IMPROVED PROXY SIGNATURE SCHEME BASED ON SCHNORR'S SCHEME WITH ECC

Asif uddin khan.[1] NIT Bhubaneswar

Banamali Dinda.[2] KEC Bhubaneswar.

Jayakrushna Sahoo.[3] CIT Bhubaneswar.

Abstract :
To overcome the security weaknesses of the strong proxy signature scheme by Lee et al, in this paper we have presented an improved scheme. The security is enhanced by using ECC public key cryptography for authentication. The analysis shows that this scheme resolves the security problem arised in Lee et al scheme.

Keywords *:proxy signature, public key cryptography, ECC, Digital signature, Authentication, Cryptanalysis.*

1.Introduction

In distributed environment digital signature plays a vital role. By using digital signature [1,2,3] the transmission of messages on internet can achieve authenticity, data intigrity and non-repudiation. The traditional hand writing are replaced by using digital ones.
The proxy signature scheme was introduced by Mambo et al in 1996[4]. It allows an entity called original signer to delegate his signing capability to another entity called proxy signer. When the original signer let say A is busy, he delegates his signing capability to proxy signer let say B. proxy signer B signs the documents on behalf of A on his absence. Since it is proposed the prosy signature scheme have been suggested for use in many applications particularly in distributed computer where delegation of rights is quite common. In 1996 many proxy signature schemes were proposed [4,5,6,7] all of which based on schnorr's signature scheme[3]. According to the

undeniability property the proxy signature schemes are classified in two catagories ie Strong proxy signature scheme and week proxy signature scheme[7].
Strong proxy signature scheme represents both original and proxy signer's signature. Ones a proxy signer creates a valid proxy signature he can't repudiate his signature creation against any one.week proxy signature scheme represents only original signer's signature.
Based on delegation type proxy signature schemes are devided into full delegation, partial delegation and delegation by warranty. Since the proxy signature appears it attracts many researchers great attention. In [7] B. Lee, H.Kim and K.Kim also proposed a strong proxy signature scheme.

This paper is structured as follows:-
In section-2 we have presented a brief overview of schnorr's scheme[3]. In section-3 review of Lee et al strong proxy signature scheme is given. In section-4 attack on Lee et al scheme is given .In section-5 we propose our improved scheme. In section-6 we have compared the improved scheme with the Lee et al scheme and in section-7 we have analyzed the improved scheme and in section-8 we conclude.

2. Review of schnorr's scheme[3]

Schnorr's scheme works as follows:
Let p & q be larger primes with $q \mid p-1$. let g be a generater of a multiplicative subgroup of Z_p^* with order q, H(.) denote a collision resistant hash function.
A signer A has a private key $x_A \varepsilon Z_p^*$ and corresponding public key $y_A=g^{xA} \bmod p$. To sign a message M A acts as follows.
i. choose a random $k \varepsilon Z_q^*$
ii. compute $r = g^k \bmod p$
and $s=k+x_A H(M,r) \bmod q$.
iii. define the signature on M to be the pair (r,s).
The signature is defined by checking that $g^s=ry_A^{H(M,r)} \bmod p$. (1)

3. Lee et al strong proxy signature scheme.

This scheme has been introduced in[7]. It is based on the above schnorr's scheme.
Suppose that the original signer A has key pair (x_A,y_A) with x_A as private key and $y_A =g^{xA} \bmod p$ his public key. The proxy signer B also has his own key pair (x_B,y_B) with x_B private key and $y_B=g^{xB} \bmod p$ public key.

3.1 generation of proxy key

The original signer A uses schnorr's scheme to sign warrant information M_w which specifies what kind of

Manuscript received August 5, 2010
Manuscript revised August 20, 2010

messages A will allow the proxy signer B to sign on his behalf.
A Chooses at random $k_A \varepsilon Z_q^*$ and computes $r_A=g^{kA}$ mod p and $sA=k_A+x_AH(M_w,r_A)$ mod q. Signer A sends (M_w,r_A,s_A) to proxy signers B secretly.
After B gets $(M_w\ r_A\ s_A)$ he verifies the validity of schnorr's signature by checking the following equation $g^{sA}=r_Ay_AH(M_w,r_A)$ modp. (2)
If equation(2) holds B computes his proxy key pair as follows
The private proxy key
$x_p=x_B+s_A$
and public proxy key is $y_p=g^{xp(}=y_Br_Ay_A^{H(M_w,rA)}$ (3))mod p (4)

3.2 Proxy signature generation

To create a proxy signature on a message M conforming to the warrant information M_w, proxy signer B uses Schnorr's signature scheme with keys (x_p, y_p) and obtains a signature (r_p,s_p) for the message M. The valid proxy signature will be the tuple (M,r_p,s_p,M_w, r_A).

Verification
A receipient can verify the validity of the proxy signature by checking that M conforms to M_w and the verification equality of schnorr's signature scheme with public key $y_p(=y_Br_Ay_A^{H(Mw,rA)})$ mod p.
Accept the proxy signature if and only if $g^{sp}=r_p(y_Br_Ay_A^{H(Mw,rA)})^{H(M,rP)}$. (5)
holds.
The authors claimed that the scheme satisfies the following security
requirements [7]: strong unforgeability, verifiability, strong identifiability,
strong undeniability and prevention of misuse. In next section a new attack on Lee etal scheme is presented.

4. Attack on Lee etal scheme

In this section it is shown that if the original signer A is dishonest he can forge the signature of B on message M from a proxy signature.
After obtaining the proxy signature (M,r_p,s_p,M_w,r_A) the original signer A may forge B's signature on message M as follows.

1. First computes $s'=s_AH(M,r_p)$mod q.
2. Then computes $s_B=s_p-s'$mod q
3. and take $r_B=r_p$.

Then (r_B,s_B) and M satisfies equation (1) ie $g^{SB}=r_By_B^{H(M,rB)}$ mod p
suppose that $r_B = r_p = g^{kp}$ mod p and $S_p=k_p + X_pH(M,r_P)$ mod q
Where kp is the random number generated by B for proxy signature on M then A can compute the following to find s_B.
A computes s_p-s'
$=k_p+x_pH(M,r_P)$modq-$s_AH(M,r_P)$ mod q
$=k_p+(x_B+s_A)H(M,r_p)$modq-$s_AH(M,r_p)$mod q
$=k_p+x_BH(M,r_p)$mod q + $s_AH(M,r_p)$mod q-$s_AH(M,r_p)$mod q
$=s_B$.
So it is obvious that (*rB; sB*) is B's Schonrr signature for message *M:*
In other words, (M, r_B, s_B) is the forged B's signature on message *M*.
Remark. J. Herranz et al.[8] claim that other signature schemes (El-
Gamal signature or DSS) can be used in Lee etal strong proxy signature
scheme. It should be noted that this attack works as well if DSS is used.

5. Our Improved Scheme

Since the Lee etal scheme is suffered from forging attack by the original signer so we have improved this scheme and given a new scheme which is free from forgeability attack and secure in every aspect. We use ECC[10] public key algorithm to provide authentication.
The original signer A has a key pair (x_A,y_A) with x_A A's private key and y_A as A's public key where $y_A=g^{xA}$ mod p and another key pair based on ECC scheme ie ECC[10] public key Q_A and private key d_A.
Proxy signer B's key pair (x_B,y_B) with x_B private key and y_B public key where $y_B=g^{xB}$mod p and ECC key pair ie ECC public key Q_B and private key d_B.Let $Ed_B(\ )$ be a symbol for encryption using private key and $DQ_B(\ )$ be the symbol for decryption using public key based on ECC scheme.

5.1 Generation of proxy key and authentication code

Let M_w warrant information which specifies what kind of messages A will allow the proxy signer B to sign on his behalf .
Steps:

1. A chooses at random $k_A \varepsilon Z_q^*$ and computes $r_A = g^{kA}$ mod q and $s_A = k_A + x_AH(M_w, r_A)$ mod q,
2. A encrypts s_A, ie $s_A'=Ed_{A(}s_{A)}$.
3. signer A sends $(M_w,r_A,s_A',_{SA)}$ to proxy signer B secretly.

after B gets $(M_w,r_A,s_A',_{SA)}$ he computes $DQ_{A(}s_A',_{)}$ and verifies the validity of schnorr's signature scheme by checking the following.

$s_A = DQ_{A(s_A')}$ (6)

$g^{sA} = r_A y_A H(M_w, r_A) \mod p$ (7)

if equation(6) and equation(7) holds B computes his proxy key pair (x_p, y_p) as follows.

$x_p = s_B + s_A$.

$y_p = g^{xp} = y_B r_A y_A^{H(Mw,rA)} \mod p$

5.2 proxy signature generation

The proxy signer B uses schnorr's scheme to create a proxy signature on a message M conforming to the warrant information M_w.

Steps:

1. B computes r_p, s_p for message M with x_p and y_p as key pair
2. Then he computes $s_p' = Ed_B(r_p)$
3. Now the valid proxy signature will be the tupple $(M, r_P, s_p', s_P, Mw, r_A)$

Verification

4. When the recipient gets $(M, r_P, s_p', s_P, Mw, r_A)$

First he computes $DQ_B(s_p')$ and verifies the validity of schnorr's signature scheme by checking the following

$s_p = DQ_B(s_p')$ (8)

and $g^{sp} = r_p (y_B r_A y_A^{H(Mw,rA)})^{H(M,rp)}$ (9)

if equation(8) and (9) holds the proxy signature is accepted.

6.Comparision of our improved scheme with Lee et al scheme:

In Lee et al scheme the original signer could compute easily s_B and therefore he could generate the proxy signer B's signature ie (M, r_B, s_B) which is B's forged signature.so this scheme is not secured against forgeability attack.

In our improved scheme in each phase we have used authentication using ECC[10] equation(8) which guarantees that B's proxy signature can not be forged.

7. Analysis of improved scheme:

The Lee et al scheme was suffering from forgeability attack by the original signer because he could determine s_B.Since in this scheme we have used the ECC encryption to encrypt s_A, s_P for A and proxy signer respectively in order to create authentication code by using their private key based on ECC it can not be forged.Therefore this scheme is secured against forgeability and other types of attacks

8. Conclusion:

In this paper we point out the drawbacks of Lee etal proxy signature scheme[7] and proposed a new proxy signature scheme based on Schnorr's scheme with RSA.We demonstrate that Lee etal scheme is insecure due to forgeability attack.our improved scheme removes all the weaknesses of Lee etal scheme and meets all the security aspects needed by proxy signature scheme.so the new scheme is more secure than the existing scheme.

References:

[1] T.ElGamal, *public key cryptosystem and a signature scheme based on discrete* . IEEE Trans. Inform. Theory, vol. IT-31, pp. 469-472, July 1985

[2] L.Harn, *New digitral signature scheme based on discrete logarithm*. Electron.Lett., vol, no. 5, pp. 296-298, Mar.1994.

[3] C.P. Schnorr, *Efficient signature generation by smart cards*. Journal of Cryptology,"vol.4, pp161-174,1991.

[4] M.Mambo, K.Usuda, and E.Okamoto, *Proxy signatures: Delegation of the power to sign messages*. IEICE Trans., 1996, E79-A, (9), pp. 1338-1354.

[5] S.Kim, S.Park, and D.Won, *Proxy signatures, revisited*. Proc. ICICS'97, Int. Conf. Information and Communications Security, 1997,(LNCS), Vol. 1334, pp.223-23

[6] W B Lee, C Y Chang, *Efficient proxy-protected proxy signature scheme based on discrete logarithm*, Proceedings of 10th Conference on Information Security, Hualien, Taiwan, ROC, 2000, pp 4-7

[7] B.Lee, H. Kim, and K. Kim. *Strong proxy signature and its applications*. The 2001 Symposium on Cryptography and Information Security (SCIS 2001) 2001.

[8] Cryptanalysis of threshold proxy signature scheme based on factoring. 2008 International Symposium on Information Science and Engineering.978-0-7695-3494-7/08, 2008 IEEE DOI 10.1109/ISISE.2008.170

[9] cryptography and network security by william stallings.

[10]http://www.tataelxsi.com/whitepapers/ECC_Tut_v1_0.pdf?pdf_id=public_key_TEL.pdf

Prof. Asif uddin khan: Received B.E degree in Computer Science & Engg. from C.V Raman College of Engineering, Bhubaneswar BPUT,India. M.Tech in Computer Science & Engg from IIIT Bhubaneswar, India. Served in both industry and Ecademics such as College of Engineering and technology (CET) Bhubaneswar, Krupajal Engineering College(KEC) Bhubaneswar,Annova Technologies Hyderabad.Presently working as an Assistant Professor in the Department of Computer Sc & Engg, Nalanda Institute of Technoloy Bhubaneswar,India.Research interests includes Cryptography and Network security,Algorithms,Operating systems,Distributed systems, and Artificial Intelligence.

Prof. Banamali Dinda: Obtained BE in Computer science and Engineering from Utkal University ,Orissa,India. M.Tech in Computer science and engineering form BPUT Orissa, India.Presently working as an Assistant professor in the Department of computer science and enginering,Krupajal engineering College Bhubaneswar,India.Research area includes sensor Network,Network security.

Prof Jayakrushna Sahoo: Received M.Tech in Computer Science & Engg from IIIT Bhubaneswar, India.Presently working as an Assistant Professor in the Department of Computer Science and Engineering,Centurian Institute of Technology,Jatni,Bhubaneswar,India .Researh area includes Cryptography and Network security,Algorithms.