Contemporary Engineering Sciences, Vol. 8, 2015, no. 17, 765 - 771
HIKARI Ltd, www.m-hikari.com
http://dx.doi.org/10.12988/ces.2015.57199

Security Analysis of Kar's ID-based Deniable Authentication Protocol

Eun-Jun Yoon[1]

Department of Cyber Security, Kyungil University
Kyungsangpuk-Do 712-701, Republic of Korea

Abstract

In 2013, Kar proposed a secure ID-based deniable authentication protocol whose security is based on computational infeasibility of solving Elliptic Curve Diffie-Hellman Problem(ECDHP). Kar claimed that the proposed protocol achieves properties of deniable authentication, mutual authentication, and message confidentiality. However, this paper points out that Kar's protocol still suffers from sender spoofing attack and message modification attack unlike its claims.

Keywords: Deniable authentication; Elliptic curve cryptography; Diffie-Hellman problem; Cryptanalysis; Spoofing attack

1 Introduction

Deniable authentication protocol is a new security authentication mechanism which can enable a receiver to identify the true source of a given message, but not to prove the identity of the sender to a third party[1]. The deniable property[1, 2, 3, 4, 5, 6] is very useful for providing secure negotiation over the Internet and it has the following two features compared with traditional authentication protocols:

1. It enables an intended receiver to identify the source of a given message.

[1]Corresponding author

2. The intended receiver cannot prove to any third party the identity of the sender.

In the past several years, numerous deniable authentication protocols have been proposed but many of them have also been proven to be vulnerable to various cryptanalytic attacks[1, 2, 3, 4, 5, 6]. In 2013, Kar[7] proposed a secure identity based deniable authentication protocol whose security is based on computational infeasibility of solving Diffie-Hellman Problem on Elliptic Curve(ECDHP). The security of the Kar's protocol is based on difficulty of breaking the ECDLP and secure one way hash function. Kar's protocol is an non-interactive protocol and can be easy implemented in mobile devices such as PDA, smart card etc. Kar claimed that the proposed protocol achieves properties of deniable authentication, mutual authentication, and message confidentiality[7, 6]. However, this paper points out that Kar's protocol still suffers from sender spoofing attack and message modification attack unlike its claims.

This paper is organized as follows: Section 2 briefly reviews the Kar's protocol. The security flaws of Kar's protocol are shown in Section 3. Finally, conclusions are given in Section 4.

2 Review of Kar's Deniable Authentication Protocol

This section briefly reviews Kar's protocol[7]. Figure 1 depicts the Kar's deniable authentication protocol. The Kar's protocol involves two entities: a sender S and a intended receiver R. It follows the followings phases.

Setup phase Let $H : \{0,1\}^* \rightarrow \{0,1\}^l$ be a secure cryptographic hash function which is of collision. In Kar's protocol, the sender has a certificate issued by the certificate authority(CA). The CA contains the public key(π_{pub}) of the Receiver, and the signature of CA for the certificate. The sender can obtain (π_{pub}) and verify the validity of it. The private key(π_{prv}) of receiver is kept secret.

Extract phase It follows the following steps.

E1. The sender S with identity $ID_s \in \{0,1\}^*$ selects t_s randomly from $[1, n-1]$.

E2. S computes $a_s = H(ID_s) \oplus t_s$ and $Q_s = a_s P$, where (Q_s, a_s) is the key pair of S.

E3. S concatenates Q_s with the time stamp $T \in Z_q^*$.

E4. S encrypts the concatenated value $(Q_s||T)$ using receiver R's public key π_{pub} as $\tilde{Q}_s = E_{\pi_{pub}}(Q_s||T)$.

E5. Similarly, the receiver R with identity $ID_r \in \{0,1\}^*$ selects t_r randomly from $[1, n-1]$.

E6. R computes $a_r = H(ID_r) \oplus t_r$ and $Q_r = a_r P$, where (Q_s, a_s) is the key pair of R.

Send phase It follows the following steps.

S1. S sends the cipher $\tilde{Q}_s$ to the the receiver R.

S2. R decrypts using his/her own private key π_{prv} as $Q_s = D_{\pi_{prv}}(\tilde{Q}_s)$, where D denotes decryption algorithm.

S3. R computes the session key $\alpha_1 = a_r Q_s$ and the hashed value as $\beta = H(ID_r, Q_r, \alpha_1)$.

S4. R sends the computed Q_r and β to S.

S5. S computes the session key as $\alpha_2 = a_s Q_r$.

S6. S checks the equality $\beta = H(ID_r, Q_r, \alpha_2)$. If it holds, S is authenticated and Q_r will be accepted, otherwise rejected.

S7. S computes $\gamma_1 = H(\alpha_2) \oplus (M||T)$, where $M \in \{0,1\}^l$ is the deniable message.

S8. S sends the deniable authenticated message $\psi = (ID_s, T, \gamma_1)$ to the recipient R.

Receive phase It follows the following steps.

R1. After receiving $\psi = (ID_s, T, \gamma_1)$, the receiver R recovers M by computing $\gamma_1 \oplus H(\alpha_2)$. Then R computes $\gamma_2 = H(\alpha_1) \oplus (M||T)$.

R2. R verifies the validity of the equality $\gamma_1 = \gamma_2$ and the time stamp T. If holds then R accepts M otherwise reject.

Figure 1 depicts the Kar's protocol.

3 Cryptanalysis of Kar's Deniable Authentication Protocol

This section demonstrates that Kar's deniable authentication protocol still suffers from sender spoofing attack and message modification attack[7, 6].

S		R
(ID_s, π_{pub})		(ID_r, π_{prv})
Select random $t_s \in [1, n-1]$		
$a_s \leftarrow H(ID_s) \oplus t_s$		
$Q_s \leftarrow a_s P$		
Generate time stamp $T \in Z_q^*$		
Encrypt $\tilde{Q}_s \leftarrow E_{\pi_{pub}}(Q_s \| T)$		
	$\{\tilde{Q}_s\}$ $\longrightarrow$	
		Decrypt $Q_s \leftarrow D_{\pi_{prv}}(\tilde{Q}_s)$
		Select random $t_r \in [1, n-1]$
		$a_r \leftarrow H(ID_r) \oplus t_r$
		$Q_r \leftarrow a_r P$
		$\alpha_1 \leftarrow a_r Q_s$
		$\beta \leftarrow H(ID_r, Q_r, \alpha_1)$
	$\{Q_r, \beta\}$ $\longleftarrow$	
$\alpha_2 \leftarrow a_s Q_r$		
Check $\beta \stackrel{?}{=} H(ID_r, Q_r, \alpha_2)$		
Choose deniable message $M \in \{0,1\}^l$		
$\gamma_1 \leftarrow H(\alpha_2) \oplus (M \| T)$		
$\psi \leftarrow (ID_s, T, \gamma_1)$		
	$\{\psi\}$ $\longrightarrow$	
		$\gamma_2 \leftarrow H(\alpha_1) \oplus (M \| T)$
		Check $\gamma_1 \stackrel{?}{=} \gamma_2$

Figure 1: Kar's Deniable Authentication Protocol

3.1 Sender spoofing attack

An attacker *Eve* can perform the following sender spoofing attack.

1. *Eve* intercepts $\{\tilde{Q}_s, \psi\}$, where $\psi = (ID_s, T, \gamma_1)$.
2. *Eve* selects a random number $t_e \in [1, n-1]$.
3. *Eve* computes $a_e = H(ID_s) \oplus t_e$ and $Q_e = a_e P$, where (Q_e, a_e) is the key pair of *Eve* to impersonate as the sender S.
4. *Eve* concatenates Q_e with the time stamp $T_e \in Z_q^*$.
5. *Eve* encrypts the concatenated value $(Q_e \| T_e)$ using receiver R's public key π_{pub} as $\tilde{Q}_e = E_{\pi_{pub}}(Q_e \| T_e)$.

6. *Eve* finally sends $\{\tilde{Q}_e\}$ to the receiver R.

After receiving $\{\tilde{Q}_e\}$, the recipient R will perform the following steps.

1. Decrypt using his/her own private key π_{prv} as $Q_e = D_{\pi_{prv}}(\tilde{Q}_e)$. Here, we can see that $D \oplus E' = D \oplus D \oplus s = s'$.
2. Compute the session key $\alpha_1 = a_r Q_e$ and the hashed value as $\beta = H(ID_r, Q_r, \alpha_1)$.
3. Send the computed Q_r and β to *Eve*.

After receiving $\{Q_r, \beta\}$, *Eve* can perform the following steps.

1. Compute the session key as $\alpha_2 = a_e Q_r$.
2. Compute $\gamma_1 = H(\alpha_2) \oplus (M_e||T_e)$, where $M_e \in \{0,1\}^l$ is the deniable message of *Eve*.
3. Send the deniable authenticated message $\psi = (ID_s, T_e, \gamma_1)$ to the recipient R.

After receiving $\{\psi\}$, the recipient R will perform the following steps.

1. Recover M_e by computing $\gamma_1 \oplus H(\alpha_2)$.
2. Compute $\gamma_2 = H(\alpha_1) \oplus (M_e||T_e)$.
3. Verify the validity of the equality $\gamma_1 = \gamma_2$ and the time stamp T_e.

Because γ_1 always equals $\gamma_2 = H(\alpha_1) \oplus (M_e||T_e)$, the recipient R will believe the trustworthy of the attacker *Eve*. Therefore, Kar's protocol is vulnerable to the above sender spoofing attack.

3.2 Message modification attack

An attacker *Eve* can perform the following message modification attack.

1. *Eve* intercepts $\psi = (ID_s, T, \gamma_1)$ and the deniable message M, where $\gamma_1 = H(\alpha_2) \oplus (M||T)$.
2. *Eve* extracts $H(\alpha_2)$ by computing $\gamma_1 \oplus (M||T) = H(\alpha_2) \oplus (M||T) \oplus (M||T) = H(\alpha_2)$.
3. *Eve* selects a fake deniable message $M_e \in \{0,1\}^l$.
4. *Eve* computes a modified $\gamma_1^* = H(\alpha_2) \oplus (M_e||T_e)$, where T_e is the current timestamp of *Eve*.

5. *Eve* sends the faked deniable authenticated message $\psi^* = (ID_s, T_e, \gamma_1^*)$ to the recipient R.

After receiving $\{\psi^*\}$, the recipient R will perform the following steps.

1. Recover M_e by computing $\gamma_1^* \oplus H(\alpha_2)$.
2. Compute $\gamma_2 = H(\alpha_1) \oplus (M_e||T_e)$.
3. Verify the validity of the equality $\gamma_1^* = \gamma_2$ and the time stamp T_e.

Because γ_1^* always equals $\gamma_2 = H(\alpha_1) \oplus (M_e||T_e)$, the recipient R will believe the trustworthy of the attacker *Eve*. Therefore, Kar's protocol is vulnerable to the above message modification attack.

4 Conclusions

This paper pointed out that recently proposed Kar's ID-based deniable authentication protocol based on Diffi-Hellman problem on Elliptic Curve suffers from sender spoofing attack and message modification attack. Further works will be focused on improving the Kar's protocol which can be able to provide strong security.

Acknowledgements

This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIP)(No. 2015R1A2A2A01006824) and partially supported by Small & Medium Business Administration grant funded by the Korea government(SMBA)(No. C0248233).

References

[1] C. Boyd, W. Mao, and K. G. Paterson, Deniable authenticated key establishment for internet protocols, *in 11th International Workshop on Security Protocols*, **3364** (2005), 255-271. http://dx.doi.org/10.1007/11542322_31

[2] J. S. Chou, Y. L. Chen, and J. C. Huang, ID-based deniable authentication protocol on pairings, *Tech.Rep. IACR ePrint*, **335**, (2006), 20.

[3] L. Fan, C. X. Xu, and J. H. Li, Deniable authentication protocol based on Diffie-Hellman algorithm, *Electronics Letters*, **38** (2002), no. 14, 705-706. http://dx.doi.org/10.1049/el:20020502

[4] M. H. Ibrahim, Receiver-deniable public-key encryption, *International Journal of Network Security*, **8** (2009), no. 2, 159-165.

[5] R. Lu, X. Lin, Z. Cao, L. Qin, and X. Liang, A simple deniable authentication protocol based on the Diffie-Hellman algorithm, *International Journal of Computer Mathematics*, **85** (2008), 1315-1323. http://dx.doi.org/10.1080/00207160701622741

[6] E. J. Yoon, E. K. Ryu, and K. Y. Yoo, Improvement of Fan et al.'s deniable authentication protocol based on Diffie-Hellman algorithm, *Applied Mathematics and Computation*, **167**, (2005), 274-280. http://dx.doi.org/10.1016/j.amc.2004.06.096

[7] J. Kar, ID-based deniable authentication protocol based on Diffie-Hellman problem on Elliptic Curve, *International Journal of Network Security*, **15** (2013), no. 5, 357-364.

Received: July 21, 2015; Published: August 26, 2015