New Forgery Attack on Chang et al.'s signature scheme

Kou Li[1], Jin Ming[2,3]

[1]Information Engineering Department, SiChuan Tianyi College, Chengdu, China
[2]Statistical Department, Chengdu College of Information and Technology, Chengdu, China
[3]Laboratory of Information Security and National Computing Grid, Southwest Jiaotong University, Chengdu, China
jindaxia20080901@126.com, 948188514@qq.com

Abstract - Chang proposed one new digital signature scheme with message recovery and claimed the scheme is secure without using one-way hash function and message recovery. Two forgery attacks have been proposed to show that attackers who have a valid signature can forge signatures that can be verified validly on any uncontrolled messages by Fu. This paper proposes one new forgery attack scheme, which means that Chang et al.'s signature scheme is not secure.

Index Terms - Digital signature, forgery attack, cryptanalysis, hash function

1. Introduction

The advent of e-government and e-services is changing the way we do business. Traditionally, we created records on paper and we authenticated a record by signing it in ink. Today, technology is making both paper and ink irrelevant to many business processes. Therefore Digital signatures has become more and more important in the modern electronic data processing systems. Examples have been discussed in the literature[1-14]. In the digital signature scheme with message recovery, a legal receiver can recover the original message from the received signatures. The correctness of the recovered messages are usually checked by the message redundancy scheme. Moreover, one-way hash function and message recovery scheme are used to resist the forgery attacks at the cost of efficiency, and it may be troublesome.

Digital signature schemes are that allow a signer to transform any arbitrary message into a signed message. Then anyone can verify the validity of the signed message using the signer's public key, but only the signer can generate signed messages. Digital signature is very important in the information security and has numerous practical applications. A digital signature scheme with message recovery[3] is useful for some applications in which small messages should be signed. In [4], Shieh et al. proposed new efficient digital multi signature schemes. The required memory of local devices is greatly reduced. Further, one-way hash functions and message redundancy schemes are not used. However, Hwang and Li indicated that the underlying signature scheme with message recovery of Shiehet al.'s multisignature schemes suffers from some attacks because of the absence of one-way hash functions and message redundancy schemes[5]. They claimed that message redundancy schemes are still needed to resist forgery attacks.

C.C.Chang and Y.F.Chang proposed one new digital signature scheme with message recovery without using one-way hash function and message redundancy scheme[1]. Unfortunately, due to the absence of one-way hash and message redundancy, Chang et al.'s scheme suffer from the forgery attacks. In paper[2], two forgery attacks are proposed to show that attackers who have a valid signature can forge signatures that can be verified validly on any uncontrolled messages. One new forgery attack is proposed in the paper which mean it may necessary to use one-way hash functions and the message redundancy schemes to overcome these attacks.

The rest of the paper is organized as follows. In the second section, we briefly review Chang et al:'s signature scheme. In the third section, one new forgery attacks are proposed that can successfully forge signatures. The last section is the conclusion.

2. Review of Chang et al:'s Signature Scheme

Firstly review Chang et al:'s signature scheme without using one-way hash function and message redundancy scheme in brief. The scheme consists of two phases: signature-generation phase and verification phase. Through our paper, we use the same notation as in the previous works.

p : a large prime number
g : a primitive element in Zp
(x,y): user U's private and public key pair.
where gcd(x, p- 1) = 1, and $y = g^x \bmod p$.
M: the message to be signed
V : the verifier.
Signature-Generation Phase:
Suppose user U wants to sign the message M. Then U dose the following steps:

Step 1 U computes $s = y^M \bmod p$,

Step 2 U chooses a random number k in [1, p-1],

computes $r = Msg^{-k} \bmod p$.

Step 3 U computes t, where

$$s + t = x^{-1}(k - r)(\bmod(p - 1))$$

step 4 U sends the signature (r,s,t) of M to the verifier V,
Verification Phase:
After receiving the signature (r,s,t), V performs as following.

Step 1 V computes:

$$M' = y^{s+t} r g^{r} s^{-1}$$
$$= g^{x(s+t)} M s g^{-k} g^{r} s^{-1}$$
$$= g^{k-r} M g^{-k+r} (\mathrm{mod}\ p)$$

step 2 V checks whether $s = y^{M}$ mod p.

If it holds, V is convinced that (r, s, t) is the signature generated by U of the recovered message.

The following section is aimed at finding forgery attack scheme to show the Chang et al:'s signature scheme is not secure.

3. One new Forgery Attacks Way on Chang et al:'s Signature Scheme

In this section, one new forgery attack is proposed to show that Chang et al.'s signature scheme is not secure and forged easily.

Assume A is an attacker and suppose that A already had a valid signature (r,s,t) generated by the legal signer U of the message M. Then, A can forge valid signature (r', s', t') as following forgery attack.

A Randomly chooses $r', a, b \in z_p^*$,

A Computes:

$$M = y^{a*b} r' g^{r'} \bmod p$$

$$s' = y^{M} \bmod p \quad t' = a*b - s' + M \bmod (p-1)$$

(r', s', t') is a forged signature of message M.

And (r', s', t') is a valid signature of message M, because:

$$M' = y^{s'+t'} r' g^{r'} (s')^{-1}$$
$$= y^{a*b} y^{M} r' g^{r'} y^{-M}$$
$$= y^{a*b} r' g^{r'}$$

Thus, $y^{M'} = y^{M} = s \bmod p$, (r', s', t') is a valid signature of message M.

4. Conclusion

One new forgery attack is proposed to show that Chang et al:'s signature scheme without using one-way hash function and message redundancy scheme is not as secure as thy claimed, and the signature can be forged on any uncontrolled messages easily. To overcome these attacks, how to set up a safe digital signature scheme without using hash functions and message redundancy is still a serious academic problem.

Acknowledgment

The work is supported by the by Scientific Research Fund of SiChuan Provincial Education Department(No:10SB095), National Statistical Research Program(No: 2012LY007), Annual Statistics Information Technology and Key Laboratory of Data Mining Program(No:SDL201207)

References

[1] Chang C C,Chang Y F(2004). Signing a digital signature without using one-way hash functions and message rudundancy schemes.IEEE Commun Lett, 8(8): 485-487.

[2] FU X T, XU C X, XIAO G Z(2004). Forgery attacks on Chang et al.'s signature scheme with message recovery. http://epring.iac.org.

[3] K. Nyberg, R.A(1995). Message Recovery for Signature Schemes Based on the Discrete Logarithm Problem, Proc. of Eurocrypt94.Springer-Verlag, LNCS 950, pp.182-193.

[4] S.P.Shih, C.-T. Lin, W.-B. Yang, H.-M. Sun.(2000). Digital multisignature schemes for authenticating delegates in mobile code systems. IEEE Trans. Veh. Technol, vol.49, pp. 1464-1473, July.

[5] S.-J. Hwang and E.-T. Li.(2003) Cryptanalysis of Shieh-Lin-Yang-Sun signature scheme. IEEE Commun. Lett, vol. 7, pp. 195-196, Apr.

[6] XuanHong,ChenKefei.(2009). Secure Multiple-Times Proxy Signature Scheme. Computer Standards and Interfaces, 31(2009), pp.19-23.

[7] Wang C T, Chang C C, Lin C H.(2000). Generalization of threshold signature an authenticated encryption for group communications. IEICE Transactions on Fundamentals, 2000, E83-A(6): 1228-1237.

[8] Kuo W-C, Chen M-Y(2005). A modified(t,n) threshold proxy signature scheme based on the RSA crypto-system. Information technology and applicatons, ICITA 2005, 2(4-7), 5769.

[9] Tan Z W, Liu Z J, Tang C M.(2003). A Proxy Blind Signature Schemes Based on DLP. Journal of Software,14(11): 1931-1935 (Ch).

[10] Zhang T, Wang Y M.(2004). Design of Several Partial Blind Signatures and the Security Analyse. Journal of Xidian University, 31(6): 963-966(Ch).

[11] Peng B,Yang Z K, Tan Y M.(2003). The Application of Blind Signature in E-Cash. Computer Engineering and Application,39(19): 31-33(Ch).

[12] Pointcheval D, Stem J.(2000). Security Arguments for Digital Signatures and Blind Signatures. Journal of Cryptology, 13(3):361-369.

[13] Long Yu, Li X-X, Chen K-F, Hongxuan.(2009). Distributed Certificateless Key Encapsulation Mechanism Secure Against the Adaptive Adversary. Journal of Shanghai Jiaotong University(Science). 14(1):102-106.

[14] Xiong H, Hua J, Chen Z, Li F(2011). On the security of an identity based multi-proxy signature scheme. Computer and Electrical Engineering, 37(2): 129-135.