2012 International Conference on Future Electrical Power and Energy Systems

An Improvement of Kwon-Song Protocol

Mingshun Yuan\textsuperscript{1,2}, Chenglian Liu\textsuperscript{2*}

\textsuperscript{1}School of Information Science and Technology, Xiamen University, Xiamen 361005, China.
\textsuperscript{2}Department of Mathematics and Computer Science, Fuqing Branch of Fujian Normal University, Fuqing 350300, China

\textsuperscript{1}yzk78@sina.com, \textsuperscript{2}chenglian.liu@gmail.com

Abstract

The Internet has been population, which it was implement information technology, to every enterprise, also changed their contact mode of information flow style. Since public key conception was proposed, it had authentication function to secure while they are communication, and defense the data to leak based on stranger. In this article, we improved the Kwon-Song protocol that it avoids password guessing attack.

© 2012 Published by Elsevier Ltd. Selection and/or peer-review under responsibility of Hainan University.

Keywords: Key agreement and password authentication, Discrete logarithm, Guessing attack

1. Introduction

Kwon and Song proposed a scheme of generalize key agreement and password authentication protocol, based on constraint status; they presented a condensed variant of original protocol with fewer steps in 2000 [3]. Yeh et al. [4] showed that the enhanced version of the generalized key agreement and password authentication protocol while it is insecure against the off-line password guessing attacks. Ku et al. [2] proposed a reflection attack and gave an improvement for original protocol. We improved an enhanced protocol to resist guessing attack. In Section 2, we briefly review and discussion the Kwon-Song protocol. In Section 3, we analyzed Yeh et al. attack method. We gave an improvement for their protocol in section 4. Section 5 is our conclusion.

2. Review of Kwon-Song Scheme

\* Corresponding Author: Mr. Liu is an associate professor with Fuqing Branch of Fujian Normal University.
Email: chenglian.liu@gmail.com ; Tel:+86-13960971195.
2.1 Kwon-Song’s Original Version

In this paper, we denote Client Alice and Server Bob while we call A and B. Alice (A) and Bob (B) are assumed to share the weak passwords in their safety way. It could be shared off-line or by any other secure channel. They agree upon a generator of \( g \) and its group \( \mathbb{Z}_p^* \). Let parameter \( \alpha, x, l \) and \( y \) are selected in \([2, p-2]\) for a uniform distribution, and \( h_1(\cdot), h_2(\cdot), h_3(\cdot), \) with \( h_4(\cdot) \) are kind of random oracles hash function. They communicate to run as following protocol. Alice wants to agree on a secure channel that chooses two random integers \( \alpha, x \) while it had computes and sends the data to Bob (1).

Step 1.

\[
A \rightarrow B : A \parallel g^\alpha \parallel g^{x + h_1(s, g^\alpha)}
\]  

(1)

Bob fetches \( s \) of A from his local secure storage. He also selects two random integer \( l \) and \( y \) gets

\[
K = h_4((g^{x + h_1(s, g^\alpha)})^y \cdot g^{-y h_1(s, g^\alpha)}) = h_4(g^{xy})
\]  

(2)

and computes

\[
g^y g^{al_s}
\]  

(3)

when he sends the plaintext (4) to Alice before.

Step 2.

\[
A \leftarrow B : l \parallel g^y g^{als}
\]  

(4)

Alice is able to compute

\[
K = h_4((g^{y + als})^y \cdot (g^a)^{-als}) = h_4(g^{xy})
\]  

(5)

and gets

\[
h_2(g^a, K)
\]  

(6)

when she sends the message (7) to Bob before.

Step 3.

\[
A \rightarrow B : h_2(g^a, K)
\]  

(7)

Bob authenticates Alice and replies with

\[
h_3(l, K + 1)
\]  

(8)

while he computes \( h_3() \) and \( h_3'(\cdot) \) made by himself if they match each other.

Step 4.

\[
A \leftarrow B : h_3(l, K + 1)
\]  

(9)

Alice gets \( h_3() \) with \( h_3'(\cdot) \) and compares each other, if they also match, then she authenticates Bob. For a result, they are agreement on a new session key in this communication.

2.2 Kwon-Song’s Enhanced Version

In favor of constrained environments, Kwon-Song [3] in addition presents a condensed variant of their original protocol to reduce one step by sharing another generator \( \eta \). The scheme is force Bob to choose \( \eta \), another generator of the same cyclic group also to \( g \).

Note that \( g^a = \eta \mod p \) where \( \gcd(a, p-1) = 1 \) for \( \mathbb{Z}_p^* \) or \( \gcd(a, p) = 1 \) for its \( q \) order subgroup. Bob is also to get \( \eta \) readily by raising \( g \) to \( a \). Also note that there are a number of generators in the group, for example, \( \phi(p-1) \) for \( \mathbb{Z}_p^* \) where \( \phi() \) indicates that Euler totient function. The reduced protocol is summarized as follows:

Reduced 1a. \( A \rightarrow B : \eta^a \parallel g^{x + h_1(s, g^\alpha)} \)
Yeh et al. focus on the enhanced version and pointed out that it suffers from the off-line password guessing attacks. They assume that Eve attempts to impersonate Alice and try to cheat Bob. Eve chooses a guessed password \(s'\) and two random integers \(\alpha\) and \(\gamma\). Then she computes the message \(\eta^\alpha \| g^{\gamma h(s', g^\alpha)}\) and sends it to Bob.

\[\text{Eve} \to B : \eta^\alpha \| g^{\gamma h(s', g^\alpha)}\]  \hfill (13)

\[\text{Eve} \leftarrow B : l \| g^{\gamma \eta^{\alpha l}} \| h_2(\eta^\alpha, K)\]  \hfill (14)

Bob fetches the password \(s\) of A from her secure local storage when he receiving the transmitted message later. He selects two random integers \((l, y)\) who is computes \(g^{\gamma \eta^{\alpha l}}\) and sends the message (14) to Eve when she gets \(K = h_4((g^{\gamma h(s', g^\alpha)})^y \cdot g^{-\gamma h(s, g^\alpha)}))\) after Eve store message (13) and message (14) locally and then executes the offline password guessing attack. Firstly, Eve guesses one password \(s''\) and gets \(R = \eta^{\alpha l}\) since \(\alpha\) is chosen by Eve and \(l\) is a plaintext data. Then, Eve computes \(K' = h_4(R)^{x + h(s', g^\alpha) - h(s, g^\alpha)}\) and computes \(h_2(\eta^\alpha, K)\) with \(h_2(\eta^\alpha, K')\). If they match each other, then Eve guesses right the password. If they do not match, the Eve guess an others password until she hit the nail on the head off-line.

4. Our Improvement

Now, we consider a more general situation in which the weak secret \(s\) could be guessed.

\[\text{Reduced 1a} \quad A \rightarrow B : \eta^{\alpha + s} \| g^{\gamma h(s, g^{\alpha s})}\]  \hfill (15)

\[\text{Reduced 2a} \quad A \leftarrow B : l \| g^{\gamma \eta^{\alpha l}} \| h_2(\eta^{\alpha + s}, K)\]  \hfill (16)

If Eve a passive attack, the information given by the oracle are as follows; \(A, \eta^{\alpha + s}, g^{\gamma h(s, g^{\alpha s})}, l, g^{\gamma \eta^{\alpha l}}, h_2(\eta^{\alpha + s}, K), h_3(l, K + 1)\). If she guessed \(s'\), then she finds \(g^{\gamma'} = (g^x g^{h(s, \eta^{\alpha s})})g^{-h(s', \eta^{\alpha s})}\) and \(g^{\gamma'} = (g^y \eta^{\alpha l})(\eta^\alpha)^{\gamma l}\). But, she has to solve the Diffie-Hellman problem for finding \(K\). This situation is negligible equal to or less than \(1/2^i\) of probability.

**Definition 1. Discrete logarithm problem (DLP)**

Discrete logarithm problem DLP\((p, g, y)\) is a problem that on input a prime \(p\) and integers \(g, y \in \mathbb{Z}_p^*\), outputs \(\alpha \in \mathbb{Z}_{p-1}\) satisfying \(y \equiv g^\alpha \pmod{p}\) if such an \(\alpha\) exists. Otherwise, it outputs \(\bot\).

The above function, which outputs \(\bot\) if there is no solution to the query, should be expressed as DLP and the notation DLP should be used only for a weaker function such that nothing is specified for the behaviour of the function in the case when there is no solution to the query [1]. We say, if Eve try to
guess the exponential $\alpha$, it is very difficult. On the other hand, those $\eta^{a+s}, g^x g^{h(x; g)}$, $g^y \eta^{alh}$ and $l$ reside in the cycle group and the random oracle $h_i(s, \eta^{a+s}), h_2(\eta^{a+s}, K)$, and $h_3(l, K+1)$ are in \{0, 1\}^{l(k)}, there is no way to find the relationship between the rejected password and the remained password.

5. Conclusion

Here we improved a revision of Kwon-Song enhanced scheme. Whatever Bob or Alice, they could identify the impersonator will be failure while apocryphal offensive on session revised 1a and 2a. Our method can resist yet et al.’s impersonate attack.

Acknowledgment

The authors would like to thank the reviewers for their comments that help improve the manuscript. This research is partially supported by the National Natural Science Foundation of China under Grant No. 61103247, and supported by the Department of Education of Fujian Province funding under the type B funding number JB09244. This research was supported in part by the Fuqing Branch of Fujian Normal University of China under the contract number KY2010-030.

References


