_X^*$ where $\Gamma_X = \{D_X, E_X, E_Y, i_X, i_Y, d_X, d_Y\}$, and similarly for a receiver-verification sequence. But more importantly, since there are operator words in $(I \cup J \cup D \cup E)^*$ which do not have left inverses, the argument given in the sketch of the proof of Theorem 1(a) fails since equations of the form $\bar{\gamma} = \overline{\delta w}$ do not necessarily have solutions, let alone unique solutions. In fact, Theorem 1 fails for name-stamp protocols. Therefore we are forced to put an additional constraint on the type of verification sequences used.

We make the following notational convention. If $\gamma \in (D \cup E \cup I \cup J)^*$ has a (two-sided) inverse, then let $\gamma^{-1}$ be the unique irreducible word such that $\gamma\gamma^{-1} = \gamma^{-1}\gamma = 1$. If $\gamma \in (D \cup E \cup I \cup J)^*$ has only a one-sided inverse, either right or left, then let $\gamma^{-1}$ be the unique irreducible word with the appropriate property. Notice that there is no ambiguity introduced.

The following theorem gives a characterization for name-stamp protocols that are sender-verifiable where the verifiability is carried out by a strong sender-verification sequence $\{(u_j, v_j)\}_{j=1}^{t'}$, i.e., each $v_j$ is left-invertible. Thus, this characterization will allow the argument used to prove Theorem 1(a) to carry over to name-stamp protocols.

Theorem 4. Let $P = \{\tilde{\alpha}_i, \tilde{\beta}_j \mid 1 \leq i \leq t, 1 \leq j \leq t'\}$ be a two-party name-stamp protocol, and let X and Y be any two users. Then P has a strong sender-verification sequence $\{(u_j, v_j)\}_{j=1}^{t'}$ if and only if the following conditions hold: for each $j \geq 1$, let $\overline{\beta_j(X,Y)\alpha_j(X,Y)} = w_1w_2$, $\overline{N_{2j-2}(X,Y)} = w_2^{-1}w_3$, and $\overline{N_{2j}(X,Y)} = w_1w_3$ where $w_2$ is right-invertible. Let z be the longest common suffix of $w_1$ and $w_2^{-1}$, let $w_1 = f_1f_2z$ where $f_1 = 1$ or $f_1$ ends in $D_Y$ and $f_2 \in \Gamma_X^*$, and let $w_2^{-1} = g_1g_2z$ where $g_1 \in (D \cup \{E_X\} \cup I)^*$ and $g_2 = 1$ or $g_2$ begins in $E_Y$. Then either
(a) $g_2 = 1$ and $f_1 \in (D \cup \{E_X\})^*$, or
(b) $f_1, f_2 \in (D \cup \{E_X\})^*$ and $g_2 \in (E \cup \{D_X\} \cup I)^*$.

The conditions in Theorem 4 are such that for any name-stamp protocol P one can check in linear time whether P has a strong sender-verification sequence $\{(u_j, v_j)\}_{j=1}^{t'}$. Further, we have the analogue of Theorem 3.

Theorem 5. There is a linear time algorithm that on input a two-party name-stamp protocol P will halt and output a strong sender-verification sequence for P if such a sequence exists and will halt and output "NO" otherwise.

Theorems 4 and 5 are concerned with sender-verifiability. However the notion of receiver-verifiability is essentially isomorphic and the analogous theorems also hold.

The reader may question why we have not stated our characterization theorems in terms of name-stamp protocols that are secure, similar to Theorem 2. Not only is there no known characterization of secure name-stamp protocols of the same type as the characterization of secure cascade protocols given by Dolev and Yao, in fact we have shown that no such characterization can exist [1].

Finally, we consider one other aspect of these models for protocols. The protocols discussed so far can be called symmetric since for every user X, the encryption function composed with the decryption function yields the identity, i.e., $E_XD_X = 1$. By definition of decryption, the decryption function composed with the encryption function yields the identity, i.e., $D_XE_X = 1$. There are valid reasons for considering protocols that are nonsymmetric in the sense that for every user X, $E_XD_X \neq 1$ (while $D_XE_X = 1$). We have developed the entire theory of nonsymmetric protocols in terms of the properties of security and verifiability and have obtained results similar to those reported in this paper.

Acknowledgement

This research was supported in part by the National Science Foundation under Grant DCR83-14977.

References

1. R.V. Book and F. Otto, On the security of name-stamp protocols, Theoret. Comput. Sci. 40 (1985), to appear.
2. W. Diffie and M. Hellman, New directions in cryptography, IEEE Trans. Information Theory IT-22 (1976), 644-654.
3. D. Dolev and A. Yao, On the security of public key protocols, IEEE Trans. Information Theory IT-29 (1983), 198-208. An extended abstract appears in Proc. 22nd IEEE Symp. Foundations of Computer Science (1981), 350-357.