http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 12 (3): 466-469, 2013
ISSN 1812-5638 / DOI: 10.3923/itj.2013.466.469

Security of Proxy Blind Signature Scheme

Jianhong Zhang, Yuanbo Cui and Zhipeng Chen
College of Sciences, North China University of Technology, Beijing, China

Abstract: As an important anonymity technology, proxy blind signature scheme is an important cryptographic primitive, it not only has the advantages of blind signature and proxy signature but also has some new features, it can solve many practical problems and has wide applications. Recently, an efficient certificateless proxy blind signature scheme is built with forward security. However, by our analysis, we show that the scheme is insecure, it exists unforgeable attack and also not provides forward security. Finally, the corresponding attacks are given and we also analyze the reason to produce such attack.

Key words: Proxy blind signature, certificateless scheme, unforgeability

INTRODUCTION

In traditional Public Key Infrastructure (PKI), the public key is a "random" string that is unrelated to the identity of the user. Thus, a trusted authority is needed to assure the relationship between public key and the user by producing a certificate which results in complex certificate management, such as key distribution, certificate revocation. When using a public key of a user, we first verify whether a certificate is valid or not. In 1984, the notion of ID-based cryptography is introduced to solve the certifi-cate management problem (to simplify key management and remove the public key certificate). A distinguishing property of ID-based is introduced cryptography is that a user's public key can be any binary string, such as IP address or an email address, that can identify the user's identity. The private key of a user is produced by a trusted party called a Private Key Generator (PKG), with the help of the PKG's master secret key. In such a setting, the only thing that should be certificated is the public key of the PKG, so ID-based cryptography drastically reduces the needs for certificate. However, an inherent problem of ID-PKC is that a Key Generation Center (KGC) generates any user's private key using a master-key of KGC. Obviously a malicious KGC is able to forge the signature of any signer. This is called "key escrow" problem. It means that all users must unconditionally trust the KGC.

To solve key escrow problem, Al-Riyami and Paterson (2003) proposed a novel public cryptosystem. In this system, the user's private key is not generated by the KGC solely but by the combination of part private key which generated by KGC and the secret which user selected. Without any certificates, it solves the certificates management problem in certificate-based public key systems and more suitable for secure application in low bandwidth and low-power environment.

The notion of proxy signature scheme introduced by Mambo *et al.* (1996). A proxy signature scheme allows an entity called original signer to delegate his signing capability to other entities which were called proxy signer. Since it is proposed, the proxy signature schemes have been suggested for use in many applications, particularly in distributed computing where delegation of rights is quite common. Examples discussed in the literature include distributed systems, grid computing, mobile agent applications, distributed shared object systems, global distribution networks and mobile communications. And to adapt different situations, many proxy signature variants are produced, such as one-time proxy signature, proxy blind signature, multi-proxy signature and so on. Since the proxy signature appears, it attracts many researchers' great attention. Based on the delegation type, proxy signature schemes are divided into full delegation, partial delegation and delegation by warrant. According whether the original signer know the proxy secret key, proxy signatures can also be classified as proxy-unprotected and proxy-protected schemes. In a proxy-protected scheme the original signer cannot forge the proxy signer to produce proxy signature. Thus we can clearly distinguish the rights and responsibilities between the original signer and the proxy signer.

Chaum (1983) first proposed blind signature, in the scheme, the signer can sign the document without knowing the content of it. Since, it was introduced, blind signature schemes have been used in numerous application, most prominently in anonymous voting and anonymous e-cash. By combining blind signature and proxy signature, proxy blind signature scheme not only

Corresponding Author: Jianhong Zhang, North China University of Technology, 100144, Beijing, China

has the advantages of blind signature and proxy signature but also has some new features, it can solve many practical problems and has wide applications. First of all Lin and Jan (2000) proposed proxy blind signature by the combination of proxy signature and blind signature. Later, a proxy blind signature scheme was proposed based on discrete logarithm. However, Wang *et al.* (2005) pointed out that this scheme was insecure and proposed a new proxy blind signature scheme based on scheme (Mambo *et al.*, 1996). Sun and Hsieh (2004) showed that the schemes didn't satisfy the unforgeability and unlinkability properties and they also pointed out that Lal's scheme (Wang *et al.*, 2005) didn't possess the unlinkability property either. Recently, Sun et.al proposed an efficient ceritificateless proxy blind signature based on pairing and claimed that their scheme was secure and satisfied forward security. By our analysis, we show that the scheme is insecure and the corresponding attacks are given.

REVIEWS OF CERTIFICATELESS PROXY BLIND SIGNATURE

Sun *et al.* (2011), gave a new forward-security certificateless proxy blind signature scheme and showed that their scheme was secure. To better explain the security of the scheme, the scheme is detailed as follows.

System establishment: Let G_1 and G_2 be two cyclic groups with prime order q. P is a generator of group G_1. e: $G_1 \times G_1 \rightarrow G_2$ is a bilinear pairing map. H_1: $\{0,1\}^* \rightarrow G_1$, H_2: $\{0,1\}^* \times G_1 \rightarrow Z_q$ are two hash function. Randomly choose $s \in Z_q$ and compute $P_{pub} = sP$, then the master key s is secretly kept. The system parameters Param = (G_1, G_2, e, P, P_{pub}, H_1, H_2) are published.

Key generations:

Step 1: The original signer A chooses $x_A \in Z_q$ to compute $X_A = x_A P$, $Y_A = x_A P_{pub}$, then publish $P_A = <X_A, Y_A>$ as public key

Step 2: The original signer A uses his legal identity ID_A to apply to the KGC. KGC verifies the legitimacy of the identity and computes $Q_A = H_1 (ID_A \| P_A)$, $D_A = sQ_A$, then send D_A to the original signer via a secure authentication channel

Step 3: A verifies whether $e(D_A, P) = e(Q_A, P_{pub})$ is valid. If it is, then the original signer A computes $S_A = x_A D_A$ and keeps (x_A, S_A) as private key

Step 4: The proxy signer B generates his public key $P_B = <X_B, Y_B>$ and private key (x_B, S_B) as the same process of A

Proxy authorization:

Step 1: Original signer A randomly chooses $r_A \in Z_q$, then compute $U_A = r_A Q_A$, $h = H_2(m_w, U_A)$, $V_A = (r_A + h) S_A$, where m_w is the proxy warrant which includes a detailed description. A sends (m_w, U_A, V_A) to the proxy signer B

Step 2: Proxy signer B verifies w hether $e(X_A, P_{pub}) = e(Y_A, P)$ is correct or not. If it is valid, then it computes $h = H_2(m_w, U_A)$ and verifies whether $e(P, V_A) = e(Y_A, hQ_A + U_A)$ is correct or not. If it is valid, then accept (m_w, U_A, V_A) and choose $r_i \in Z_q$ to compute proxy signing key $R_0 = r_0 Q_B$, $S_{P0} = V_A + r_0 S_B$

Key update: When in i period, B uses proxy signing key (R_{i-1}, S_{pi-1}) of i-1 period, chooses $r_i \in Z_q$, then compute the proxy signing key of i period:

$$R_i = R_{i-1} + r_i Q_B$$

$$S_{pi} = S_{pi-1} + r_i S_B = V_A + \Sigma^i_{j=0} r_j S_B$$

Forward-secure proxy blind signature: The client C has a signed message m, it collaborates with B to execute as below:

Step 1: B chooses $P_1 \in G_1$ to compute $r_B = e(P_1, P)$, then send (r_B, m_w) to C

Step 2: Upon receiving (r_B, m_w), C randomly chooses $P_2 \in G_1$, k, $c \in Z_q$ to compute $r = r_B^k e(P_2, P)^c$, $V = H_2(m, r, P_B)$, $V' = V/k$. Then send V' to B

Step 3: After B receives V', it computes $U_B = V' S_{Pi} + P_1$ and sends U_B to C

Step 4: After C obtains U_B, it computes $U = kU_B + cP_2$, then the signature on message m is (U, U_A, V, m_w, R_i). Note that in study of Sun *et al.* (2011), U_A is left out. It should be attached in the signature, otherwise, it cannot be verified

Signature verifying: The verifier of proxy blind signature can verify the validity of the proxy blind signature (U, U_A, V, m_w, R_i) of message m:

Step 1: It checks whether the message m is in accord with the requirement in the warrant m_w

Step 2: Then it computes $Q_A = H_1(ID_A \| P_A)$, $Q_B = H_1(ID_B \| P_B)$, $h = H_2(m_w, U_A)$

Step 3: Finally, it verifies the equation $e(U, P) = e(Y_A, hQ_A + U_A)^V e(Y_B, R_i)^V r$

Step 4: If it holds, then this signature is valid

SECURITY ANALYSIS

Sun *et al.* (2011) claimed that their scheme was secure. It satisfies unforgeability, blindness and forward security. However, by analyzing the security of the scheme, it is showed that their scheme is insecure. It does not satisfy unforgeability which is a primitive property of a digital signature and forward security. And it is universally forgeable, note that any one can produce a forged blind signature on arbitrary a message.

Attack on unforgeability: In the subsection, we show the scheme is universally forgeable. Assume that an adversary wants to attack the scheme, it can do the following:

Step 1: Let m^* be a forged message
Step 2: It randomly chooses $U'_A \in G_1$, $V' \in Z_q$
Step 3: Then it computes $Q_A = H_1(ID_A \| P_A)$, $Q_B = H_1(ID_B \| P_B)$, $h^* = H_2(m_w, U'_A)$
Step 4: It sets $r^* = e(Y_A, h^*Q_A + U'_A)^{-V'}$
Step 5: Randomly choose $k \in Z_q$ to compute $R_i^* = kP$
Step 6: It sets: $U^*_A = U'_A$, $V^* = V'$, $U^* = kV^*Y_B$
Step 7: The forged blind signature is: U^*, V^*, m_w, r^*, R^*_i, U^*_A

In the following, we show that our forged signature can pass the verification of signature.

Since:

$$e(Y_A, h^*Q_A + U^*_A)^{V^*} e(Y_B, R_i^*)^{V^*} r^* = e(Y_A, h^*Q_A + U^*_A)^{V^*} e(Y_B, R_i^*)^{V^*}$$
$$e(Y_A, h^*Q_A + U'_A)^{-V'} = e(Y_B, R_i^*)^{V^*} = e(kV^*Y_B, P) = e(U^*, P)$$

Obviously, our forged blind signature satisfies the verification equation of signature, it means that our attack is valid. The main reason to our attack is that V in the signature is free. In fact, our attack is easily resisted. V should not be a part of the blind signature, it should be computed by $V = H_2(m, r, P_B)$. However, even if V is represented as $V = H_2(m, r, P_B)$, it is also attacked. In the following, we give another an attack.

Another attack on unforgeability: In a certificateless cryptography, the user can randomly choose his public key, thus the unforgeability of a certificateless signature scheme must be able to against such attack. In the following, we will show that Sun et al's scheme is not able to resist such attack, namely, an adversary can produce a forgery in name of the proxy signer without the delegation of the original signer. The detail attack is given as follows:

Step 1: The adversary randomly chooses $k \in Z_q$ to set $Y_B^* = kY_A$ where Y_A is the public key of the original signer
Step 2: Then the adversary randomly chooses $l \in Z_q$ to compute $r^* = e(P, lP)$
Step 3: Compute $V^* = H_2(m, r^*, P_B^*)$
Step 4: Randomly choose $\alpha \in Z_q$ and U'_A to set $R_i^* = -k^{-1}(hQ_A + U'_A) + \alpha P$
Step 5: Finally, the adversary computes $U^* = k\alpha V^* Y_A + lP$ and $U^*_A = U'_A$
Step 6: The resultant blind signature on message m is $(U^*, U^*_A, R^*_i, r^*, V^*)$

In the following, we show that the forged signature $(U^*, U^*_A, R^*_i, r^*, V^*)$ is valid.

Since:

$$e(Y_A, h^*Q_A + U^*_A)^{V^*} e(Y_B, R_i^*)^{V^*} r^* = e(Y_A, h^*Q_A + U^*_A)^{V^*} e(Y_B, -k^{-1}(hQ_A + U^*_A) + \alpha P)^{V^*} r^* = e(\alpha k V^* Y_A + lP, P) = e(U^*, P)$$

According the above equation, we know that the forged signature can pass verification equation of signature. It means that our forgery is valid.

By the same way, we also show that the original signer can also produce a forgery in name of the proxy signer but it has not delegate the right to the proxy signer. The main reason to produce such attack is that R_i in the signature is freedom and Y_B (or Y_A) can been randomly chosen.

Attack on forward security: In Sun et al's scheme, they claimed that their scheme satisfies forward security. Namely, the adversary obtains the *i* period proxy signing key (R_i, S_{Pi}), he cannot fore the valid proxy blind signature in the j ($j<i$) period. In the following, by analyzing the scheme, we will show that the scheme doesn't satisfy forward security.

According the key update, we know that:

$$R_i = R_{i-1} + r_i Q_B,\ S_{pi} = S_{pi-1} + r_{i-1} S_B$$

Thus, we have:

$$R_i = R_0 + (\sum_{i=1} r_i) Q_B, S_{Pi} = r_0 S_B + V_A \sum_{i=1} r_i S_B$$

CONCLUSION

As an important cryptographic primitive, Proxy blind signature not only has the advantages of blind signature and proxy signature but also has some new features, it

can solve many practical problems and has wide applications. To realize efficient management and solve key escrow problem, Researchers gave an efficient certificateless proxy blind signature scheme with forward security. And they claimed that their scheme was secure. However, by our analysis, we show that the scheme is insecure, it exists unforgeable attack and also not provides forward security. Finally, the corresponding attacks are given and we also analyze the reason to produce such attack.

ACKNOWLEDGMENT

This study was supported partly by Beijing Natural Science Foundation (No. 4122024).

REFERENCES

Al-Riyami, S.S. and K.G. Paterson, 2003. Certificateless public key cryptography. Lecture Notes Comput. Sci., 2894: 452-473.

Chaum, D., 1983. Blind Signature for Untraceable Payments. Plenum Press, New York, pp: 199-203.

Lin, W.D. and J.K. Jan, 2000. A security personal learning tools using a proxy blind signature scheme. Proceedings of the International Conference on Chinese Language Computing, July 2000, USA., pp: 273-277.

Mambo, M., K. Usuda and E. Okamoto, 1996. Proxy signatures for delegating signing operation. Proceedings of the 3rd ACM Conference on Computer and Communications Security, March 14-15, 1996, New Delhi, India, pp: 48-57.

Sun, H.M. and B.T. Hsieh, 2004. On the security of some proxy blind signature schemes. Proceedings of the 2nd Workshop on Australasian Information Security, Data Mining and Web Intelligence and Software Internationalisation, January 2004, Dunedin, New Zealand, pp: 75-78.

Sun, J., J. Wei and P. Wei, 2011. New forward-secure certificateless proxy blind signature scheme. Proceedings of the IEEE 3rd International Conference on Communication Software and Networks, May 27-29, 2011, Xi'an, Shaanxi, China, pp: 496-499.

Wang, S.H., G.L. Wang, F. Bao and J. Wang, 2005. Cryptanalysis of a proxy blind signature scheme based on DLP. J. Software, 16: 1234-1239.