Security Weakness in Two Authenticated Key Exchange Protocols

Qingfeng Cheng, Chuangui Ma

Zhengzhou Information Science and Technology Institute
Zhengzhou 450002, P. R. China
qingfengc2008@sina.com

Abstract. In ICA3PP 2009, Xinglan Zhang proposed two one-round authenticated key exchange protocols and proved their security in the standard model. In this paper, we analyze these two protocols and find that both of them exist some flaws.

Key words: Authenticated key exchange, Key compromise impersonation attack, Ephemeral key compromise attack.

1 Introduction

Authenticated key exchange (AKE) protocols enable two party to share common session keys in an authentic way. An AKE protocol is called secure if under the allowed adversarial actions it is infeasible for the attacker to distinguish the value of a key generated by the protocol from an independent random value.

In the following, we describe some security properties.

- **Key compromise impersonation (KCI) resilience**: A party's static private key is disclosed. But the adversary will not enable to masquerade as other legitimate parties to this party.
- **Ephemeral key compromise (EKC) resilience**: The adversary can obtain the ephemeral private key of parties. But the session key under attack still remains secure. It means that the adversary can't compute the session key.
- **Key independence (KI)**: session keys are computationally independent from each other.

KCI resilience and KI are often seen as two desired security attribute for two party authenticated key exchange protocols [1]. Moreover, EKC resilience [2] is also important security attribute. More and more AKE protocols have been rigorously analyzed under EKC attack. Recently, Xinglan Zhang proposed two one-round authenticated key exchange protocols [3] which are claimed to be provably secure based on Decisional Diffie-Hellman problem. For simplicity of description, we refer to the two protocols as the P1 and P2 protocols. In this paper, we will show that they can't resist KCI and EKC attacks. Especially, they also can't provide KI completely.

The rest of this paper is organized as follows. In Section 2, we review both the P1 and the P2 protocols. In Section 3, we show that both of them suffer from KCI attack. Finally, the conclusions will be given in Section 4.

2 Review of the P1 and the P2 protocols

Let k be the security parameter, and G is a group of prime order q. Let $\bigoplus$ denote the operation XOR in the finite field $GF(2)$ and g be a generator of group G. Every party has a public key and a static private key, denoted by pk_i, sk_i, where $pk_i = g^{sk_i}$.

2.1 Description of the P1 protocol

In this subsection, we briefly review the P1 protocol. Since our attacks are mainly related to the key exchange phase, we omit the initiation phase. For more details about the P1 protocol, refer to [3].

In the following description we suppose that two communications parties, A and B wish to communicate with each other.

Step1: Party A chooses $r_A \in \{0,1\}^k$ randomly and computes $\alpha_A = g^{r_A}$, then sends α_A to B.

Step2: Upon receiving the message α_A, party B chooses $r_B \in \{0,1\}^k$ randomly and computes $\alpha_B = g^{r_B}$, then sends α_B to A. and computes the session key: $K_{AB} = pk_A^{sk_B} \bigoplus \alpha_A^{r_B}$.

Step3: Upon receiving the message α_B, party A also computes the session key: $K_{AB} = pk_B^{sk_A} \bigoplus \alpha_B^{r_A}$.

2.2 Description of the P2 protocol

In this subsection, we briefly review the P2 protocol. Since our attacks are mainly related to the key exchange phase, we omit the initiation phase. For more details about the P2 protocol, refer to [3].

In the following description we suppose that two communications parties, A and B wish to communicate with each other.

Step1: Party A chooses $r_A \in \{0,1\}^k$ randomly and computes $\alpha_A = g^{r_A}$, then sends α_A to B.

Step2: Upon receiving the message α_A, party B chooses $r_B \in \{0,1\}^k$ randomly and computes $\alpha_B = g^{r_B}$, then sends α_B to A. and computes the session key: $K_{AB} = pk_A^{r_B} \bigoplus \alpha_A^{sk_B} \bigoplus \alpha_A^{r_B}$.

Step3: Upon receiving the message α_B, party A also computes the session key: $K_{AB} = pk_B^{r_A} \bigoplus \alpha_B^{sk_A} \bigoplus \alpha_A^{r_A}$.

3 KCI Attack on the P1 and the P2 Protocols

3.1 KCI Attack on the P1 Protocol

In this subsection, we will show that the P1 protocol can be intruded by using KCI attack. Assume that the adversary E has the knowledge of party A's

static private key sk_A and he intends to launch the attack against party A by pretending party B. The adversary E can carry out his KCI attack as follows:

Step1: Party A chooses $r_A \in \{0,1\}^k$ randomly and computes $\alpha_A = g^{r_A}$, then sends α_A to B.

Step2: Upon intercepting the message α_A, the adversary E chooses $r_E \in \{0,1\}^k$ randomly, computes $\alpha_E = g^{r_E}$, then E impersonates party B, sends $\alpha_E = g^{r_E}$ to party A and computes the session key:

$$K^*_{AB} = pk_A^{sk_B} \bigoplus \alpha_A^{r_E} = pk_B^{sk_A} \bigoplus \alpha_A^{r_E}.$$

Step3: Upon receiving the message $\alpha_E = g^{r_E}$, party A computes the session key:

$$K^*_{AB} = pk_B^{sk_A} \bigoplus \alpha_E^{r_A} = pk_B^{sk_A} \bigoplus \alpha_A^{r_E}.$$

So we have successfully launched the KCI attack to party A, who is the initiator. Similarly we can also launch the KCI attack to party B, who is the responder. The details are omitted.

3.2 EKC Attack on the P1 Protocol

In this subsection, we will present EKC attack on the P1 protocol. Since the session key is $K_{AB} = pk_A^{sk_B} \bigoplus \alpha_A^{r_B}$, so if the adversary E gets the ephemeral private key r_B, he will mount the attack, the details of which will be introduced in next subsection. So we can conclude that the P1 protocol can't resist EKC attack.

3.3 Analysis of the P1 Protocol' KI

Xinglan Zhang shows that the P1 protocol provides KI if the adversary can not learn the session key which is not established successfully. In this subsection, we will show that session keys generated by the P1 protocol are related to each other only if the adversary can get some session ephemeral private key. Assume that the adversary E has the knowledge of party A's session key K^1_{AB} and ephemeral private key r^1_A. The adversary E can carry out this attack as follows:

Step1: The adversary E can use r^1_A and K^1_{AB} to get the value $pk_B^{sk_A}$.

$$K^1_{AB} \bigoplus \alpha_B^{r^1_A} = pk_B^{sk_A} \bigoplus \alpha_B^{r^1_A} \bigoplus \alpha_B^{r^1_A} = pk_B^{sk_A}$$

Step2: The adversary E can impersonate party B to cheat party A. The adversary E chooses $r_E \in \{0,1\}^k$ randomly, computes $\alpha_E = g^{r_E}$, then E impersonates party B, sends $\alpha_{B^*} = g^{r_E}$ to party A.

Step3: Upon receiving the message α_{B^*}, party A chooses $r_A \in \{0,1\}^k$ randomly and computes $\alpha_A = g^{r_A}$, then sends α_A to B. and computes the session key:

$$K_{AB} = pk_A^{sk_B} \bigoplus \alpha_{B^*}^{r_A} = pk_A^{sk_B} \bigoplus g^{r_E r_A}.$$

Step4: Upon intercepting the message α_A, the adversary E computes the session key:

$$K_{AB^*} = pk_A^{sk_B} \bigoplus \alpha_A^{r_E} = pk_B^{sk_A} \bigoplus g^{r_A r_E}.$$

It is easy to see that the adversary E has succeeded in impersonating party B to party A. Especially, he does not need to learn party A's static private key.

3.4 EKC Attack on the P2 Protocol

In this subsection, we will present EKC attack on the P2 protocol. Since the session key is $K_{AB} = pk_A^{r_B} \bigoplus \alpha_A^{sk_B} \bigoplus \alpha_A^{r_B}$ and $\alpha_A = g^{r_A}$, so if the adversary E gets the ephemeral private key r_A and r_B, he can compute the session key. So we can conclude that the P2 protocol can't resist EKC attack.

4 Conclusion

In this paper, we have demonstrated certain security vulnerabilities in two authenticated key exchange protocols.

References

1. Krawczyk, H.: HMQV: A High-Performance Secure Diffie-Hellman Protocol, In: CRYPTO 2005. Lecture Notes in Computer Science 3621, 2005, pp. 546-566. Full version available at http://eprint.iacr.org/2005/176.
2. LaMacchia, B., Lauter,K., Mityagin, A.: Stronger Security of Authenticated Key Exchange, In: ProvSec 2007, Lecture Notes in Computer Science 4784, 2007, pp.1-16.
3. Xinglan Zhang.: Authenticated Key Exchange Protocol in One-Round. In: ICA3PP 2009, Lecture Notes in Computer Science 5574, 2009, pp. 226-233.