Information Processing Letters 111 (2011) 744–747

Contents lists available at ScienceDirect

Information Processing Letters

www.elsevier.com/locate/ipl

Extended KCI attack against two-party key establishment protocols

Qiang Tang [a,*], Liqun Chen [b]

[a] DIES, Faculty of EEMCS, University of Twente, The Netherlands
[b] Hewlett–Packard Laboratories, Bristol, UK

ARTICLE INFO

Article history:
Received 14 September 2010
Received in revised form 10 May 2011
Accepted 10 May 2011
Available online 12 May 2011
Communicated by D. Pointcheval

Keywords:
Cryptography
Key establishment
KCI attack
Extended KCI attack

ABSTRACT

We introduce an extended Key Compromise Impersonation (KCI) attack against two-party key establishment protocols, where an adversary has access to both long-term and ephemeral secrets of a victim. Such an attack poses serious threats to both key authentication and key confirmation properties of a key agreement protocol, and it seems practical because the adversary could obtain the victim's ephemeral secret in a number of methods; for example, by installing some Trojan horse into the victim's computer platform or by exploiting the imperfectness of the pseudo-random number generator in the platform. We demonstrate that the 3-pass HMQV protocol, which is secure against the standard KCI attack, is vulnerable to this new attack. Furthermore, we show a countermeasure to prevent such an attack.

1. Introduction

The history of two-party key establishment goes back a long way, although the modern study of key establishment protocols can be traced back to the seminal work of Needham and Schroeder [11]. Particularly, since the seminal work of Diffie and Hellman [4], key establishment has been a very fruitful area in cryptography. So far, numerous protocols have been proposed, as surveyed in [3,10]. The standardization bodies, such as ISO and IEEE, have also created a number of key establishment standards [5,6,8].

With respect to two-party key establishment protocols, there are two fundamental properties, namely key authentication and key confirmation. Suppose that Alice runs a protocol to establish a session key with Bob. The key authentication property means that Alice is assured that only Bob is able to learn the session key. The key confirmation property means that if Alice has successfully ended a protocol execution then Alice is assured that Bob has actually learned the session key. In most cases, the key confirmation property implies entity authentication, which means that if Alice is assured that Bob actually participates in the protocol execution. There have been many attack scenarios against these properties, including attacks against forward secrecy, unknown key share attacks, and key compromise impersonation (KCI) attacks, as surveyed in [3,10].

In this Letter, we are interested in KCI attacks, as described in [1,3], where an adversary, which has obtained Alice's *long-term secret* (such as a decryption key or a signing key), impersonates Bob to run the protocol with Alice. A successful KCI attack may represent a violation to both key authentication and key confirmation properties. A two-party key establishment protocol is secure against KCI attacks assures that the adversary cannot impersonate another user, say Bob, to Alice even with access to Alice's long-term secret. Clearly, with Alice's long-term secret, the adversary can trivially impersonate Alice to any other user, say Bob. Nonetheless, KCI attack resilience provides the additional security assurance that, in the absence of Bob, an adversary cannot successfully impersonate Bob to establish a session key with Alice. This property has been advocated for many protocols.

The contribution of this Letter is that we introduce a new type of KCI attacks, namely the extended KCI attack. In such an attack, the adversary has access to not only Alice's *long-term secret* but also her *ephemeral secret* such as

[*] Corresponding author.
E-mail addresses: q.tang@utwente.nl (Q. Tang), liqun.chen@hp.com (L. Chen).

0020-0190/$ – see front matter © 2011 Elsevier B.V. All rights reserved.
doi:10.1016/j.ipl.2011.05.009

the ephemeral Diffie–Hellman key. Note that, in practice, to obtain the ephemeral secret, the adversary could install some Trojan horse in the participant's computing device to steal the secrets, or it could make use of the imperfectness of the pseudo-random number generator in use. We demonstrate that the well-known 3-pass HMQV protocol by Krawczyk [9], which is secure against the standard KCI attack, is vulnerable to this new attack.

In order to avoid the extended KCI attack, we require each participant individually provides a piece of evidence that s/he is in possession of her/his long-term secret, apart from using the secret in the Diffie–Hellman key exchange. As a countermeasure, we show that a deterministic signature scheme can be used as this evidence and enables a 2-party key agreement protocol to prevent from such an attack.

By following the security notion of KCI, as addressed in [1], the adversary against the property of extended KCI resilience is actively involved in the test session in the sense that if the adversary challenges the oracle that belongs to Alice and has a matching oracle belonging to Bob, the adversary is required to provide a signature on the protocol transcripts under Bob's long-term private signing key. With this restriction, we can address the functionality of the adversary who has the goal of impersonating Bob to Alice under the condition of corrupting Alice's long-term and ephemeral secrets.

The rest of the paper is organized as follows. In Section 2, we demonstrate the extended KCI attack against the 3-pass HMQV protocol. In Section 3, we show how to enhance the HMQV protocol to prevent the extended KCI attack. In Section 4, we conclude the paper.

2. Demonstration of the new attack

2.1. Description of the 3-pass HMQV

We recall the 3-pass protocol of the HMQV family [9], and it is proven secure against the standard KCI attacks. Let Alice and Bob be two users who trust a TTP in common and agree on a group $\mathbb{G}$ of prime order q, a generator g of $\mathbb{G}$, a hash function H, and a message authentication code MAC. Alice selects her long-term private key $a \in_R \mathbb{Z}_q$ and lets the TTP certify the public key g^a, and Bob selects his long-term private key $b \in_R \mathbb{Z}_q$ and lets the TTP certify the public key g^b. The protocol is shown in Fig. 1.

The values σ_a and σ_b are defined as follows:

$$d = \bar{\mathsf{H}}(X || \text{“Bob”}), \qquad e = \bar{\mathsf{H}}(Y || \text{“Alice”}),$$
$$\sigma_a = \left(Y g^{be}\right)^{x+da}, \qquad \sigma_b = \left(X g^{ad}\right)^{y+eb},$$

where $\bar{\mathsf{H}}$ outputs the first ℓ bit of the input of the hash function H given that the security parameter is ℓ. It is straightforward to verify that

$$\sigma_a = \sigma_b = g^{(x+ad)(y+be)}.$$

2.2. Extended key compromise impersonation attack

We show an extended KCI attack, where the adversary is allowed to access not only Alice's long-term secret a but also the ephemeral secret, namely the ephemeral Diffie–Hellman key x. It is worth noting that this attack is beyond the security model described in [9], so that it does not imply the protocol is insecure in the original model.

$$\begin{array}{lcr}
\hline
\text{Alice } (a, g^a) & & \text{Bob } (b, g^b) \\
\hline
x \in_R \mathbb{Z}_q & & \\
X = g^x & & \\
 & \xrightarrow{X} & \\
 & & y \in_R \mathbb{Z}_q,\ Y = g^y \\
 & & k_m = \mathsf{H}(\sigma_b || 0) \\
 & & Z = \mathsf{MAC}(\text{“1”}, k_m) \\
 & \xleftarrow{Y,Z} & \\
k_m = \mathsf{H}(\sigma_a || 0) & & \\
\text{Verify } Z & & \\
W = \mathsf{MAC}(\text{“0”}, k_m) & & \\
 & \xrightarrow{W} & \\
 & & \text{Verify } W \\
sk = \mathsf{H}(\sigma_a || 1) & & sk = \mathsf{H}(\sigma_b || 1) \\
\hline
\end{array}$$

Fig. 1. The 3-pass HMQV protocol.

The attack is indeed fairly straightforward. Referring to the protocol in Fig. 1, suppose that an adversary has access to x and a, and mounts an attack against Alice. To do so, the adversary computes $\sigma'_b = g^{(x+ad)y} \cdot (g^b)^{(x+ad)e}$ and impersonates Bob to send all the messages. Note the fact that the computation of σ'_b does not need the knowledge of b. It is straightforward to verify that $\sigma'_b = \sigma_a$, and the adversary always succeeds in the attack. In addition, the adversary computes the same session key as that of Alice.

Generally speaking, in the 3-pass HMQV protocol, one can compute the session key with the knowledge of (x, y, b) or (x, y, a) but without knowing a or b. We observe that if any 2-party authenticated key agreement protocol with this property, then it suffers from the extended KCI attack. For example, Key Agreement Mechanisms 8–10 of ISO/IEC 11990-3:2008 [7] are secure against a KCI attack but vulnerable to an extended KCI attack. Note that, for Key Agreement Mechanism 8, we only consider Entity A, since Entity B suffers from the KCI attack.

3. Prevention of the attack

With respect to the extended KCI attack against the 3-pass HMQV protocol, the problem is that, once obtaining Alice's both long-term and ephemeral secrets the adversary is able to compute the authentication message Z without the knowledge of Bob's private key b. We observe that in order to prevent such an attack, the users (Alice and Bob) should additionally and individually demonstrate the knowledge of their long-term private key to each other. To do this, we make use of deterministic EU-CMA secure signature schemes. By a deterministic signature, we mean that a signature is a function of the private signing key and a signed message, and does not involve any ephemeral secret, since we assume our solution works in the environment where the ephemeral secret might be vulnerable. As an example, we choose the BLS signature for a reasonably good performance [2], although other secure deterministic signature schemes should also suffice.

$$\begin{array}{lcr}
\hline
\text{Alice } (a, A = g^a) & & \text{Bob } (b, B = g^b) \\
\hline
x \in_R \mathbb{Z}_q,\ X = g^x & & \\
 & \xrightarrow{X} & \\
 & & y \in_R \mathbb{Z}_q,\ Y = g^y \\
 & & k_m = \mathsf{H}(\sigma_b||0) \\
 & & Z = \mathsf{MAC}(\text{“1''}, k_m) \\
 & & m = \text{“}Alice\text{''}\|\text{“}Bob\text{''}\|A\|B\|X\|Y \\
 & & \boxed{V = (\mathsf{H}_1(m))^b} \\
 & \xleftarrow{Y, Z, \boxed{V}} & \\
k_m = \mathsf{H}(\sigma_a||0) & & \\
\text{Verify } Z & & \\
W = \mathsf{MAC}(\text{“0''}, k_m) & & \\
\boxed{\text{Verify } V} & & \\
m = \text{“}Alice\text{''}\|\text{“}Bob\text{''}\|A\|B\|X\|Y & & \\
\underline{V' = (\mathsf{H}_1(m))^a} & & \\
 & \xrightarrow{W,\ \underline{V'}} & \\
 & & \text{Verify } W \\
 & & \underline{\text{Verify } V'} \\
sk = \mathsf{H}(\sigma_a||1) & & sk = \mathsf{H}(\sigma_b||1) \\
\hline
\end{array}$$

Fig. 2. The enhanced 3-pass HMQV protocol.

In the following, we first describe the BLS signature scheme, and then present the enhanced 3-pass HMQV protocol.

3.1. *The BLS signature scheme*

Let $\mathbb{G}, \mathbb{G}_T$ be groups of prime order q, and g be a generator of $\mathbb{G}$. Let $\mathsf{H}_1 : \{0,1\}^* \rightarrow \mathbb{G}$. Suppose that there exists a bilinear map $\hat{e} : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$. If a signer possesses the private/public key pair (α, g^α), where $\alpha \in_R \mathbb{Z}_q$. For a message $\beta \in \{0,1\}^*$, the signature generation and verification procedures are as follows:

1. The signer computes V as the signature, where $V = (\mathsf{H}_1(\beta))^\alpha \in \mathbb{G}$.
2. The verifier verifies that $\hat{e}(V, g) = \hat{e}(\mathsf{H}_1(\beta), g^\alpha)$. If so, the signature is accepted.

This scheme is proven to be EU-CMA secure under the computational Diffie–Hellman assumption [2]. Moreover, it is straightforward to check that the signature V leaks no information about α given that H_1 is modeled as a random oracle and the discrete-logarithm problem is hard in $\mathbb{G}$.

3.2. *Enhanced 3-pass HMQV protocol*

We assume the same setting of the original 3-pass HMQV protocol shown Fig. 1. But, for the group $\mathbb{G}$ defined in the original protocol, we further assume that there exists a group $\mathbb{G}_T$ of prime order q and a bilinear map $\hat{e} : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$. Let H_1 be a hash-function, $\mathsf{H}_1 : \{0,1\}^* \rightarrow \mathbb{G}$. The enhanced 3-pass HMQV protocol is shown Fig. 2, where Alice and Bob use BLS signatures to demonstrate their knowledge of their long-term secrets. Note that the data used by Alice to demonstrate her knowledge is underlined, and that used by Bob to demonstrate his knowledge is boxed.

With respect to this enhanced protocol, we briefly analyse its security properties from two aspects:

1. Since a BLS signature leaks no information about the signing key, Alice (Bob) does not leak any information about a (b) by getting involved in the additional procedure. As a result, the security properties of the original 3-pass HMQV protocol, as described in [9], will still hold.
2. Because the BLS signature scheme is EU-CMA secure, an adversary cannot impersonate Alice to Bob (or Bob to Alice), i.e. mounting an extended KCI attack against Bob (or Alice), even if it has compromised Bob's (or Alice's) long-term and ephemeral secrets. Because the BLS signature is deterministic, security of this signature does not rely on the assumption that any ephemeral secret is safe in the system.

In summary, the enhanced 3-pass HMQV protocol preserves the original security properties described in [9], and it is also secure against the extended KCI attack.

4. Conclusion

In this Letter, we have introduced an extended KCI attack against two-party key establishment protocols and shown that the 3-pass HMQV protocol is vulnerable to the new attack. In the enhanced 3-pass HMQV protocol, because of involving the BLS signature, Alice (Bob) needs to compute one exponentiation and one pairing. Compared with the original protocol, this is a substantial increase in the computational complexity. In addition, the enhanced protocol requires the existence of a bilinear map for $\mathbb{G}$. It is an interesting future work to improve its efficiency and avoid the additional requirement. Another interesting future work is to analyse the security of other protocols with respect to this new attack and investigate the corresponding countermeasures. Yet another interesting future work is to formalise the notion of extended KCI resilience to formally study the new property.

References

[1] S. Blake-Wilson, D. Johnson, A. Menezes, Key agreement protocols and their security analysis, in: M. Darnell (Ed.), Proceedings of Cryptography and Coding, 6th IMA International Conference, in: Lecture Notes in Computer Science, vol. 1355, Springer, 1997, pp. 30–45.

[2] D. Boneh, B. Lynn, H. Shacham, Short signatures from the Weil pairing, Journal of Cryptology 17 (4) (2004) 297–319.

[3] C. Boyd, A. Mathuria, Protocols for Authentication and Key Establishment, Springer, 2004.

[4] W. Diffie, M. Hellman, New directions in cryptography, IEEE Transactions on Information Theory IT-22 (6) (1976) 644–654.

[5] Institute of Electrical and Electronics Engineers, Inc. IEEE P1363-2000: Standard Specifications for Public-Key Cryptography and IEEE 1363a-2004: Standard Specifications for Public-Key Cryptography – Amendment 1: Additional Techniques.

[6] Institute of Electrical and Electronics Engineers, Inc. IEEE P1363.2 draft D26, Standard Specifications for Password-Based Public-Key Cryptographic Techniques, September 2006.

[7] International Organization for Standardization, ISO/IEC 11770–3:2008, Information technology — Security techniques — Key management — Part 2: Mechanisms Using Asymmetric Techniques.

[8] International Organization for Standardization, ISO/IEC 11770 (all parts), Information technology — Security techniques — Key management.

[9] H. Krawczyk, HMQV: A high-performance secure Diffie–Hellman protocol, in: Victor Shoup (Ed.), Advances in Cryptology — CRYPTO 2005, in: Lecture Notes in Computer Science, vol. 3621, Springer, 2005, pp. 546–566. Also available at Cryptology ePrint Archive: Report 2005/176.

[10] A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1997.

[11] R. Needham, M. Schroeder, Using encryption for authentication in large networks of computers, Communications of the ACM 21 (12) (1978) 993–999.