

Formal analysis of robust email protocol based on authentication tests

Jiang Rui Hu Aiqun

(School of Information Science and Engineering, Southeast University, Nanjing 210096, China)

Abstract: Based on the authentication tests and the strand space model, the robust email protocol with perfect forward secrecy is formally analyzed, and the security shortcomings of the protocol is pointed out. Meanwhile, the man-in-the-middle attack to the protocol is given, where the attacker forges the messages in the receiving phase to cheat the two communication parties and makes them share the wrong session keys with him. Therefore, the protocol is not ensured to provide perfect forward secrecy. In order to overcome the above security shortcomings, an advanced email protocol is proposed, where the corresponding signatures in the receiving phase of the protocol are added to overcome the man-in-the-middle attack and ensure to provide perfect forward secrecy. Finally, the proposed advanced email protocol is formally analyzed with the authentication tests and the strand space model, and it is proved to be secure in authentication of the email sender, the recipient and the server. Therefore, the proposed advanced email protocol can really provide perfect forward secrecy.

Key words: email protocol; authentication tests; formal method; perfect forward secrecy; strand space model

Modern email systems have been wildly used instead of traditional communication established by pen and paper. It can transfer not only text but also electronic documents, voice, graphics, and financial transactions through the Internet. Recently, Kim et al. proposed two practical email protocols^[1] providing perfect forward secrecy (PFS), which means that the exposure of a sender's or a recipient's long-term secret keys does not compromise previous session keys. The authors claimed that protocol 1 has the advantage that an encryption or a signature algorithm can be implemented using any public key algorithm, and protocol 2 achieves efficiency and perfect forward secrecy simultaneously.

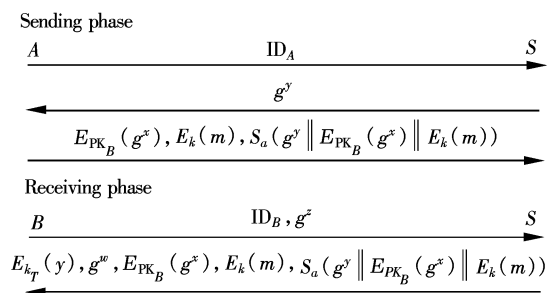
Compared with the schemes of Sun et al.^[2], which cannot really provide PFS shown by Dent^[3], Kim et al. claimed that they improved the second protocol of Sun et al. and made it really provide PFS by establishing an additional temporary short-term key between an email server and a recipient using the Diffie-Hellman key exchange^[4]. However, Yoon and Yoo^[5] pointed out that protocol 2 is vulnerable to two impersonation attacks, where an attacker can easily impersonate a legal sender in order to send a forged message to a recipient, or an attacker can easily impersonate a legal email server in order to obtain all messages sent from senders to recipients. They only gave the informal security analysis on protocol 2 and did not make improvements on it.

In this paper, we first formally analyze email protocol 1 on the basis of authentication tests to disclose the insecurity of the protocol. Secondly, we give our man-in-the-middle attack to it. Thirdly, we propose our advanced protocol with perfect forward secrecy. Finally, we formally analyze our advanced email protocol with the authentication tests^[6-7], which are based on the strand space model^[8], and prove the security on authentication of the email sender, recipient and server in our advanced scheme.

1 Robust Email Protocol 1

The schemes of Kim et al. have two protocols. Protocol 1 is an improved version of the second protocol of Sun et al. and protocol 2 is more efficient than the first one by using a concept of the signcryption of Zheng^[9].

Protocol 1 has two phases, the sending phase and the receiving phase, which can be shown as follows:



where A, B, S are the sender, the recipient and the email server, respectively; ID_X is the identity of X ; PK_X is the public key of X ; SK_X is the secret key of X corresponding to PK_X ; a, b, s are the signing keys of A, B, S , respectively; k is the session key; t, w, x, y, z, z' are the random numbers; p, q are the large prime numbers; m is the message; $S_s(m)$ is the signature with signing key s on a message m ; $E_k(m)$ is the symmetric encryption of a plaintext m using a symmetric key k ; $E_{PK_X}(m)$ is the public encryption of a plaintext m using a public key PK_X ; \parallel represents the concatenation of binary strings.

In the sending phase, when A wants to send an email to B , A sends its identity ID_A to server S . Upon receiving ID_A , S randomly selects y , computes $g^y \bmod p$, and sends it to A . A then randomly chooses x and computes a session key $k = (g^y)^x \bmod p$. A encrypts email contents m with k , $g^x \bmod p$ with PK_B , and signs on $g^y \parallel E_{PK_B}(g^x) \parallel E_k(m)$. Finally, A transmits $E_{PK_B}(g^x)$, $E_k(m)$, and $S_a(g^y \parallel E_{PK_B}(g^x) \parallel E_k(m))$ to S . Having received the email, S verifies the signature to explicitly authenticate A and stores the email.

In the receiving phase, when B wants to receive the email, B first selects a random number z , computes $g^z \bmod p$, and sends it with ID_B to S . Then S chooses a random number w , computes a temporary short-term key $k_T = (g^z)^w \bmod p$,

Received 2008-12-18.

Biography: Jiang Rui (1968—), male, doctor, associate professor, R. Jiang @ seu. edu. cn.

Foundation item: The Natural Science Foundation of Jiangsu Province (No. BK2006108).

Citation: Jiang Rui, Hu Aiqun. Formal analysis of robust email protocol based on authentication tests [J]. Journal of Southeast University (English Edition), 2009, 25(2): 147 – 151.

and encrypts y with k_T . Finally, S sends the email with $E_{k_T}(y)$ and $g^w \bmod p$ back to B . Having received the encrypted email, B verifies the signature $S_a(g^y \| E_{PK_B}(g^x) \| E_k(m))$ and computes $k_T = (g^w)^z \bmod p$, then decrypts $E_{k_T}(y)$ and $E_{PK_B}(g^x)$ to derive a session key k . Finally, B decrypts the email from $E_k(m)$ using $k = (g^x)^y \bmod p$.

2 Formal Analysis of the Robust Email Protocol

2.1 Authentication tests

In this section, we describe the authentication tests in Refs. [6–7] which are based on the strand space theory. The basic ideals of the strand space theory can be referred to Ref. [8].

Fix some strand space Σ . We identify segments of regular strands that amount to tests. Their presence will guarantee the existence of other regular strands in the bundle.

Definition 1 The edge $n_1 \Rightarrow^+ n_2$ is a transformed edge [respectively, a transforming edge] for $a \in A$ if n_1 is positive and n_2 is negative [respectively, n_1 is negative and n_2 is positive], $a \subset \text{term}(n_1)$, and there is a new component t_2 of n_2 such that $a \subset t_2$.

Definition 2 $t = \{ |h| \}_K$ is a test component for a in n if
1) $a \subset t$ and t is a component of n ;
2) The term t is not a proper subterm of a component of any regular node $n' \in \Sigma$.

The edge $n_0 \Rightarrow^+ n_1$ is a test for a if a uniquely originates at n_0 and $n_0 \Rightarrow^+ n_1$ is a transformed edge for a .

Definition 3 The edge $m_0 \Rightarrow^+ m_1$ is an outgoing test for a in $t = \{ |h| \}_K$ if it is a test for a in which $K^{-1} \notin K_P$; a does not occur in any component of m_0 other than t ; and t is a test component for a in m_0 . The edge $m_0 \Rightarrow^+ m_1$ is an incoming test for a in $t_1 = \{ |h| \}_K$ if it is a test for a in which $K \notin K_P$ and t_1 is a test component for a in m_1 .

Outgoing test Let C be a bundle with $m_1 \in C$, and let $m_0 \Rightarrow^+ m_1$ be an outgoing test for a in t .

1) There exist regular nodes $n_0, n_1 \in C$ such that t is a component of n_0 and $n_0 \Rightarrow^+ n_1$ is a transforming edge for a ;
2) Suppose that a occurs only in component $t_1 = \{ |h_1| \}_{K_1}$ of n_1 , that t_1 is not a proper subterm of any regular component, and that $K_1^{-1} \notin K_P$, then there is a negative regular node with t_1 as a component.

The meaning of this assertion is illustrated in Fig. 1. Assume that $\{ |h| \}_K \not\subset \text{term}(n_1)$, a originates uniquely at m_0 , and a is contained only in $\{ |h| \}_K$; then we can conclude that node n_0, n_1 exist in C and are regular, $\{ |h| \}_K \not\subset t_1$, and $m_0 < n_0 < n_1 < m_1$.

Incoming test Let C be a bundle with $m_1 \in C$, and let $m_0 \Rightarrow^+ m_1$ be an incoming test for a in t' . Then there exist

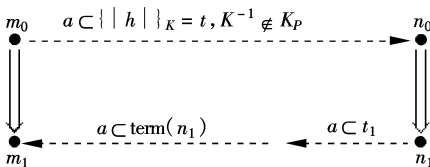


Fig. 1 Outgoing authentication test

regular nodes $n_0, n_1 \in C$ such that t' is a component of n_1 and $n_0 \Rightarrow^+ n_1$ is a transforming edge for a .

The meaning of this assertion is illustrated in Fig. 2. Assume that $\{ |h| \}_K \not\subset \text{term}(m_0)$, a originates uniquely at m_0 ; then we can conclude that node n_0, n_1 exist in C and are regular, and $m_0 < n_0 < n_1 < m_1$.

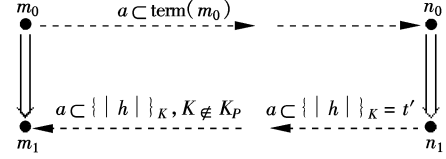


Fig. 2 Incoming authentication test

Definition 4 A negative node m is an unsolicited test for $t = \{ |h| \}_K$ if t is a test component for any a in m and $K \notin K_P$.

Unsolicited test Let C be a bundle with $m \in C$ and let m be an unsolicited test for $t = \{ |h| \}_K$. Then there exists a positive regular node $n \in C$ such that t is a component of n .

Definition 5 (recency) A node n is recent for a regular node m_1 in C if there is a regular node $m_0 \in C$ such that $m_0 \Rightarrow^+ m_1$ and $m_0 \leq_c n <_c m_1$.

The incoming test and outgoing test entail recency. That is, if $m_0 \Rightarrow^+ m_1$ is a test edge, and $n_0 \Rightarrow^+ n_1$ is the corresponding transforming edge in C , then $m_0 < n_0 < n_1 < m_1$, so that n_0 and n_1 are recent for m_1 . By contrast, the unsolicited test establishes nothing about recency.

2.2 Formal analysis

In the formal analysis we consider that the robust email protocol involves three types of regular strands based on the strand space model (see Fig. 3).

1) Sender A strand with traces

$$\langle +\text{ID}_A, -g^y, +\{ |g^x| \}_{PK_B} \{ |m| \}_k \{ |g^y| \}_{PK_B} \{ |m| \}_k \{ |a| \} \rangle$$

where $\text{ID}_A, m, g^y, g^x \in T$; $PK_B, k, a, x, y \in K$. $\text{Send}[\text{ID}_A, m, g^y, g^x, x]$ will denote the set of all the traces shown.

2) Server S strand with traces

$$\begin{aligned} &\langle -\text{ID}_A, +g^y, -\{ |g^x| \}_{PK_B} \{ |m| \}_k \{ |g^y| \}_{PK_B} \{ |m| \}_k \{ |a| \}, \\ &\quad -\text{ID}_B g^z, +\{ |y| \}_{\{ |g^w| \}}, g^w \{ |g^x| \}_{PK_B} \{ |m| \}_k \cdot \\ &\quad \{ |g^y| \}_{PK_B} \{ |m| \}_k \{ |a| \} \rangle \end{aligned}$$

where $\text{ID}_A, \text{ID}_B, m, g^y, g^x, g^z, g^w \in T$; $PK_B, k, a, x, y, z, w \in K$. k_T is formalized as $\{ |g^w| \}_{\{ |g^z| \}}$. $\text{Serv}[\text{ID}_A, \text{ID}_B, m, g^y, g^x, g^z, g^w, y, w]$ will denote the set of all the traces shown.

3) Recipient B strand with traces

$$\begin{aligned} &\langle +\text{ID}_B g^z, -\{ |y| \}_{\{ |g^w| \}}, g^w \{ |g^x| \}_{PK_B} \{ |m| \}_k \cdot \\ &\quad \{ |g^y| \}_{PK_B} \{ |m| \}_k \{ |a| \} \rangle \end{aligned}$$

where $\text{ID}_B, m, g^y, g^x, g^z, g^w \in T$; $PK_B, k, a, z, w, x, y \in K$. k_T is formalized as $\{ |g^w| \}_{\{ |g^z| \}}$. $\text{Recp}[\text{ID}_B, m, g^y, g^x, g^z, g^w, z]$ will denote the set of all the traces shown.

Fix a strand space Σ in which all regular strands are of these forms.

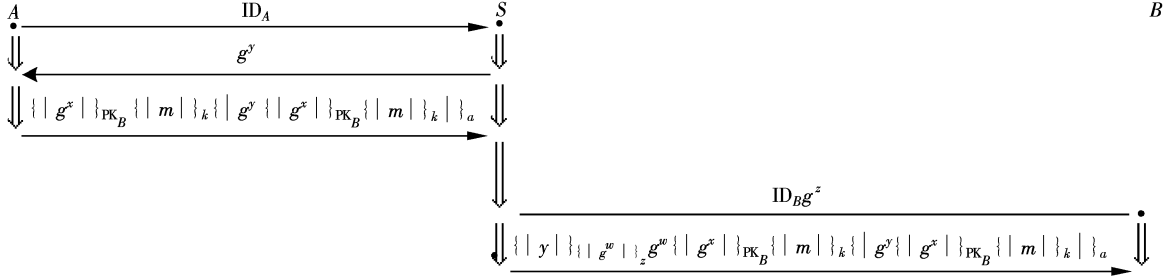


Fig. 3 Message exchange in the robust email protocol

Proposition 1 Let C be a bundle in Σ , and s be a server strand in $\text{Serv}[\text{ID}_A, \text{ID}_B, m, g^y, g^x, g^z, g^w, y, w]$ with C -height 3. Assume PK_B^{-1} , $a \notin K_p$. Suppose that g^y is uniquely originating. Then there is a regular sender strand $s' \in \text{Send}[\text{ID}_A, m, g^y, g^x, x]$ with C -height 3.

Proof First, we show that the nodes $\langle s, 2 \rangle$ and $\langle s, 3 \rangle$ on s form an incoming test for g^y (see Fig. 3). $\{ | g^y | \{ | g^x | \}_{\text{PK}_B} \{ | m | \}_k \}_a$ is a test component for g^y in $\langle s, 2 \rangle$ according to definition 2 because it contains g^y , and no regular node has any term of this form as a proper subterm. Checking the assumption, if $a \notin K_p$, it follows that $\langle s, 2 \rangle \Rightarrow^+ \langle s, 3 \rangle$ is an incoming test for g^y in $\{ | g^y | \{ | g^x | \}_{\text{PK}_B} \{ | m | \}_k \}_a$ according to definition 3.

By the incoming test, there exist regular nodes $n_0, n_1 \in C$ such that $\{ | g^y | \{ | g^x | \}_{\text{PK}_B} \{ | m | \}_k \}_a$ is a component of n_1 and $n_0 \Rightarrow^+ n_1$ is a transforming edge for g^y .

Because n_1 is a positive regular node and $\{ | g^y | \{ | g^x | \}_{\text{PK}_B} \{ | m | \}_k \}_a = \text{term}(n_1)$, g^y is uniquely originating in $\langle s, 2 \rangle$, then there exists a negative regular node n_0 to receive g^y . Since n_0 is a negative node, it is at $\langle s', 2 \rangle$ for some sender strand $s' \in \text{Send}[\text{ID}'_A, m', g'^y, g'^x, x']$. Since $\langle s', 2 \rangle \Rightarrow^+ \langle s', 3 \rangle$ and $\text{term}(\langle s', 3 \rangle) = \{ | g^y | \{ | g^x | \}_{\text{PK}_B} \{ | m | \}_k \}_a$, according to the signing key a

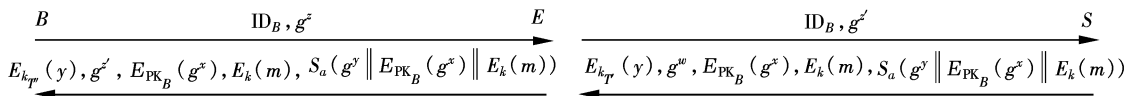
of A , we see $\text{ID}'_A = \text{ID}_A$, $m' = m$, $g^{y'} = g^y$, $g^{x'} = g^x$, $x' = x$. The C -height of s' is 3.

Proposition 1 enables the secure authentication for the sending phase of protocol 1. After the sending phase, the server can authenticate the sender A , and stores the email.

In the receiving phase, the most important for the server is to authenticate the recipient B , then the server can send the stored email to the authenticated recipient. However, protocol 1 uses only one message $\text{ID}_B g^z$ (see Fig. 3) for the server to authenticate the recipient B in the receiving phase. On the basis of authentication tests, the server strand s should have an unsolicited test for ID_B and g^z at node $\langle s, 4 \rangle$ in order to ensure the secure authentication. Unfortunately, the message is only $\text{ID}_B g^z$, therefore according to definition 4 and the unsolicited test, the server strand s has no unsolicited test for user's ID_B and g^z . Therefore, the receiving phase of protocol 1 may be insecure based on authentication test.

In fact, we show that protocol 1 easily suffers from the man-in-the-middle attack and cannot provide perfect forward secrecy. In the sending phase, the adversary E eavesdrops the messages sent between A and S . When the receiving phase begins, he can make the man-in-the-middle attack on the protocol, which is shown as follows:

Receiving phase



The adversary E first intercepts the message ID_B and g^z sent by B to S , selects a random number z' , computes $g^{z'} \bmod p$, then replaces $g^z \bmod p$ with $g^{z'} \bmod p$, and sends the changed message ID_B and $g^{z'}$ to S . Upon receiving the message, S will compute a wrong temporary short-term key $k_T = (g^{z'})^w \bmod p$, and encrypt y with k_T . Finally, S sends the email with $E_{k_T}(y)$ and g^w back to B . The adversary E again intercepts the message sent by S to B , decrypts $E_{k_T}(y)$ to obtain y with the key $k_T = (g^w)^{z'} \bmod p$, then computes $k_T = (g^{z'})^{z'} \bmod p$, encrypts y with k_T , and replaces g^w with $g^{z'}$. Finally, the adversary E sends the email with $E_{k_T}(y)$ and $g^{z'}$ back to B . Having received the encrypted email, B can verify the signature, compute $k_T = (g^{z'})^z \bmod p$, then decrypt $E_{k_T}(y)$ and $E_{\text{PK}_B}(g^x)$ to derive session key k . Finally, B can get the email content m from $E_k(m)$ with the session key $k = (g^x)^y \bmod p$.

When the protocol finishes, everything seems well to both B and S . However, both S and B do not know they

share the wrong temporary short-term keys k_T and $k_{T'}$ with the adversary, respectively. More important, the secret number y is disclosed. Unfortunately, both S and B still think they share the common short-term key with each other. This is the typical man-in-the-middle attack.

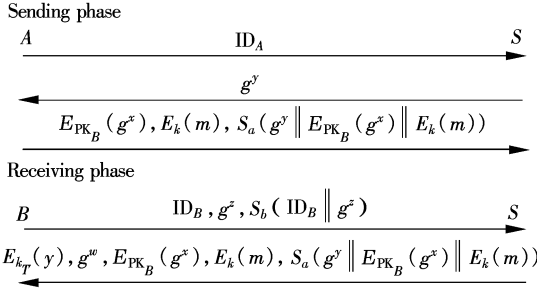
Moreover, when the recipient's long-term secret key is exposed, i. e., SK_B is exposed, the adversary can easily obtain g^x from $E_{\text{PK}_B}(g^x)$, and compute session key $k = (g^x)^y \bmod p$ (because he obtains the secret y early). Thus, the session key k is disclosed. Therefore, protocol 1 cannot provide perfect forward secrecy.

3 Our Advanced Protocol

In this section, we propose our advanced protocol to overcome our attacks and provide perfect forward secrecy.

The reason why the robust email protocol easily suffers from the man-in-the-middle attack is that the server S cannot authenticate the recipient B . The server S cannot distin-

guish whether the message ID_B, g^z is sent by B or the adversary. So, in order to overcome this kind of attack, we propose our advanced protocol 1, which is shown as follows:



Our advanced protocol 1 has two phases, the sending phase and the receiving phase. The sending phase in our advanced protocol 1 is the same as that in the former protocol 1. In the receiving phase, when B wants to receive the email, B should add his signature in the message, that is, B should send $ID_B, g^z, S_b(ID_B \parallel g^z)$ instead of ID_B, g^z to S . Having received this message, S can make sure the message $ID_B, g^z, S_b(ID_B \parallel g^z)$ is sent only by B , according to the verification of the signature $S_b(ID_B \parallel g^z)$, for any adversary

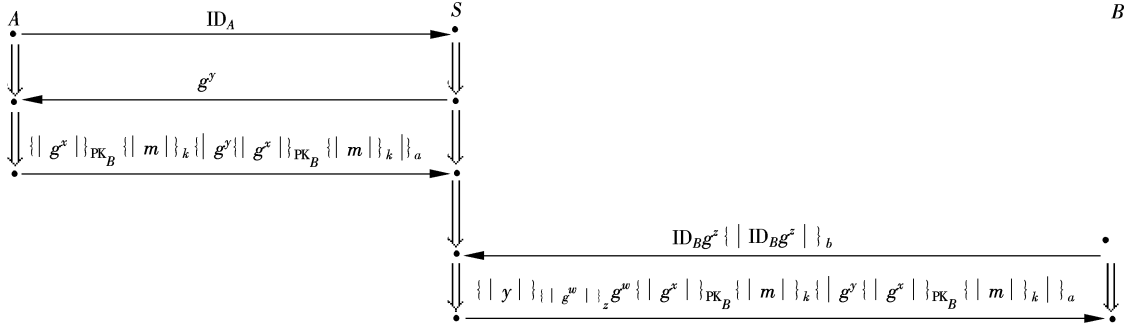


Fig. 4 Message exchange in our advanced protocol

1) Sender A strand with traces

$$\langle +ID_A, -g^y, +\{ \{ g^x \}_{PK_B} \{ m \}_k \mid g^y \{ g^x \}_{PK_B} \{ m \}_k \}_a \rangle$$

where $ID_A, m, g^y, g^x \in T$; $PK_B, k, a, x, y \in K$. $\text{Send}[ID_A, m, g^y, g^x, x]$ will denote the set of all the traces shown.

2) Server S strand with traces

$$\langle -ID_A, +g^y, -\{ \{ g^x \}_{PK_B} \{ m \}_k \mid g^y \{ g^x \}_{PK_B} \{ m \}_k \}_a, \\ -ID_B g^z \{ ID_B g^z \}_b, +\{ \{ y \}_{k_T} \mid g^w \mid g^x \}_{PK_B} \{ m \}_k \mid g^y \{ g^x \}_{PK_B} \{ m \}_k \}_a \rangle$$

where $ID_A, ID_B, m, g^y, g^x, g^z, g^w \in T$; $PK_B, k, a, b, x, y, z, w \in K$. k_T is formalized as $\{ \{ g^w \} \}_z$. $\text{Serv}[ID_A, ID_B, m, g^y, g^x, g^z, g^w, y, w]$ will denote the set of all the traces shown.

3) Recipient B strand with traces

$$\langle +ID_B g^z \{ ID_B g^z \}_b, -\{ \{ y \}_{k_T} \mid g^w \mid g^x \}_{PK_B} \{ m \}_k \mid g^y \{ g^x \}_{PK_B} \{ m \}_k \}_a \rangle$$

where $ID_B, m, g^y, g^x, g^z, g^w \in T$; $PK_B, k, a, b, z, w, x, y \in K$. k_T is formalized as $\{ \{ g^w \} \}_z$. $\text{Recp}[ID_B, m, g^y, g^x, g^z, g^w, z]$ will denote the set of all the traces shown.

cannot forge the correct $S_b(ID_B \parallel g^z)$. S then sends the message $E_{k_T}(y), g^w, E_{PK_B}(g^x), E_k(m), S_a(g^y \parallel E_{PK_B}(g^x) \parallel E_k(m))$ back to B , and finally B obtains the email from $E_k(m)$ using $k = (g^x)^y \bmod p$.

When an adversary wants to replace $g^z \bmod p$ with $g^z \bmod p$ as he does in our attack 1, he cannot calculate the correct $S_b(ID_B \parallel g^z)$, because he does not know the signing key b of the recipient B . Thus, the server S can easily discover the forged message and discard it; therefore, the above man-in-the-middle attack 1 can be avoided, and the secret number y can be protected. So, even if the long-term secret keys SK_A and SK_B are exposed to an adversary, computing $k = (g^x)^y \bmod p$ is infeasible without y under the hardness assumption of the Diffie-Hellman problem. Therefore, our advanced protocol can provide PFS.

4 Formal Analysis of Our Advanced Protocol

In this section, we formally analyze our advanced protocol with authentication tests to prove the secure authentication of the advanced protocol and provide PFS.

In the form we consider, our advanced protocol involves three types of regular strands (see Fig. 4).

Fix a strand space Σ in which all regular strands are of these forms.

The sending phase of our advanced protocol is the same as that of protocol 1; therefore, proposition 1 is also held in our advanced scheme. This means that the sending phase of our advanced protocol is secure, and after the sending phase, the server can authenticate the sender A , and stores the email. Let us focus on the receiving phase.

Proposition 2 Let C be a bundle in Σ , and s be a recipient strand in $\text{Recp}[ID_B, m, g^y, g^x, g^z, g^w, z]$ with C -height 2. Assume $b, z, w, t \notin K_p$. Suppose that ID_B, g^z and g^w are uniquely originating. Then there is a regular server strand $s' \in \text{Serv}[ID_A, ID_B, m, g^y, g^x, g^z, g^w, y, w]$ with C -height 2.

Proof First, we show the node on s' forms an unsolicited test for ID_B and g^z . $\{ ID_B g^z \}_b$ is a test component for ID_B and g^z in $\langle s', 4 \rangle$, because it contains ID_B and g^z , and no regular node has any term of this form as a proper subterm. Checking the assumptions, if $b \notin K_p$, it follows that the negative node on s' is an unsolicited test for ID_B and g^z in $\{ ID_B g^z \}_b$ according to definition 4.

By an unsolicited test, there exists a positive regular node $n \in C$ such that $\{ ID_B g^z \}_b$ is a component of n . Because

n is a positive regular node and $\{ |ID_B g^z| \}_b = \text{term}(n)$, then n is $\langle s, 1 \rangle$ for some regular recipient strand $s \in \text{Recp}[ID'_B, m', g^y, g^x, g^{z'}, g^{w'}, z']$. Because ID_B and g^z are uniquely originating, then $\text{term}(\langle s, 1 \rangle) = ID_B g^z \{ |ID_B g^z| \}_b$; therefore, we see that $ID'_B = ID_B, m' = m, g^{z'} = g^z, g^{w'} = g^w, z' = z$; i. e., there exists the regular recipient node $\langle s, 1 \rangle$.

Secondly, we show that the node on s forms an unsolicited test for g^w . $\{ |y| \}_{\{ |g^w| \}_i}$ is a test component for g^w in $\langle s, 2 \rangle$ because it contains g^w , and no regular node has any term of this form as a proper subterm. Checking the assumptions, if $z, w \notin K_p$, it follows that the negative node on s is an unsolicited test for g^w in $\{ |y| \}_{\{ |g^w| \}_i}$ according to definition 4.

In an unsolicited test, there exists a positive regular node $n \in C$ such that $\{ |y| \}_{\{ |g^w| \}_i}$ is a component of n . Because n is a positive regular node and $\{ |y| \}_{\{ |g^w| \}_i} = \text{term}(n)$, then n is $\langle s', 5 \rangle$ for some regular server strand $s' \in \text{Serv}[ID_A, ID'_B, m', g^y, g^x, g^{z'}, g^{w'}, y, w']$. Because g^w is uniquely originating, then $\text{term}(\langle s', 5 \rangle) = \{ |y| \}_{\{ |g^w| \}_i} g^w \{ |g^x| \}_{\text{PK}_s} \{ |m| \}_k \{ |g^y| \}_{\text{PK}_s} \{ |m| \}_k \{ |a| \}_a$, we see that $ID'_B = ID_B, m' = m, g^{z'} = g^z, g^{w'} = g^w, w' = w$; i. e., there exists the regular server node $\langle s', 5 \rangle$.

Therefore, when there is a recipient strand in $\text{Recp}[ID_B, m, g^y, g^x, g^z, g^w, z]$ with C -height 2, there is a regular server strand $s' \in \text{Serv}[ID_A, ID_B, m, g^y, g^x, g^z, g^w, y, w]$ with C -height 2.

Proposition 2 enables the secure authentication of the receiving phase in our advanced protocol. It also enables our advanced protocol to overcome the man-in-the-middle attack and protect the secret of y . Therefore, our advanced protocol can provide perfect forward secrecy.

5 Conclusion

In this paper, we first introduce the robust email protocol 1 proposed by Kim et al., where the authors claimed protocol 1 has the advantage that an encryption or a signature algorithm can be implemented using any public key algorithm. We then formally analyze the robust email protocol 1

on the basis of authentication tests to disclose its insecurity. Also, we give our man-in-the-middle attack to it, and show that the protocol cannot provide perfect forward secrecy. Later, we propose our advanced protocol to withstand the man-in-the-middle attack, and make it provide perfect forward secrecy. Finally, we formally analyze our advanced email protocol with the authentication tests and the strand space model, and prove the security on authentication of the server, the sender and the recipient in it. Our advanced protocol also preserves the merits of the original protocol, and can provide perfect forward secrecy indeed.

References

- [1] Kim B, Koo J, Lee D. Robust e-mail protocols with perfect forward secrecy [J]. *IEEE Communications Letters*, 2006, **10** (6): 510–512.
- [2] Sun H, Hsieh B, Hwang H. Secure e-mail protocols providing perfect forward secrecy[J]. *IEEE Communications Letters*, 2005, **9**(1): 58–60.
- [3] Dent A W. Flaws in an e-mail protocol of Sun, Hsieh, and Hwang [J]. *IEEE Communications Letters*, 2005, **9**(8): 718–719.
- [4] Diffie W, Hellman M E. New directions in cryptography [J]. *IEEE Transactions on Information Theory*, 1976, **22** (5): 644–654.
- [5] Yoon E J, Yoo K Y. Cryptanalysis of robust e-mail protocols with perfect forward secrecy[J]. *IEEE Communications Letters*, 2007, **11**(5): 372–374.
- [6] Guttman J D, Thayer Fabrega F J. Authentication tests and the structure of bundles [J]. *Theoretical Computer Science*, 2002, **283**(2): 333–380.
- [7] Guttman J D. Security protocol design via authentication tests [C]//*Proceedings of the 15th IEEE Workshop on Computer Security Foundations*. Washington, DC, USA: IEEE Computer Society, 2002: 65–80.
- [8] Thayer Fabrega F J, Herzog J C, Guttman J D. Strand spaces: proving security protocols correct [J]. *Journal of Computer Security*, 1999, **7**(2/3): 191–230.
- [9] Zheng Y. Digital signcryption or how to achieve cost(signature and encryption) [C]//*CRYPTO'97. Lecture Notes in Computer Science*, 1997, **1294**: 165–179.

基于认证测试的鲁棒电子邮件协议形式化分析

蒋 睿 胡爱群

(东南大学信息科学与工程学院, 南京 210096)

摘要: 基于认证测试方法及 strand space 模型, 形式化分析了具有完美前向机密性的鲁棒电子邮件协议, 指出该协议存在安全缺陷. 同时给出了针对该协议的中间人攻击方法, 即攻击者在协议的接收阶段通过伪造消息即可欺骗通信双方, 使通信双方与其共享错误的会话密钥, 由此使得协议的完美前向机密性得不到保证. 针对协议的上述缺陷, 提出一种改进方案, 即通过在协议的接收阶段加入相应的签名信息, 以保证改进协议能够克服中间人攻击并且提供完美前向机密性. 最后, 基于认证测试方法及 strand space 模型, 形式化证明了改进协议在发起者、接收者及服务器之间的安全认证, 确保了改进协议具备真正的完美前向机密性.

关键词: 电子邮件协议; 认证测试; 形式化方法; 完美的前向机密性; strand space 模型

中图分类号: TP393