What are Multi-Protocol Guessing Attacks*  
And  
How to prevent them

Sreekanth MALLADI, Jim Alves-Foss  
Center for Secure and Dependable Systems  
University of Idaho  
Moscow, ID - 83843  
{msskanth,jimaf}@cs.uidaho.edu

Sreenivas MALLADI  
Satyam Computers Private Ltd.  
Hyderabad - 500044, A.P  
India.  
Sreenivas_Malladi@satyam.com

April 1, 2002

Abstract

A guessing attack on a security protocol is an attack where an attacker guesses a poorly chosen secret (usually a low-entropy user password) and then seeks to verify that guess using other information. Past efforts to address guessing attacks in terms of design or analysis considered only protocols executed in isolation. However, security protocols are rarely executed in isolation and reality is always a case of mixed-protocols. In this paper, we introduce new types of attacks called multi-protocol guessing attacks, which can exist when protocols are mixed. We then develop a systematic procedure to analyze protocols subject to guessing attacks. Using this procedure, we will present a method of deriving some syntactic conditions to be followed in order for a protocol to be secure against multi-protocol guessing attacks. Lastly, we use the strand space framework to prove that a protocol will remain secure, given that these conditions are followed, by modeling the conditions within the strand space framework. We illustrate these concepts using the Mellowin and Berritt protocol (EKE) as an example.

1. Introduction

Since people tend to choose poor passwords [17], security protocols using them are vulnerable to guessing attacks [9]. As an example, consider the following simple protocol:

- **Msg 1.** \(a \rightarrow s : a\)
- **Msg 2.** \(s \rightarrow a : n_s\)
- **Msg 3.** \(a \rightarrow s : \{n_s\}_{\text{passwd}(a,s)}\)

Here, user \(a\) aims to authenticate itself to server \(s\). \((n_s)\) is a nonce. \(\{m\}_k\) represents \(m\) encrypted with key \(k\).

Now an attacker observing these communications can mount a guessing attack by guessing the user’s password. For example, if the user is one of the authors of this paper, then he might guess “alwaysalves” as the password. He can then do \(\{n_s\}_{\text{alwaysalves}}\) and compare it with message 3 that he obtained (\(\{n_s\}_{\text{passwd}(a,s)}\)). A successful comparison indicates with high probability that this might be the user’s password.

Past efforts to address guessing attacks in terms of design [9] or analysis [15] focussed only on protocols executing in isolation. However, security protocols are rarely executed in an isolated environment, without interaction from other protocols. Some of the main reasons for “mixed” operation of protocols include:

- deliberate use of sub-protocols such as Kerberos, Neuman-Stubblebine etc. [13, 18], which use those sub-protocols for re-authentication, or
- protocols having different options and hence multiple sub-protocols [5, 12, 16] or
- accidental execution of different protocols on the user’s machine (many times with the same parties, through the same communication channels and having the same message formats and/or keying material).

Together with these, re-using the same keying material (due to the high cost of certified keys), multiple uses of keying formats and keys (due to the widespread use of cryptographic APIs) and using the same password for different applications (which is a commonly observed characteristic of human chosen passwords), make a mixed environment, hostile for protocols.

Hence, the interesting questions to ask are,

- can mixing of two protocols result in new attacks that were not known to exist when either of them executes in isolation?

*This work was funded in part by DARPA under grant no. MDA972-00-1-0001.
What are multi-Protocol Guessing Attacks and How to prevent them
• each of the protocols may be easy to analyze independently. But, how should we analyze them when they are operating in a varying, mixed environment?

• what are the conditions (if there exist any) under which a protocol can operate securely, without fear of being attacked by mixing information from other protocols?

In this paper we introduce new attacks called “multi-protocol guessing attacks” which are guessing attacks that are launched when protocols are mixed. Firstly, we will present a background and motivation, together with some examples of multi-protocol guessing attacks in section 2. Next, we will give an overview of strand space framework and present a systematic procedure to analyse a protocol for guessing attacks (section 3). We will then use this procedure to derive some syntactic conditions under which, a protocol can remain secure against guessing attacks even in a mixed environment. We will model these conditions within the strand space framework and prove that, as long as these conditions are satisfied, a protocol cannot be attacked through multi-protocol guessing attacks (section 4). We sum up with a conclusion and some possible extensions for future work in section 5.

2. Background

In [1, 2, 3] we have presented multi-protocol attacks on security protocols which can exist on interleaved protocols. We have also suggested some techniques that must be adopted for a protocol to remain secure in a mixed environment. Subsequently, Guttman et. al [11] proved a useful result, that protocols are independent if they use disjoint encryption—one of our suggestions earlier to resist multi-protocol attacks. Thus, Guttman et. al virtually buried the threat of multi-protocol attacks.

In this paper, we revive multi-protocol attacks, but this time considering them in the context of guessing attacks (section 2). We will then use this procedure to derive some syntactic conditions under which, a protocol can remain secure against guessing attacks even in a mixed environment. We will model these conditions within the strand space framework and prove that, as long as these conditions are satisfied, a protocol cannot be attacked through multi-protocol guessing attacks (section 4). We sum up with a conclusion and some possible extensions for future work in section 5.

We will illustrate how multi-protocol guessing attacks can be launched the using EKE protocol. Firstly, we make two assumptions about the guessing attacks we consider in this paper:

1. The passwords being guessed have low-entropy (typically, chosen by humans). Contrast this with high-entropy passwords such as machine-generated, where the passwords are chosen from a large space, making guessing infeasible.

2. The verification of a guess does not need repeated on-line interaction with other parties—typically, for repeated unsuccessful attempts, servers raise an alarm and mount additional countermeasures like shutting down the connection etc. In this paper, we consider only those guessing attacks that can be launched entirely off-line, where failed attempts are undetectable.

Now consider the following EKE (Encrypted Key Exchange) protocol presented by Mellovin and Berritt in [4]:

\[
\begin{align*}
\text{Msg 1. } a &\rightarrow b : \{pk_a\} passwd(a, b) \\
\text{Msg 2. } b &\rightarrow a : \{k\} pk_a passwd(a, b) \\
\text{Msg 3. } a &\rightarrow s : \{n_a\}_k \\
\text{Msg 4. } s &\rightarrow a : \{n_a, n_b\}_k \\
\text{Msg 5. } a &\rightarrow s : \{n_b\}_k
\end{align*}
\]

Here, \(a\) and \(b\) try to agree on a shared session key \(k\), with \(passwd(a, b)\) representing the password that \(a\) shares with \(b\) and \(pk_a\), an asymmetric key of \(a\). Lowe [15] analyzed this protocol using FDR [14] and found no attacks.

Now consider another protocol presented in [9]:

\[
\begin{align*}
\text{Msg 1. } a &\rightarrow b : \{c, n\}_k \equiv \{c\} \equiv 1 \\
\text{Msg 2. } b &\rightarrow a : \{f(n)\} passwd(a)
\end{align*}
\]

\(k1\) is \(a\)’s public key, and \(c\) is a “confounder” (a redundant random number) to prevent guessing. \(n\) is any number and \(f\) is a function which is publicly known. This protocol as well was not known to have any flaws when executed in isolation.

It is interesting to ask if \(c\) is really necessary. Without \(c\), a penetrator can guess \(passwd(a)\) and decrypt message 2. He can then do \(f^{-1}(f(n))\) and encrypt the result with \(k1\). A successful comparison with message 1 (without \(c\), just \(\{n\}_k\)) would verify the guess.

Gong et. al [?] suggest that using \(c\) is unnecessary if \(k1\) is unknown—i.e. given that \(k1\) is unknown to the penetrator (as assumed in the EKE protocol above), the protocol is secure.

However, if the protocol is combined with the EKE protocol, i.e. in a mixed environment, the following attack can be visualised:
Attack 1. Let \( P_1 \) represent the first protocol (EKE) and \( P_2 \), the second protocol. A penetrator can initially guess \( \text{passwd}(a) \) in \( P_1 \) and decrypt message 1 to obtain \( pk_a \). He can then guess \( \text{passwd}(a) \) in \( P_2 \) and get \( f(a) \). From this value he can obtain \( n \) and encrypt it with \( pk_a \) that he obtained from \( P_1 \). Finally he can match this value with it’s recorded value in message 1 of \( P_2 \) to verify his guess.

Now consider another identification protocol\(^1\) similar to the one presented in [9]:

\[
\begin{align*}
\text{Msg 1.} & \quad a \rightarrow s : a, s \\
\text{Msg 2.} & \quad b \rightarrow a : n_s \\
\text{Msg 3.} & \quad b \rightarrow a : \{\{a, n_s\}_{pv_a}\}_{\text{passwd}(a)}
\end{align*}
\]

Let this protocol be represented as \( P_3 \). Here user \( a \) aims to identify itself to server \( s (pv_s \) is the private key of \( a \)). This protocol as well is secure, given that the corresponding public key of \( a (pk_a) \) is unknown to the penetrator.

However, when it is mixed with \( P_1 \) due to any of the reasons mentioned in section 1, the following attack can be visualised:

**Attack 2.** The penetrator can initially guess \( \text{passwd}(a, b) \) and decrypt message 1 in \( P_1 \) to obtain \( pk_a \). He can then guess \( \text{passwd}(a) \) and decrypt message 3 in \( P_3 \) to obtain \( \{a, n_s\}_{pv_s} \). Finally he can decrypt \( \{a, n_s\}_{pv_s} \) with \( pk_a \) (from \( P_1 \)) and match \( n_s \) in it with \( n_s \) sent in message 2 to verify his guess.

Similar attacks can be found on many existing protocols. Observe that these attacks were possible even though all the protocols, \( P_1, P_2, P_3 \) were otherwise secure in an isolated environment. Also, none of the attacks assumed that the user used the same passwords in each protocol—Thus, in general, the effect when the same passwords are chosen in different protocols cannot be overstated. Ofcourse, both assumed that users use the same public key in more than one application, which is not unreasonable to assume, given the facts in section 1.

3. Strand Space Frame Work

In this section, we will give an introduction to strand space framework of [6, 7, 8]. We chose strand spaces since it is a particularly suitable framework to derive and demonstrate the results required in these contexts.

To start with, let Fact denote the set of all possible elements in a protocol\(^2\) and Atom, the set of atomic values (eg. \( Alice, Bob, N_A, PubKey(A) \) etc.) assumed to contain in a protocol. When two data items \( a \) and \( b \) are to be concatenated, we will write \( a . b \) or \( (a, b) \). When a data item \( a \) is to be encrypted with a key \( k \), we will write \( \{a\}_k \) and the inverse of \( a \) as \( k^{-1} \).

When we talk about the first or second component in a fact with two components we will use subscripts “1” and “2” as: \( (f_1, f_2) \), \( f_1 \), \( f_2 \).

Also, subfact relation \( \square \) is defined as the smallest relation on facts such that,

\[
f \sqsubseteq f' \iff f \sqsubseteq f' \text{ and } f' \sqsubseteq f \text{ and } f f' \sqsubseteq f f'.
\]

**Definition 1.** A strand is a sequence of communications by any agent in a protocol run, represented as \( \langle \pm f_1, \pm f_2, \ldots, \pm f_n \rangle \). Each node in the set of nodes \( N \), receives (represented as \( - \)) or transmits (represented as \( + \)) a fact \( (fi) \) and belongs to a unique strand.

1. An edge \( \Rightarrow \) is drawn between all consecutive nodes on the same strand.
2. An edge \( \rightarrow \) is drawn between nodes belonging to different strands, if one node transmits a fact and the other node receives the same fact.
3. A strand space \( \Sigma \) is a directed graph with all the nodes in \( N \) as vertices and \( (\Rightarrow \cup \Rightarrow) \) as edges.

A bundle represents a partial or complete history of the network. Let \( C \) be a bundle and \( \Rightarrow (\Rightarrow \cup \Rightarrow) \) be a finite set of edges. Then,

1. If \( n_2 \in N_C \) receives a fact, then there exists a unique \( n_1 \) with \( n_1 \Rightarrow n_2 \).
2. If \( n_2 \in N_C \) with \( n_1 \Rightarrow n_2 \), \( n_1 \Rightarrow n_2 \).
3. \( C \) is acyclic.

A node \( n \) is an entry point to a set of facts \( F \), if there is no node previous to \( n \) transmitting a fact in \( F \). A fact originates on \( n \) if \( n \) is an entry point to all possible facts. A fact is uniquely originating in a bundle if it does not originate on any other node in the bundle.

The penetrator is assumed to possess some message elements, \( M_p \), and keys \( K_p \).

**Definition 2.** A penetrator strand is one of the following:

\[
\begin{align*}
M & \quad \text{Text message } \langle + f \rangle \text{ with } f \in M_p. \\
F & \quad \text{flushing } \langle - f \rangle. \\
T & \quad \text{Tee } \langle - f, + f, + f \rangle. \\
C & \quad \text{Concatenation } \langle - f_1, - f_2, + f_1 f_2 \rangle. \\
S & \quad \text{Separation } \langle - f_1 f_2, + f_1, + f_2 \rangle. \\
K & \quad \text{Key } \langle + k \rangle \text{ with } k \in K_p. \\
E & \quad \text{Encryption } \langle - k, - f, + (f) k \rangle, k \in K_p. \\
D & \quad \text{Decryption } \langle - k^{-1}, - \{f\} k, + f \rangle, k \in K_p.
\end{align*}
\]
A regular strand in contrast, is one corresponding to an honest agent. An ideal captures all possible operations of an honest agent on a given set using a given set of keys. In particular, a smallest k-ideal for an element \( h \in \text{Fact} \) using set of keys \( k \) is denoted as \( I_k[h] \). It consists of all possible operations (concatenation and encryption) between \( h \) and all the elements of \( \text{Fact} \).

Since we deal with mixed protocols, we use the concept of mixed strand spaces as well.

**Definition 3.** A mixed strand space consists of combined strands from different protocols. Some particular strands in this space are called primary strands, implying the primary protocol under consideration and secondary strands, consisting of all the remaining protocols. Set of facts \( I \in \text{Fact} \) is unserved in a strand space \( \Sigma \) if an entry point for \( I \) does not lie on a secondary strand. Similarly \( I \) is strongly unserved in \( \Sigma \) if no element in \( I \) ever originates on a secondary strand.

We will now present our method to analyze protocols for guessing attacks using this framework and illustrate it on an example. The basic idea for the method is derived from [10] where Gutman uses the concept of identifying the unintended services by honest agents to find attack scenarios. The method we give below is such a practical recipe for an informal analysis.

Firstly, we denote \( \simeq \) as a binary relation on facts that returns true if there is a match between two facts and a false otherwise. Also, we define some more sets of facts, classified into:

1. Facts that can be guessed (as set \( G \));
2. Facts that can be derived by the penetrator \( P \) in all possible roles and combinations (as set \( D \));
3. Facts that can be verified (as set \( V \)), e.g. \( \{n_a\}_\text{passwd(a)} \) can be compared with \( \{n_a,n_b\}_\text{passwd(a,b)} \) by guessing \( \text{passwd(a,b)} \) and\(^3\) doing \( n_a \simeq \{n_a,n_b\} \);
4. Facts that can be constructed (as set \( C \))—These are typically those that the penetrator can construct using his knowledge and derived knowledge (\( D \) and facts obtained by guessing, \( O \)).

Firstly, we identify all unintended services offered by honest agents that increase the penetrator knowledge and capability. Then, we will list out the initial penetrator knowledge in terms of facts that he knows and use the unintended services to derive all possible facts that he can derive—For this, we consider all possible roles that a penetrator can play. Then, we will use set \( G \) to enumerate the facts that he can obtain corresponding to decrypting facts using guesses in place of \( G \) (set \( O \)). Finally, we will list out all possible verification attempts using \( V \) to verify a guess and all possible facts that can be constructed using the updated penetrator knowledge, similar to the form of any recorded messages—which again would verify a guess.

Now consider the following “demonstration protocol” presented by Gong et. al [9]:

\[
\begin{align*}
\text{Msg 1.} & \quad a \rightarrow b : \{a,b,na1,na2,ca,\{ta\}_K_a\}_K_s \\
\text{Msg 2.} & \quad s \rightarrow b : a,b \\
\text{Msg 3.} & \quad b \rightarrow s : \{a,b,nb1,nb2,cb,\{tb\}_K_b\}_K_s \\
\text{Msg 4.} & \quad s \rightarrow a : \{na1,na2 \oplus k\}_K_a \\
\text{Msg 5.} & \quad s \rightarrow b : \{nb1,nb2 \oplus k\}_K_b \\
\text{Msg 6.} & \quad a \rightarrow b : \{ra\}_\epsilon \\
\text{Msg 7.} & \quad b \rightarrow a : \{f1(ra),rb\}_k \\
\text{Msg 8.} & \quad a \rightarrow b : \{f2(rb)\}_k
\end{align*}
\]

Lowe [15] analyzed this protocol and found no attacks. To illustrate our method, let us assume that the server cannot detect replays.

Let init, resp and serv denote the regular strands of \( a, b \) and \( s \) in the protocol. We will remove lot of redundant steps in the illustration because of the obvious symmetry visible in the protocol steps—\( a \) and \( b \) have the same message formats in four messages.

**Step 1.** We first identify the unintended services provided by serv. From the protocol it is evident that messages 1 and 3 are “junk”. i.e. any one can replay them spoofing as \( a \) or \( b \) (provided that the server cannot detect those replays which was part of our initial assumptions). Hence, strand serv gives a message \( \{na1,na2 \oplus k\}_\text{passwd(a)} \) each time with a different key for each of such replays.

**Step 2.** The facts that can be guessed (presumably, poorly chosen secrets) in this protocol are: \( \text{passwd(a)} \) and \( \text{passwd(b)} \).

**Step 3.** The facts initially known to \( P \) (\( M_P \cup K_P \)) are: \( a, b, s, K_s, \{a,b,na1,na2,ca,\{ta\}_K_a\}_K_s, \{b,a,nb1,nb2,cb,\{tb\}_K_b\}_K_s, \{na1,na2 \oplus k\}_K_a, \{nb1,nb2 \oplus k\}_K_b, \{ra\}_k, \{f1(ra),rb\}_k, \text{ and } \{f2(rb)\}_k \).

**Step 4.** We will now enumerate all derivable facts (set \( D \)) by considering all possible interactions of \( P: \{a,b\}, (Pa,b), (a,P), (Pa,P). \) (Here \( Pa \) represents \( P \) masquerading as \( a \)). We do not need to consider the remaining possibilities because of the symmetry in the protocol. From combinations (\( a,b \) and \( (Pa,P) \)) and since \( s_{serv} \) gives two instances of \( \{na1,na2 \oplus k\}_K_a \) (from step 1 above on unintended services), \( P \) can now have, \( \{na1,na2 \oplus k\}_K_a \) and \( \{na1,na2 \oplus k\}_K_a \) (with \( k \neq k’ \)).

We leave it to the reader to check the remaining combinations to make sure that no useful terms can be derived.

**Step 5.** We now derive all possible facts obtainable by using elements in set \( G \): These are, \( \{na1,na2 \oplus k\}, \{nb1,nb2 \oplus k\} \). Also, the penetrator can

\(^3\)Recall that subscripts “1” and “2” return the first and second elements respectively from a fact with two elements.
obtain $na2$, since in combination $(a, P)$ of $s_b$ knows $k$ and hence obtains $na$ from $na2 \oplus k$.

Step 6. We now consider the set $V$ (verifiable facts) obtained from the guessing of the protocol. From step 4 using set $D$, $P$ can compare $na1 \{na1, na2 \oplus k\}_{passwd(a)}$ and $\{na1, na2 \oplus k'\}_{passwd(a)}$ and decrypting both. i.e. the guess, he can do, $\{(na1, na2 \oplus k)_{passwd(a)}\}$ and $(\{na1, na2 \oplus k'\}_{passwd(a)})_{g^{-1}}$.

Step 7. We will now show how we uncover ancillary facts on this protocol and the importance of the and cb. We will try to find the facts that $P$ can construct using his knowledge that he obtained from constructing a similar message to verify the guess. Similarly, the case for cb.

4. Mixing EKE

In this section we will use the procedure we developed in the previous section on the EKE protocol, which showed to be vulnerable to multi-protocol guessing attacks in section 2. The analysis would help in deriving rules about some “critical” messages which would be then framed within the strand space model to prove the correctness of EKE protocol in a mixed environment, when the rules are followed.

Figure 1 represents the EKE protocol.

Step 1. The unintended services here are only that of agent b’s. — corresponding to $\{pk\}_{passwd(a,b)}$, b gives, $\{\{k\}_{pk}\}_{passwd(a,b)}$.

Step 2. $G = \{passwd(a,b)\}$.

Step 3. $M_P = \{pk_a\}_{passwd(a,b)}, \{k\}_{pk}\}_{passwd(a,b)}, \{na\}_k, \{na, nb\}_k, \{nb\}_k$.

Step 4. Possible interactions: $(a, b), (a, P), (a, Pb), (P, b), (Pa, b)$. From $(a, P)$, $P$ can obtain $PK_a$. Hence $D = \{PK'_a\}$. (Again we leave it to the reader to check all the remaining combinations to verify that there are no other possible derivations).

Step 5. Facts obtained by guessing: $O = \{PK_a, \{k\}_{PK_a}\}$.


However, from steps 4 and 5, $P$ can do (with guess $g$), $pk'_a = \{pk_a\}_{passwd(a,b)}_{g^{-1}}$.

Step 7. Constructible facts: $C = \emptyset$. Since none of the terms in $M_P \cup D \cup O$ can be used to construct a recorded value for verification.

From the results in the procedure, and in particular, steps 6 and 7, it is evident that, the protocol remains secure as long as,

1. $pk_a$ is never obtainable from a secondary strand (i.e., using any secondary strand $s$, $pk_a \not\in f, \forall f \in D$, obtained from $s$).
2. No term encrypted with $pv_a = pk_a^{-1}$ should be obtainable as well.
3. No term encrypted with $PK_a$ should be verifiable ($\not\in D \cup M_P$).

We will now represent these conditions in a mixed strand space reflecting EKE protocol as a “primary” protocol and all others as secondary protocols.

Definition 4. Let $\Sigma$ be a strand space.

1. $Init[pk_a, passwd(a,b), k, na, nb]$ is the set of strands in $\Sigma$ whose trace is $\langle \{pk_a\}_{passwd(a,b)}, \{k\}_{pk}\}_{passwd(a,b)}, \{na\}_k, \{na, nb\}_k \rangle$.

$\Sigma_{init}$ is the union of the range of $Init$.

2. $Resp[pk, passwd(a,b), k, na, nb]$ is the set of strands in $\Sigma$ whose trace is $\langle \{pk\}_{passwd(a,b)}, \{k\}_{pk}_{passwd(a,b)}, \{na\}_k, \{na, nb\}_k \rangle$.

$\Sigma_{resp}$ is the union of the range of Resp.
Also, $\Sigma_{\text{init}}, \Sigma_{\text{resp}}$ are pairwise disjoint and form the primary strands in $\Sigma$, denoted as $\Sigma_P (= \Sigma_{\text{init}} \cup \Sigma_{\text{resp}})$. Rest of the strands in $\Sigma$ are secondary strands and are represented as $\Sigma \setminus \Sigma_P$ ($\setminus$ is the set difference operator).

The following definition defines the required sets of items that we would need to define the rules that we derived above.

**Definition 5.** Let $L_0$ and $I_D$ be defined such that,

- $L_0$ denotes the set of all terms such that $\forall pk \in PK, \exists f \in M_p \cup D \cup O, pk \sqsubseteq f$.
- $I_D = I_k[D]$ with $k = PV_2 \cup PK_2$

We will now model the conditions we derived using the procedure above, within the strand space framework. Our main theorem states that a mixed protocol environment containing the EKE protocol as the primary protocol is secure against multi-protocol guessing attacks as long as the strand space respects those conditions:

**Theorem 1.** Let $\Sigma$ represent a mixed strand space with the EKE protocol representing the primary strands. Let $C$ be a bundle in $\Sigma$. Then, no guessing attacks can succeed in $C$ if:

1. $PK_a$ is unserved in $\Sigma$.
2. $I_D$ is strongly unserved in $\Sigma$.

**Proof.** We will do a case analysis. Firstly, observe from our procedure that, a guessing attack is feasible if, either verification using set $V$ (step 6) or set $C$ (step 7) is successful. Hence, we will consider those sets and use the above conditions to prove that the sets will always be null under those conditions.

**Part 1.** $PK_a$ is unserved. From step 5, verification of any $g \in G$ is possible, if $(D \cup M_p \cup K_p) \cap O \neq \emptyset$. In this case, from the our analysis, $(D \cup M_p \cup K_p) \cap O = \{pk_a\}$ iff $pk_a = pk_a'$. However, according to condition 1 in the theorem, $PK_a$ is unserved in $\Sigma$. i.e., If $pk_a$ originates in $(\Sigma_{\text{init}} \cup \Sigma_{\text{resp}})$ then $\forall pk_a'$ originating in $\Sigma \setminus \Sigma_P, pk_a \neq pk_a'$. Hence, $(D \cup M_p \cup K_p) \cap O \neq \emptyset$.

**Part 2.** Again observe that, for verification, $pk_a$ should be verifiable since $O = \{pk_a, \{k\}pk_a \}$ and $k \notin (D \cup M_p \cup K_p)$. The procedure demonstrated that, $pk_a$ is not verifiable in $\Sigma_P$.

A verification is still possible, if $f$ encrypted with $pk_a$ or $pk_a^{-1}$ is verifiable and $\in \Sigma \setminus \Sigma_P$. However, in contradiction, condition 2 requires that, $I_D$, (all verifiable terms encrypted with $pk_a$ or $pv_a$ from definition 5), is strongly unserved in $\Sigma$. Or no such term ever originates on a secondary strand as well. Hence, a verification attempt is infeasible as long as the condition holds.

5. **Conclusion**

In this paper we have introduced new types of attacks called multi-protocol guessing attacks, on protocols using weak secrets. We have developed a systematic procedure to derive some conditions that would prevent these attacks. We then proved that—as long as these conditions are satisfied—a protocol can never be attacked through multi-protocol guessing attacks.

Some points are worth mentioning here. Our procedure to analyze protocols is stronger than Gong et. al’s [9] since we consider all obtainable knowledge sets by the penetrator, as Lowe [15] does, whereas Gong et. al consider only fixed penetrator knowledge. The uniqueness in the procedure is that, it allows to pin point the exact kind of vulnerabilities that a protocol might present in terms of especially when operating in a mixed environment. By determining the conditions that prohibit any new vulnerabilities that can possibly arise, a more concrete designing of protocols is possible.

One immediate extension of this work is related to automating the procedure we have used to detect possible guessing attacks. Another possible extension would be to find out techniques of general applicability to prevent multi-protocol guessing attacks, as in [11].

**References**


