Available online at www.sciencedirect.com

SciVerse ScienceDirect

Energy Procedia 17 (2012) 655 – 658

Energy Procedia

2012 International Conference on Future Electrical Power and Energy Systems

Security of Analysis Liu's Signature Scheme

Shaoka Zhao[1], Chenglian Liu[2*]

Department of Mathematics and,Computer Science
Fuqing Branch of Fujian Normal University,Fuqing 350300 China
[1]strawboyzsk@163.com, [2]chenglian.liu@gmail.com

Abstract

In 2007, Liu proposed an improvement of Shieh et al. multi-signature scheme in mobile code system. There exist forgery attacks of multiplicative algebra method in his scheme. It is therefore insecure for his improvement. In this paper, we pointed out who do a forge attack successfully.

Keywords: Forgery attack, Algebra construction, Multiplicative property.

1. Introduction

People tend to communicate with each other on the internet through common but insecure channels. Because of this, proving the source and confirming the integrity of transmitted messages becomes an important issue. Making digital signatures is more significant than ever. Most internet applications require the help of digital signatures for authentication purposes, such as authenticating electronic tax reports, stock transactions, and electronic commerce deals. This is the major reason why digital signatures have become so valuable in the modern digital data processing world. Several important works dealing with digital signatures have been proposed in [1] [2] [3] [4] [5] [6]. In Shieh et al. scheme [7], the required memory for local devices is greatly abridged. They do not use message redundancy or one-way hash functions. However, Hwang pointed out the underlying signature from the forgery attack [8]. Wu [9] demonstrated some insider forgery attacks. Recently, Chang and Chang [10] presented a new digital signature without using one-way hash functions or message redundancy and claimed that their scheme modified the properties of Shieh et al. scheme. Afterward, Zhang [11] showed that Chang et al.'s version was still vulnerable to forgery attacks. Liu [12] improved the signature which is based on Shieh's scheme using neither one-way hash functions nor message redundancy. In this paper, we point out a leak in Liu's

* Corresponding Author: Mr. Liu is an associate professor with Fuqing Branch of Fujian Normal University.
Email:chenglian.liu@gmail.com ;Tel:+86-13960971195.

 doi:10.1016/j.egypro.2012.02.150

signature scheme that shows it is not secure. Section 2 briefly reviews Liu's improvement signature scheme. Section 3 is our attack method. A conclusion will be drawn in Section 4.

2. Review of Liu'S Signature Scheme

2.1 Liu's Scheme

There are two public system parameters, p and g, where p is a large prime and g is a primitive element in GF(p). Each user selects his private key xi and computes his public key

$$y_i \equiv g^{x_i} \pmod{p}. \tag{1}$$

with $\gcd(x_i, p-1) = 1$. Each user agrees upon the same system parameters p and g. Liu's underlying digital signature scheme is composed of two phases: the signature generation phase and the verification phase. Here, we use the same notation as in [12].

2.2 Signature Generation Phase:

Step 1. U_i computes

$$s_i \equiv (y_i)^{m_i} \pmod{p}. \tag{2}$$

Step 2. U_i randomly selects an integer number ki in [1, p-1] and computes

$$r_i \equiv m_i \cdot g^{-k_i s_i} \pmod{p}. \tag{3}$$

Step 3. U_i computes ti, where

$$(s_i \cdot t_i) \equiv [-s_i^2 + s_i x_i^{-1} \cdot (k_i - r_i)] \pmod{p-1}. \tag{4}$$

Step 4. U_i sends the signature $(s_i; r_i; t_i)$ of mi to the verifier V .

2.3 Verification Phase:

Step 1. V computes

$$\begin{aligned} m_i' &\equiv (y_i)^{(s_i t_i)} \cdot r_i \cdot (y^{r_i})^{s_i} \cdot (y_i)^{s_i^2} \\ &\equiv (g^{x_i})^{(s_i t_i)} \cdot r_i \cdot y^{r_i s_i} \cdot g^{s_i^2 x_i} \\ &\equiv (g^{x_i})^{-s_i^2 + s_i x_i^{-1}(k_i - r_i)} \cdot r_i \cdot g^{r_i s_i} \cdot g^{s_i^2 x_i} \\ &\equiv g^{si(k_i - r_i)} \cdot m_i \cdot g^{-k_i s_i} \cdot g^{r_i s_i} \\ &\equiv g^{si(k_i - r_i)} \cdot m_i \cdot g^{s_i(-k_i + r_i)} \\ &\equiv m_i \pmod{p}. \end{aligned} \tag{5}$$

Step 2. V checks whether

$$s_i \equiv (y_i)^{m_i} \pmod{p}. \tag{6}$$

If it holds, V can be convinced that $(s_i; r_i; t_i)$ is indeed the signature generated by U_i in the recovered message m_i'.

3. Our Attack

In this section, we assume that si is relatively prime to (p-1). Then the equation for the signature generation can be modified as the new equation

$$x_i (t_i - s_i) \equiv (k_i - r_i) (\text{mod } p-1). \tag{7}$$

A universal forgery attack by chosen message attack is given below. Suppose that an attack has a signature (s_i; r_i; t_i) on some chosen message m_i, where mi is relatively prime to (p-1). Now the attacker Eve wants to forge a signature (s_i', r_i', t_i') on some message m_i'.

Step 1. Eve computes

$$\delta \equiv \left(m_i' / m_i\right) (\text{mod } p-1). \tag{8}$$

Here assume that δ is relative prime to (p-1). Cause (p-1) contains a large prime factor, it is possible that δ is relative prime to (p-1).

Step 2. Eve computes

$$r_i' \equiv \delta r_i (\text{mod } p), \tag{9}$$

$$s_i' \equiv \delta^{-1} s_i (\text{mod } p-1), \tag{10}$$

And

$$t_i' \equiv \delta(t_i - s_i + s_i') (\text{mod } p-1). \tag{11}$$

The following shows why this attack can work successfully.

Proof:

$$\begin{aligned} m_i' &\equiv (y_i)^{s_i' t_i'} (r_i') \left(y_i^{r_i'}\right)^{s_i'} (y_i)^{s_i'^2} \\ &\equiv (y_i) \delta^{-1 s_i t_i'} (\delta r_i) y_i^{r_i s_i} (y_i)^{s_i^2 \delta^{-2}} \\ &\equiv \delta m_i \\ &\equiv m_i (\text{mod } p-1). \end{aligned} \tag{12}$$

4. Conclusion

We proposed an forgery attack to Liu's signature scheme which it existed an algebra construction leakage of multiplicative. In our method, we successfully forged a valid signature to cheat Liu's scheme. It is therefore that the Liu's scheme cannot against forgery attack.

Acknowledgements

The authors would like to thank anonymous reviewers for their valuable comments. This research is partially supported by the National Natural Science Foundation of China under Grant No. 61103247, and the Fuqing Branch of Fujian Normal University of China under the contract numbers KY2010-030 and KY2008-022.

References

[1] T. ElGamal, 'A Public Key Cryptosystem and a Signature Scheme Based On Discrete Logarithm,' IEEE Transaction on Information Theory, Vol. IT-31, pp.469-472, July 1985.

[2] L. Harn, 'New Digital Signature Scheme Based on Discrete Logarithm,' Electronics Letters, Vol. 30, No. 5, pp. 296-298, Mar. 1994.

[3] S.-J. Hwang, C.-C. Chang, and W.-P. Yang, 'An Encryption Signature Scheme with Low Message Expansion,' J. Chinese Inst. Eng., Vol. 18, No.4, pp. 591-595, Sept. 1995.

[4] K. Nyberg and R.-A. Rueppel, 'Message Recovery for Signature Schemes Based on the Discrete Logarithm Problem,' In Proc. Eurocrypt'94, Perugia, Italy, May 1994, pp. 182-193.

[5] J. M. Piveteau, 'New Signature Scheme with Message Recovery,' Electronics Letters, Vol. 29, No. 25, pp. 2185-2185, Dec. 1993.

[6] Z. Shao, 'Signature Scheme Based on Discrete Logarithm Without Using One-way Hash Function,' Electronics Letters, Vol. 34, No. 11, pp. 1079-1080, May 1998.

[7] S.-P. Shieh, C.-T. Lin, W.-B. Yang and H.-M. Sun, 'Digital Multisignature Scheme for Authenticating Delegates in Mobile Code Systems,' IEEE Transaction on Vehicular Technology, Vol. 49, pp.1464-1473, July 2000.

[8] S-J. Hwang and E.-T. Li, 'Cryptanalysis of Shieh-Lin-Yang- Sun Signature Scheme,' IEEE Communications Letters, Vol. 7, No. 4, April 2003.

[9] T.-C. Wu and C.-L. Hsu, 'Cryptanalysis of Digital Multisignature Scheme for Authenticating Delegates in Mobile Code Systems,' IEEE Transaction on Vehicular Technology, Vol. 52, No. 2, pp.462-465, March 2003.

[10] C.-C. Chang and Y.-F. Chang, 'Signing a Digital Signature Without Using One-Way Hash Functions and Message Redundancy Schemes,' IEEE Communication Letter, Vol. 8, No.8, pp.485-487, August 2004.

[11] F. Zhang, 'Cryptanalysis of Chang et al. Signature Scheme with Message Recovery,' IEEE Communication Letter, Vol. 9, No. 4, pp. 358-359, April 2005.

[12] C. Liu, 'An Improvement of Shieh et al.'s Multi-Signature Scheme in Mobile Code Systems,' The 17th Cryptology and Information Security Conference (CISC 2007), Chiayi, Taiwan, August 2007.