VULNERABILITIES OF E-VOTING SYSTEMS

Tohari Ahmad
Department of Informatics, Faculty of Information Technology,
Institut Teknologi Sepuluh Nopember
Gedung Teknik Informatika, Kampus Sukolilo Surabaya, Indonesia 60111
email: tohari@its-sby.edu

ABSTRACT

Practically, e-voting should comply with the social acceptance, technology and law. Many believe that e-voting is better than manual voting, as the former has less manual involvement. It is also believed that it is more secure and transparent. However, some security attacks may be launched which result in breaking both voting and e-voting requirements. In this paper, we discuss some aspects of the e-voting, especially from the security point of view.

Keywords: electronic voting, security, information security.

1 INTRODUCTION

Electronic voting (e-voting) has been applied in real systems, either small or large scales, despite its security issues. For example, it is used in Estonian public election [1]. In Indonesia, Jembrana district is preparing to be the first in carrying out this system for upcoming election [2]. Moreover, the Indonesian constitutional court has already approved it [3]. These support one of Hof's [4] arguments, namely the law, besides two other basic requirements: technology and social acceptance.

Additionally, the use of e-voting may increase the participation as it is relatively easier and faster than conventional system, even though it needs training for many users. Furthermore, it may also be cheaper in the long term use.

However, many parties still have a doubt whether the e-voting system is able to keep the election principle, namely: free, direct and fair. On the other hands, the system has to also meet the information security requirements, such as: confidentiality, integrity and authenticity. So, before employing the system in the real election, those two aspects must be met.

Overall, using this system, a legitimate user must be able to give his/her vote once (and only once) without being known and modified by others and counted as a legitimate vote. Therefore, the system must also be able to defend against illegitimate voters.

In this paper, we will briefly discuss vulnerabilities of the e-voting system and whether it is feasible to use. The rest of the paper is structured as follows. Section 2 provides the related works. Section 3 discusses the issues may arise. The paper is summarized in section 4.

2 RELATED WORKS

The detail of e-voting's requirements and principles is explained in [5, 6]. For the authentication process, [4] proposes to use biometrics. This is because biometrics is unique, stable and never forgotten. Yet, storing biometric information securely is also an issue as it can be a target of attacks.

Ahmad et al. [7] perform an experiment of mobile voting (m-voting) where the voters give their vote through a mobile device. This is more challenging because the mobile devices' capability is limited while the security level must be maintained. They encrypt the data being transmitted using ECC whose key is encrypted using AES; and also encrypt the data directly using ECC. Another ECC development in mobile devices is researched in [8]. A research in [9] proposes to use MSR for the encryption. It is believed that it is appropriate for the mobile device characteristics.

Security aspects of internet voting are discussed in [10, 11]. Some social aspects, such as costs, transparency and turnout, which have been pros and cons factors, are also provided.

Overall, various e-voting procedures and architectures have been proposed in [7, 9-12]. This will include some voting entities:

- Voter – who gives the vote
- Administrator – who checks voters' eligibility
- Counter – who count the votes
- Commissioner - who monitors the voting process

In [7], there are two counters which are independent each other as in fig 1. It is claimed that it can

ISSN 2085-1944

increase the fairness because counting is performed by more entities. In addition to those, third entities, such as the certificate authority, are involved in the system to increase the security. This is the extension of the anonymous-blind channels procedure [10].

3 DISCUSSION

Some aspects of e-voting systems can be analyzed from many points of view. Here, we will analyze it in term of security, transparency and verifiability. This will cover the election principle, especially for the fairness.

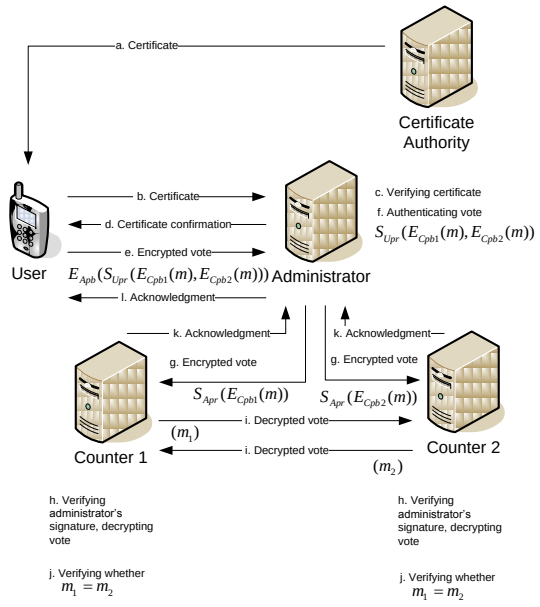

Figure 1 m-voting architecture [7]

3.1 Security

Security can be analyzed from several security properties, such as authenticity, confidentiality, integrity and privacy.

- **Authenticity**

The authentication can be done by employing biometrics. Different from other authentication tools, such as password and smart card, biometrics is believed to be more effective to prevent illegitimate users from committing an impersonation attack. This is because biometrics is not transferable, and its "liveness" can be checked to increase the security. More over, voters do not need to memorize and hold its biometric traits as password and smart card do. Password and smartcard can also be combined with biometrics to achieve high security. Technically, authentication can be developed either in passive, active, or basic access control as in the e-passport used [13].

For this authentication system, all voters have to register at first step by giving theirs biometric data to the administrator. A blind authentication mechanism should be used, as the system must be able to authenticate the voters but not revealing their identity.

However, biometrics data itself may be attacked by modifying, copying or deleting. Furthermore, this may also be vulnerable to privacy attacks. As biometrics data is the main key in the system, compromising it will affect the result. Moreover, biometric authentication may not be able to achieve 100% successful authentication as false acceptance and false rejection rates are still greater than zero due to intra-user variation and inter-user similarity.

To avoid this attack, some mechanisms can be implemented to protect the biometric data. For example, cancelable template, fuzz vault and fuzzy extractor. To increase biometrics performance, multi-modal biometrics may be used.

- **Confidentiality and privacy**

It relates to the secrecy of the votes, that is, only the respective voter knows what his/her vote is. It also means that a voter and his/her vote must be linked but there is no way to reveal what the vote for [4]. In addition, the voters' identity is also secret. Furthermore, if biometrics is used for the authentication tools, non-cross matching databases property should be kept.

Confidentiality may be achieved by encrypting the votes using cryptographic algorithms, such as MSR as in [9]. Privacy may be achieved by employing the homomorphic property [14] of the cryptographic algorithm used.

In general, cryptographic voting mechanisms are based on the Diffie-Hellman [15] and Rivest et. al [16] concepts, where each voter has a public key-pair for encrypting and signing the vote. This has been illustrated in fig. 1. The use of public key algorithms has made it easy for the system to distribute the key.

- **Integrity**

As shown in fig 1, integrity can be maintained by using multiple digital signatures. In [7], the message is signed by the voter and administrator before being counted. These signatures are applied to the encrypted message.

Blind signatures, which signatures are applied to the disguised message, can be developed by using Chaum's blinding [17]. An example of this mechanism is developed in [18] where a e-voting protocol is built in typed MSR..

3.2 Transparency

The voters should be able to check whether their votes are counted correctly. In case there is a dispute, the respective voter should be able to complain.

However, this may cause a trade-off between this and privacy properties that the link between voters and their votes must be blindly maintained. The procedure how the complain should be performed is also a dilemma as the voters should not have the proof to what they vote for but it is needed in this case. In the common DRE (Direct Recording Electronic) machines, the voters receive a verification paper as voters' confirmation. Besides using the voting procedure, this potential dispute problem may be solved by encrypting the verification paper which only the administrator is able to decrypt. This can minimize the possibility of vote buying.

3.3 Verifiability

By employing additive homomorphic encryption, the relation between entities in the message and cipher text spaces is kept. This can be performed by using public cryptographic algorithms, for instance El-Gamal encryption scheme [14].

Let m_1 and m_2 are groups of encrypted votes and f is a defined function. The aggregate votes can be illustrated as:

$$f(m_1 + m_2) = f(m_1) + f(m_2) \quad (1)$$

4 CONCLUSION

The implementation of an e-voting system may be able to increase the security, transparency and other voting properties' level. As mobile devices have been widely used in the community, for flexibility, e-voting may be extended into mobile voting.

However, some weakness may still appear for both in the concept and practice. The technology alone is not able to alleviate e-voting shortcomings. So, an appropriate architecture and procedure should also be applied concurrently.

REFERENCES

[1] Trechsel A H, and Breuer F (2006) Voting: E-voting in the 2005 local elections in Estonia and the broader impact for future e-voting projects. In: 2006 International Conference on Digital Government Research.

[2] Jembrana told to prepare for e-voting (2010). The Jakarta Post.

[3] Constitutional Court Clears Way for Electronic Voting (2010). Jakarta Globe.

[4] Hof S (2004) E-voting and Biometric System? In: Electronic Voting in Europe - Technology, Law, Politics and Society, Lake of Constance.

[5] Simidchieva B I, Marzilli M S, Clarke L A, and Osterweil L J (2008) Specifying and verifying requirements for election processes. In: International Conference on Digital Government Research 2008.

[6] Volkamer M, and McGaley M (2007) Requirements and Evaluation Procedures for eVoting. In: The Second International Conference on Availability, Reliability and Security.

[7] Ahmad T, Hu J, and Han S (2009) An Efficient Mobile Voting System Security Scheme based on Elliptic Curve Cryptography. In: IEEE IDSS-NDS, Network and System Security, Gold Coast, Australia, 2009.

[8] Light J, and David D (2008) An efficient security algorithm in mobile computing for resource constrained mobile devices. In: 4th ACM Symposium on QoS and Security for Wireless and Mobile Networks, Vancouver, Canada.

[9] Yi X, Cerone P, and Zhang Y (2006) Secure Electronic Voting for Mobile Communications. In: Vehicular Technology Conference 2006.

[10] Schryen G (2004) Security aspects of Internet voting. In: 37th Annual Hawaii International Conference on System Sciences.

[11] Kiayias A, Korman M, and Walluck D (2006) An Internet Voting System Supporting User Privacy. In: 22nd Annual Computer Security Applications Conference 2006 (ACSAC'06).

[12] Wang C, and Leung H F (2005) A secure voter-resolved approval voting protocol over internet. In: The 7th International Conference on Electronic Commerce, 2005.

[13] Vijayakrishnan, Pieprzyk J, and Wang H, Formal Security Analysis of Australian E-passport Implementation. In: 6th Australasian Information Security Conference (AISC 2008), Wollongong, Australia, 2008.

[14] Fontaine C, and Galand F (2007) A Survey of Homomorphic Encryption for Nonspecialists. EURASIP Journal on Information Security vol. 2007.

[15] Diffie W, and Hellman M E (1976) New Directions in Cryptography. IEEE Transaction on Information Theory 22: 644-654.

[16] Rivest R, Shamir A, and Adleman L (1978) A method for obtaining digital signatures and

public-key cryptosystems. Communication of the ACM 21: 120-126.

[17] Chaum D (1985) Security without identification: transaction systems to make big brother obsolote. Communication of the Association for Computing Machinery 28(10): 1030-1044.

[18] Balopoulos T, Gritzalis S, and Katsikas S K (2005) Specifying electronic voting protocols in typed MSR. In: 2005 ACM Workshop on Privacy in the Electronic Society.