Journal of Applied Sciences

ISSN 1812-5654

science alert

ANSInet
an open access publisher
http://ansinet.com

Journal of Applied Sciences 5 (4): 794-797, 2005
ISSN 1812-5654

Cryptanalysis of Security Enhancement for Anonymous Secure E-voting over a Network

[1]Chou-Chen Yang, [2]Hung-Wen Yang and [2]Ren-Chiun Wang
[1]Department of Management Information System, National Chung Hsing University,
250 Kuo Kuang Road, 402 Taichung, Taiwan, Republic of China
[2]Department of Information Management, Chaoyang University of Technology,
168 Gifeng E.Rd., Wufeng, Taichung County, Taiwan 413, Republic of China

Abstract: In 1998, Mu and Varadharajan proposed an anonymous secure e-voting scheme over a network. Unfortunately, many researches have pointed out that Mu and Varadharajan's scheme was not secure. Attackers can easily forge a valid ballot and can vote more than once. Later, Lin *et al.* proposed a scheme that improved upon Mu's scheme. Lin *et al.* claimed that their scheme can not only prevent double voting but can also defend against attacks from conspiring parties. In this study, we shall show that Lin *et al.* scheme still can not prevent double voting and can not detect forged ballots. A voter can vote more than once without being detected. Moreover, an attacker can forge valid tickets and pass the verification of authentication server.

Key words: Cryptography, electronic voting, blind signature, ElGamal public key cryptosystem

INTRODUCTION

Voting is one of the most important activities in a democratic country. In a traditional voting environment, many eligible voters, for whatever reasons, give up their right by not voting. One of the reasons may be that an overwhelming majority has no time to vote. In addition to that, traditional voting requires considerable expenses. To raise the voting rate and to save expenses, David[1] first introduced the concept of electronic voting and the concept of blind signatures[2]. In recent years, more and more research has been conducted on secure electronic voting systems. Secure electronic voting must be achieved to ensure democracy, accuracy, privacy, mobility and efficiency[3].

Yi and Vijay[4] proposed an anonymous secure electronic voting scheme which is based on the ElGamal digital signature algorithm. They claimed that the scheme can not only prevent double voting but can also protect the privacy of voters. Unfortunately, Lin *et al.*[5] and Chien[6] pointed out that the weaknesses of Mu-Varadharajan's scheme are that a voter's identity can be easily traced and that the scheme can not detect double voting or forged tickets.

To enhance security in Mu-Varadharajan's scheme's, Lin *et al.*[5] corrected the weaknesses in Mu-Varadharajan's scheme and declared that their improved scheme overcame the weaknesses of Mu-Varadharajan's scheme. However, in this study, we shall show that, despite Lin *et al.*[5] improvement, their scheme still cannot detect forged tickets.

REVIEW OF LIN *et al.* E-VOTING SCHEME

There are three phases in Lin *et al.*[5] e-voting scheme: the ticket obtaining phase, the voting and ticket collecting phase and the ticket counting phase. In this study, the following abbreviations are used: AS-authentication server; VS-voting server; TCS-ticket counting server; CA-certificate authority; V-voter. Furthermore, each participant owns a RSA[7] key pair $\{e_x, d_x\}$, where x denotes the participant in the election; for example, a voter's public key and private key are represented by $\{e_v, d_v\}$.

The ticket obtaining phase

Step 1: A voter chooses two blind factors, b_1 and b_2 and two random numbers, k_1 and r. Furthermore, the voter can compute three are shown below equations with these parameters as follows:

$$E_1 = g^r b_1^{e_{AS}} \bmod n_{AS}$$

$$E_2 = g^{k_1} b_2^{e_{AS}} \bmod n_{AS}$$

$$E_3 = (E_1 \| E_2 \| TS)^{d_V} \bmod n_V$$

Corresponding Author: Hung-Wen Yang, Department of Information Management, Chaoyang University of Technology, Information Security Research Center (M317), Taiwan, Republic of China
Tel: +886 4 2332 3000/4169 E-mail: s9214605@mail.cyut.edu.tw

where, $g \in Z_p^*$ is a public parameter, TS denotes a timestamp and || denotes a concatenation of bits. Finally, the voter sends the following message to AS.

$$V \rightarrow AS: \{V, AS, Cert_V, TS, E_1, E_2, E_3\}$$

Step 2: When AS receives the message from the voter, AS first verifies whether the certificate is valid or not and validates the signature E_3. If all verifications are valid, then AS chooses a random number k_2 and computes the following equations:

$$E_4 = (k_2 \| TS)^{e_V} \bmod n_V$$

$$E_5 = (E_1 \cdot AS)^{d_{AS}} \bmod n_{AS}$$

$$= (a \cdot AS)^{d_{AS}} \; b_1 \bmod n_{AS}$$

$$E_6 = (E_2 \cdot g^{k_2} \cdot AS)^{d_{AS}} \bmod n_{AS}$$

$$= (y_1 \cdot AS)^{d_{AS}} \; b_2 \bmod n_{AS}$$

$$E_7 = (E_2^2 \cdot g^{k_2} \cdot AS)^{d_{AS}} \bmod n_{AS}$$

$$= (y_2 \cdot AS)^{d_{AS}} \; b_2^2 \bmod n_{AS}$$

$$E_8 = (E_5 \| E_6 \| E_7 \| TS)^{e_V} \bmod n_V$$

where, $a = g^r$, $y_1 = g^{k1+k2}$, $y_2 = g^{2k1+k2}$. AS records k_2 and the voter's identity in the database. Finally, AS sends the following message to the voter.

$$AS \rightarrow V: \{AS, V, E_4, E_8\}$$

Step 3: When the voter receives the message from AS, the voter decrypts E_4 to obtain k_2. Therefore, the voter can compute the parameters y_1 and y_2 using $y_1 = g^{k1+k2}$ and $y_2 = g^{2k1+k2}$ and can calculate the signatures using the following equations:

$$S_1 = E_5 \cdot b_1^{-1} \bmod n_{AS}$$

$$= (a \cdot AS)^{d_{AS}} \bmod n_{AS}$$

$$S_2 = E_6 \cdot b_2^{-1} \bmod n_{AS}$$

$$= (y_1 \cdot AS)^{d_{AS}} \bmod n_{AS}$$

$$S_3 = E_7 \cdot b_2^{-2} \bmod n_{AS}$$

$$= (y_2 \cdot AS)^{d_{AS}} \bmod n_{AS}$$

Step 4: In this step, the voter signs the polling content m using the following equations:

$$S_4 = X_1^{-1} (ma - r) \bmod p-1$$

$$S_5 = X_2^{-1} (ma - r) \bmod p-1$$

where, $X_1 = k_1 + k_2$, $X_2 = 2k_1 + k_2$.
Finally, the voting ticket is composed as follows:

$$T: \{S_1 \| S_2 \| S_3 \| S_4 \| S_5 \| a \| g \| y1 \| y2 \| m\}$$

The voting and ticket collecting phase

Step 1: The voter sends the ticket T to the voting system VS.

Step 2: VS verifies the parameters a, y_1 and y_2 using the following equations:

$$AS \cdot a = S_1^{e_{AS}} \bmod n_{AS}$$

$$AS \cdot y_1 = S_2^{e_{AS}} \bmod n_{AS}$$

$$AS \cdot y_2 = S_3^{e_{AS}} \bmod n_{AS}$$

If the above equations are valid, then VS can go on to the next step.

Step 3: VS verifies whether the polling content's signatures are valid or not by checking the following equations:

$$g^{ma} \bmod p = y_1^{S_4} a \bmod p$$

$$g^{ma} \bmod p = y_2^{S_5} a \bmod p$$

If all the verifications are valid, VS can ensure that the ticket is valid. However, VS stores all the tickets in voting boxes. If a voting box is full, then VS sends it to TCS over the network.

The ticket counting phase: In this phase, detecting double voting and counting all the tickets are major tasks for TCS. TCS will check whether these parameters {a, y_1, y_2} have been used before. If these parameters

have been used, then TCS can compute the parameter k_2 as follows:

$$\frac{m'a-ma}{s_4'-s_4} \bmod p-1=X_1$$

$$\frac{m'a-ma}{s_5'-s_5} \bmod p-1=X_2$$

$$X_2-X_1=(2k_1+k_2)-(k_1+k_2)=k_1$$

$$X_1-k_1=k_2$$

When TCS obtains the parameter k_2, TCS can find the identity of the corresponding voter.

CRYPTANALYSIS OF LIN *et al.* E-VOTING SCHEME

In this section, we shall show that Lin's improved scheme still cannot detect a forged ticket. There are five equations used for checking in Lin's improved scheme, as shown below:

$$AS \cdot a = S_1^{e_{AS}} \bmod n_{AS} \quad (1)$$

$$AS \cdot y_1 = S_2^{e_{AS}} \bmod n_{AS} \quad (2)$$

$$AS \cdot y_2 = S_3^{e_{AS}} \bmod n_{AS} \quad (3)$$

$$g^{ma} \bmod p = y_1^{S_4} a \bmod p \quad (4)$$

$$g^{ma} \bmod p = y_2^{S_5} a \bmod p \quad (5)$$

If an attacker wants to forge a valid ticket, then he/she must forge these parameters: a, y_1, y_2, S_1, S_2, S_3, S_4 and S_5. First, the attacker chooses a prime number p_1 randomly. In Eq. 1, e_{AS} and p_1 are prime numbers, so the attacker can easily find u_1 and v_1 such that $u_1 \cdot e_{AS}-v_1 \cdot p_1=1$ using Euclid's algorithm, as the following theorem shows:

Theorem: If e and p are relatively prime, then we can find the integers u and v such that $e \cdot u-p \cdot v=1$[7].

Hence, the attacker can forge the parameters a and S_1 as follows:

$$S_1=AS^{u_1}$$

$$a=AS^{p_1 \cdot v_1}$$

The forged parameters still satisfy Eq. 1, as shown below:

$$AS \cdot a = S_1^{e_{AS}} \bmod n_{AS}$$

$$AS \cdot AS^{p_1 \cdot v_1} = AS^{u_1 \cdot e_{AS}} \bmod n_{AS}$$

$$AS^{1+p_1 \cdot v_1} = AS^{u_1 \cdot e_{AS}} \bmod n_{AS}$$

where:

$$e_{AS} \cdot u_1-p_1 \cdot v_1=1$$

$$e_{AS} \cdot u_1=1+p_1 \cdot v_1$$

Therefore, the attacker can refer to the above method to find the parameters p2, u_2, v_2,y_1, S_2, p_3, u_3, v_4, y_2 and S_3 to satisfy Eq. 2 and 3.

In Eq. 4, g is a public parameter, m is the attacker who wants to forge the polling content and y_1 and a have been forged previously. Hence, the attacker computes the parameter S_4 to hold Eq. 4. Obviously, the attacker has the ability to find the parameter S_4 with a very high probability, because it is different from computing a discrete logarithm in a finite field. The attacker just finds a value to satisfy Eq. 4. However, the attacker can refer to the above method to find the parameter S_5 to satisfy Eq. 5. To summarize briefly, an attacker can forge all the parameters that a valid ticket needs, so Lin's improved scheme still cannot detect a forged ticket.

In addition, Chien *et al.*[6] proposed attack on Mu-Varadharajan's scheme still applies to Lin's improved scheme. That is to say, the identity of a voter can still be traced as follows:

$$\frac{y_1^2}{y_2}=\frac{g^{(k_1+k_2)^2}}{g^{2k_1+k_2}}=k_2$$

Hence, the authorities can obtain the parameter k_2 and can trace the identity of the voter.

CONCLUSIONS

In this study, we have shown that Lin *et al.*[5] improved e-voting scheme cannot detect forged tickets. In other words, any malicious voters or attackers can forge a valid ticket without being authenticated and can vote more than once without being detected.

REFERENCES

1. David, C., 1981. Untraceable electronic mail, return address and digital pseudonyms. Communication of the ACM., 24: 884-888.
2. David, C., 1983. Blind Signatures Systems. Advances in Cryptology, CRYPTO'83, pp: 153-156.
3. Jan, J.K., Y.Y. Chen and Y. Lin, 2001. The design of protocol for e-voting on the Internet. In Security Technology, 2001 IEEE 35th Intl. Carnahan Conf., pp: 180-189.
4. Yi, M. and V. Vijay, 1998. Anonymous secure e-voting over a network. In Proceeding of the 14th Annual Computer Security Applications Conference, ACSAC'98, pp: 293-299.
5. Lin, I.C., M.S. Hwang and C.C. Chang, 2003. Security enhancement for anonymous secure e-voting over a network. Computer Standards and Interfaces, 25: 131-139.
6. Chien, H.Y., J.K. Jan and Y.M. Tseng, 2003. Cryptanalysis on muvaradharajans e-voting schemes. Applicied Mathematics and Computation, 139: 525-530.
7. Herstein, I.N., 1975. Topics in Algebra. Lexington Mass.: Xerox College.; Taipei: The Southeast Book Company.
8. Ron, R., S. Adi and A. Len, 1978. A method for obtaining digital signatures and public key cryptosystems. Communication of the ACM., 21: 120-126.