A Key Compromise Impersonation attack against Wang's Provably Secure Identity-based Key Agreement Protocol

Maurizio Adriano Strangio

University of Rome "Roma Tre", ROME, ITALY
strangio@mat.uniroma3.it

Abstract. In a 2005 IACR report, Wang published an efficient identity-based key agreement protocol (IDAK) suitable for resource constraint devices.
The author shows that the IDAK key agreement protocol is secure in the Bellare-Rogaway model with random oracles and also provides an ad-hoc security proof claiming that the IDAK protocol is not vulnerable to Key Compromise Impersonation attacks.
In this report, we claim that the IDAK protocol is vulnerable to key-compromise impersonation attacks. Indeed, Wang's results are valid only for a passive adversary that can corrupt parties or reveal certain session-specific data but is not allowed to manipulate protocol transcripts; a model considering this type of adversary is unable to afford KCI resilience.

1 Introduction

In a 2005 IACR report ([5] and also [6]), Wang proposed a novel identity-based key agreement protocol (IDAK) using the Weil/Tate pairing and also provided a security proof in the Bellare-Rogaway model [1].

In this paper, we show that the IDAK protocol is vulnerable to key-compromise impersonation (KCI) attacks; an opponent, having learned the long-term private key of an honest party (say A), can establish a valid session key with A by masquerading as another legitimate principal (say B). This attack represents a subtle threat that is often underestimated and difficult to counter [4].

2 Notation and mathematical background

To make the paper self-contained, we briefly recall the underlying mathematical concepts and notation. Let us consider two multiplicative cyclic groups G and G_1 of order q with g a generator of G. The bilinear map $\hat{e} : G \times G \rightarrow G_1$ has the following three properties:

1. bilinearity, for all $g_1, g_2 \in G$ and $x, y \in Z : \hat{e}(g_1^x, g_2^y) = \hat{e}(g_1, g_2)^{xy} = \hat{e}(g_1^y, g_2^x)$;
2. non-degeneracy, for all $g \in G$, $\hat{e}(g, g) \neq 1$ is a generator in G_1;
3. computability, for $g_1, g_2 \in G : \hat{e}(g_1, g_2) \in G_1$ is computable in polynomial time.

The modified Weil and Tate pairings associated with supersingular elliptic curves are examples of admissible pairings [3], [2].

If X is a finite set then $x \stackrel{R}{\leftarrow} X$ or $x \in_R X$ denote the sampling of an element uniformly at random from X. If α is neither an algorithm nor a set $x \leftarrow \alpha$ represents a simple assignment statement.

The Bilinear Diffie-Hellman Assumption (BDH) assumption holds in the group G if for random elements $x, y, z \in Z_q^*$ it is computationally hard to compute $\hat{e}(g, g)^{xyz}$.

Assumption 1 (BDH) *The group G satisfies the Bilinear Diffie-Hellman Assumption if for all PPT algorithms we have:*

$$\begin{array}{l} x \stackrel{R}{\leftarrow} Z_q^*; y \stackrel{R}{\leftarrow} Z_q^*; z \stackrel{R}{\leftarrow} Z_q^*; X \leftarrow g^x; Y \leftarrow g^y; Z \leftarrow g^z : \\ \Pr\left[\mathcal{A}(X, Y, Z)=\hat{e}(g, g)^{xyz}\right] < \epsilon \end{array}$$

where the probability is taken over the coin tosses of $\mathcal{A}$ (and random choices of x, y, z) and ϵ is a negligible function.

The Decisional Bilinear Diffie-Hellman Assumption (DBDH) assumption holds in the group G if for random elements $x, y, z, r \in Z_q^*$ it is computationally hard to distinguish the distributions $\langle x, y, z, r\rangle$ and $\langle x, y, z, \hat{e}(g, g)^{xyz}\rangle$.

Assumption 2 (DBDH) *The group G satisfies the Decisional Bilinear Diffie-Hellman Assumption if for all PPT algorithms we have:*

$$\begin{array}{l} x \stackrel{R}{\leftarrow} Z_q^*; y \stackrel{R}{\leftarrow} Z_q^*; z \stackrel{R}{\leftarrow} Z_q^*; X \leftarrow g^x; Y \leftarrow g^y; Z \leftarrow g^z : \\ \Pr[\mathcal{A}(X, Y, Z, r)=1]\text{-}\Pr[\mathcal{A}(X, Y, Z, \hat{e}(g, g)^{xyz})=1] < \epsilon \end{array}$$

where the probability is taken over the coin tosses of $\mathcal{A}$ (and random choices of x, y, z) and ϵ is a negligible function.

3 Review of the IDAK protocol

In this section we review the IDAK identity-based key agreement protocol. The protocol is completely specified by three algorithms Setup, Extract, Exchange:

- **Setup**, for input the security parameter k:
  1. Generate a bilinear group $G_\rho = \{G, G_1, \hat{e}\}$ with the groups G and G_1 of prime order q. Define h as the co-factor of the group order q for G;
  2. Choose a generator $g \in G$;
  3. Choose a random master secret key $\alpha \in_R Z_q^*$;
  4. Choose the cryptographic hash functions $H : \{0, 1\}^* \to G$ and $\pi : G \times G \to Z_q^*$. In security analysis of protocol IDAK, H and π are simulated as random oracles.

  The system parameters are $(hq, h, g, G, G_1, \hat{e}, H, \pi)$ and the master secret key is α.
- **Extract**, For a given identification string $ID \in \{0, 1\}^*$, the algorithm computes $g_{ID} = H(ID) \in G$ and returns the private key $d_{ID} = g_{ID}^\alpha$;

– **Exchange**, For two peers A and B with identities ID_A and ID_B respectively, the algorithm proceeds as follows (cfg Fig. 1):
  1. A selects $x \in_R Z_q^*$, computes $R_A = g_{ID_A}^x$ and sends R_A to B;
  2. B selects $y \in_R Z_q^*$, computes $R_B = g_{ID_B}^y$ and sends R_B to A;
  3. On receipt of R_B, A computes $s_A = \pi(R_A, R_B), s_B = \pi(R_B, R_A)$ and the shared secret sk_{AB} as
     $\hat{e}(g_{ID_A}, g_{ID_B})^{(x+s_A)(y+s_B)h\alpha} = \hat{e}(g_{ID_B}^{s_B} \cdot R_B, g_{ID_A}^{(x+s_A)h\alpha})$;
  4. On receipt of R_A, B computes $s_A = \pi(R_A, R_B), s_B = \pi(R_B, R_A)$ and the shared secret sk_{BA} as
     $\hat{e}(g_{ID_A}, g_{ID_B})^{(x+s_A)(y+s_B)h\alpha} = \hat{e}(g_{ID_A}^{s_A} \cdot R_A, g_{ID_B}^{(x+s_B)h\alpha})$;

The main result of [5] is Theorem 5.2 which proves that IDAK is a secure key agreement protocol in the Bellare-Rogaway model under the DBDH and random oracle assumptions. The author also presents ad ad-hoc security proof claiming that the protocol is not vulnerable to KCI attacks (Theorem 7.1).

$$
\begin{aligned}
A &: x \xleftarrow{R} Z_q^* \\
&\quad R_A \leftarrow g_{ID_A}^x \\
A \rightarrow B &: R_A \\
B &: y \xleftarrow{R} Z_q^* \\
&\quad R_B \leftarrow g_{ID_B}^y \\
B \rightarrow A &: R_B \\
A &: s_A \leftarrow \pi(R_A, R_B),\ s_B \leftarrow \pi(R_B, R_A) \\
&\quad sk_{AB} \leftarrow \hat{e}(g_{ID_B}^{s_B} \cdot R_B, g_{ID_A}^{(x+s_A)h\alpha}) \\
A &: s_A \leftarrow \pi(R_A, R_B),\ s_B \leftarrow \pi(R_B, R_A) \\
&\quad sk_{BA} \leftarrow \hat{e}(g_{ID_A}^{s_A} \cdot R_A, g_{ID_B}^{(x+s_B)h\alpha})
\end{aligned}
$$

Fig. 1. Protocol IDAK

4 A KCI attack against the IDAK protocol

Below we describe how a malicious adversary $\mathcal{A}$ can conduct a successful KCI attack against the IDAK protocol:

1. Adversary $\mathcal{A}$ obtains A's private key d_{ID_A};
2. B selects $y \in_R Z_q^*$, computes $R_B = g_{ID_B}^y$ and sends R_B to A;
3. $\mathcal{A}$ intercepts message R_B, generates a random nonce $u \in Z_q^*$, computes $R_B^{'} = g_{ID_A}^u \cdot g_{ID_B}^{-s_B}$ and sends $R_B^{'}$ to B (thus replacing message R_B);
4. On receipt of $R_B^{'}$, A follows the protocol specification and terminates with the session key $sk_{AB} = \hat{e}(g_{ID_B}^{s_B} \cdot R_B^{'}, g_{ID_A}^{(x+s_A)h\alpha})$;
5. $\mathcal{A}$ computes $sk^{'} = \hat{e}(d_{ID_A}^u, R_A \cdot g_{ID_A}^{s_A})$ and will be able to establish a communication session with A since $sk^{'} = sk_{AB}$.

The attack succeeds because the transcript $R_B^{'}$ is indistinguishable from a real one generated by an honest principal (according to the protocol specification) and $sk^{'} = sk_{AB}$ as demonstrated by the following equality:

$$\begin{aligned} sk_{AB} &= \hat{e}(g_{ID_B}^{s_B} \cdot R_B^{'}, g_{ID_A}^{(x+s_A)h\alpha}) \\ &= \hat{e}(g_{ID_B}^{s_B} \cdot R_B^{'}, (g_{ID_A}^{x} \cdot g_{ID_A}^{s_A})^{h\alpha}) \\ &= \hat{e}(g_{ID_B}^{s_B} \cdot R_B^{'}, (R_A \cdot g_{ID_A}^{s_A})^{h\alpha}) \\ &= \hat{e}(g_{ID_B}^{s_B} \cdot g_{ID_A}^{u} \cdot g_{ID_B}^{-s_B}, (R_A \cdot g_{ID_A}^{s_A})^{h\alpha}) \\ &= \hat{e}((g_{ID_A}^{h\alpha})^{u}, R_A \cdot g_{ID_A}^{s_A}) \\ &= \hat{e}(d_{ID_A}^{u}, R_A \cdot g_{ID_A}^{s_A}) \\ &= sk^{'} \end{aligned}$$

5 Conclusions

The result of Section 4 implies that the IDAK protocol is not secure against party corruption attacks brought by an active adversary. In particular, Theorem 7.1 in Wang's paper is valid under the hypothesis that R_B is chosen according to some probabilistic polynomial time distribution; this assumption is correct only for passive adversaries.

To define a meaningful notion of KCI-resilience requires a model that considers an active adversary in the security experiment who can ask corrupt queries and also freely manipulate network message transcripts. With such a powerful (and more realistic) adversary, it is difficult to design KCI-resilient key agreement protocols since there are infinite ways to exploit the algebraic structure of the underlying group to attack the protocol (because the specification simply requires that a message transcript be a group element).

References

1. M. Bellare and P. Rogaway. Entity authentication and key distribution. *In Proceedings of CRYPTO 1993*, LNCS 773:232–249, 1993.
2. D. Boneh and M. Franklin. Identity-based encryption from the weil pairing. *Proceedings of Crypto01, Springer-Verlag, New York*, LNCS 2139:213–229, 2001.
3. L. Chen and C. Kudla. Identity based authenticated key agreement protocols from pairings. *Cryptology ePrint Archive, Report 2002/184*, http://eprint.iacr.org/2002/184.pdf, 2002.
4. M. A. Strangio. On the Resilience of Key Agreement Protocols to Key Compromise Impersonation. *Cryptology ePrint Archive, Report 2006/252*, http://eprint.iacr.org/2006/252.pdf, 2006.
5. Y. Wang. Efficient Identity-Based and Authenticated Key Agreement Protocol. *Cryptology ePrint Archive, Report 2005/108*, http://eprint.iacr.org/2005/108.pdf, 2005.
6. Y. Wang. Efficient Identity-Based and Authenticated Key Agreement Protocol. *CoRR*, abs/1207.5438, 2012.