International Journal of Advanced Computer Science and Information Technology (IJACSIT)
Vol. 1, No.1, October 2012, Page: 14-24, ISSN: 2296-1739

www.elvedit.com

Definitions and Criteria of CIA Security Triangle in Electronic Voting System

Authors

Saman Shojae Chaeikar
Department of Software Engineering, Islamic Azad University, Khorramabad Branch
saman_shoja@yahoo.com
Khorramabad, Iran

Mohammadreza Jafari
Department of Industrial Engineering, Payamenoor University
jafari_mohammadreza@yahoo.com
Khorramabad, Iran

Hamed Taherdoost
Department of Computer Engineering, Islamic Azad University, Semnan Branch
hamed.taherdoost@gmail.com
Semnan, Iran

Nakisa Shojae Chaei kar
Department of Software Engineering, Islamic Azad University, Khorramabad Branch
nks_shoja@yahoo.com
Khorramabad, Iran

Abstract

Confidentiality, Integrity, and Availability are three sides of the famous CIA security triangle. Since the e-voting systems are built from particular components, the CIA security triangle of these systems has particular definitions for each side. This paper presents these CIA security definitions and criteria which each state-of-the-art electronic voting system must meet based on the view point of National Institute of Standard and Technology (NIST) and also the criteria proposed by pioneer e-voting researchers. According to jurisdiction of different countries some of the given definitions and criteria might be excluded for developed e-voting system of their territory. Beside of the definitions and criteria, current threats and proposed solutions (in 2012) of each CIA triangle side and current unresolved security threats are concisely described.

Key Words

E-voting, Electronic Voting, CIA, E-Voting Confidentiality, E-Voting Integrity, E-Voting Availability.

I. INTRODUCTION

Today developed countries are benefit from the advantages of e-government systems and under development countries are moving toward replacing traditional government systems with electronic ones. Electronic voting system is one of the e-government sub-systems which can change destiny of its country, and even other countries, as its outcome will grant political, military, and economy power to the winner political party. Since the e-voting systems play vital role in future of the nations, they have to be secure enough against any fraud or attack. CIA is the famous security triangle which defines definitions and criteria which each secure system must meet.

Confidentiality is keeping sensitive data secret against unauthorized users. The most important way to achieve confidentiality is using cryptographic techniques like SSL or TSL [1], [4]. Access control also helps to grant access only to legitimate users. Integrity is assurance of originality of data and realizing any data alteration or tampering. Most important method to protect integrity is utilizing cryptographic techniques like SSL, TSL, MAC, or digital signature [1]. Availability is portion of time which a system must be active and available for its legitimate users. Most important factors for preserving system availability are capability of failure resiliency and DoS attack counter measures [1 , 2].

This paper concisely describes important properties which every e-voting system must have regardless of criteria of jurisdictions. The threats which endanger each side of the triangle are counted and solutions which can resolve or mitigate the threats effects are listed. For each CIA triangle side unresolved issues explain the current remained threats which endanger safety of the electronic voting systems and need more research endeavor to overcome.

II. CIA DEFINITIONS AND CRITERIA IN E-VOTING

There are particular criteria and definitions which describe each side of CIA triangle. Certain threats endanger safety of properties of each side and some techniques resolve or mitigate the threats which endanger these properties. Properties, threats, solutions and remained issues of each CIA side are described in following sections.

A. Confidentiality

Protection of confidentiality against illegitimate users and attackers is vital factor for e-voting systems as they store voters' authentication information, casted votes, passwords, and encryption/decryption keys inside and also may transmit them online. Two of e-voting systems critical confidentiality approaches are preserving ballot secrecy and banning voters' coercion. In traditional or mail-in systems corrupted staff will have chance of manipulating votes while by utilizing modern cryptographic schemes votes are ideally not alterable. Coercion also could be banned by letting voters to vote more than once. The main limitation for notion of multiple voting is the country's jurisdictions and support of developed machines [1].

1. Properties:

The main important confidentiality factors are privacy and autonomy. The following definitions help to achieve these main criteria.

- Ballot secrecy: content of the casted ballots must be kept secret against disclosure in the system.
- Protection of personal information: voter's identity must be kept secret against disclosure.
- *Receipt freeness*: the system should not let voters to proof content of their votes to any third party.
- Protection of secret data against disclosure: content of stored sensitive data must be comprehensible only for authorized administrators and election officials.
- Minimal storage: only vital data to keep the e-voting system in functioning mode must be stored.
- Minimal communication: transmitted data between components of the system must be kept in minimum.

2. Threats :

Following threats endanger safety of confidentiality of electronic voting systems.

Disclosure of stored central data: leaking central stored data will result in loss of secrecy of voters' private information. The main sources of secret data disclosure are insecure internet connection, unencrypted stored data, poor passwords and encryption, and poor key management.

Coercion: this confidentiality threat can be prevented by support of multiple voting and preserving secrecy of casted votes.

Trade of votes: public and private voting platforms are more in exposure of danger of buying and selling voters' credentials. To win an election, political parties can buy credentials to cast votes in favor of themselves. To mitigate danger of selling credentials, this information must be distributed in short time before voting [2].

Presence of malware on client machines: malwares can monitor voter's activities or even may change ballot content. A study revealed that up to 15% of voters' machines could be infected by malwares [3].

3. Solutions :

Following techniques and security measures would assist protecting confidentiality of the electronic voting systems.

Cryptography: encrypted data could be stored in the systems and transmitted over networks

safely. Various techniques like SSL or TSL can be utilized for data encryption/decryption. Proper selection of key management scheme would dramatically enhance confidentiality [4]-[7].

Advanced voting cryptographic techniques: these techniques are designed to let run a secure electronic election. These techniques will work properly if voters do not make any mistake and also no malware exist on the systems [4, 8-11].

Access control: access control will help to grant resources only to legitimate users. Users may try to access resources indirectly like using other software, other OS, or even through installed OS services. To ban indirect resources access the stored data should be encrypted and only be accessible through access control [1].

Separation of duties: to achieve higher security, procedural and technical mechanisms must be combined by sharing responsibilities among few legitimate users. In this way all of legitimate users must collude together to run an attack against the system [1].

4. Unresolved problems :

Despite all of the advances in security technology, confidentiality of e-voting systems still suffers from following problems:

- Secrecy of ballots in remote systems (authentication problem)
- Comprehensive cryptography technique to support different aspects
- Pre-distribution of cryptographic keys in advanced cryptosystems
- Coercion in remote e-voting systems
- Buy/sell of credentials in remote systems
- Secret data leakage

B. Integrity

In this field integrity deals with trustworthiness of both data and functions. In fact integrity is implementation of safeguards to ensure that data and software will not alter in unauthorized way. To protect stored data cryptographic techniques like public key, and to protect transmitted data cryptographic protocols like IPSec or TSL could be utilized [1].

1. Properties:

Integrity falls into two categories of data and software integrity. Data integrity is preserving integrity of ballot information and audit records. Software integrity is ensuring that only genuine software is running on the system components.

- Accuracy: election result is calculated only based on casted votes [12].
- Auditability: system behavior could be traced during and after election [12].

- Verifiability: result of election could be verified by auditors by provided system evidences.
- Public verifiability: public can verify outcome of election.
- Traceability: the electronic voting system will generate enough records to let officials trace root of problems.
- Recoverability: generated system records will let to recover from any loss of integrity.
- Protection against data alteration: the system should not allow unauthorized insertion, modification, and deletion of records.
- Logging data alteration: the system must generate enough logs to proof who has changed the data which might affect election result.
- Data authenticity: the system must generate enough evidence for auditors to show which record has been generated by which entity.
- Integrity of server software: both front-end and back-end components will run only authorized software.
- Authenticity of server software: to ensure protection against malware, auditors and administrators can verify whether only authorized software is installed.
- Choosing most appropriate software engineering model: chosen model is one of current best practices.

2. Threats:

The same as other systems, e-voting systems may suffer from system bugs which may result in integrity loss and affecting election outcome. Particularly public and private platforms are more vulnerable. Following items are the threats which endanger integrity of e-voting systems.

Software bugs: software bugs, the same as malicious codes, are one of main causes of integrity loss. On average every 1000 lines of code might have 15 to 50 errors [13] and by considering this fact that an e-voting system has tens of thousands of code lines then likeliness of existence of severe bugs is considerable. These bugs could be exploited by attackers to get control of the system or manipulating votes.

Server side malicious codes: malicious codes which may affect the election outcome might be installed on server even by administrators or IT staff.

Client side malicious code: since normally non expert people operate client machines, these systems are more prone to be compromised via malicious codes, worms, Trojans, or viruses. Attackers may try to take control of clients to alter votes or even use it as stepping stone to attack other clients.

Data and records alteration: due to vulnerabilities or compromised integrity attackers or even system administrators may alter stored data to affect the outcome.

3. Solutions:

Following techniques can help to solve or at least mitigate integrity threats.

Cryptography: some cryptographic techniques like Secure Socket Layer (SSL) or Transport Layer Security (TSL) can protect integrity of transmitted data and some like Message Authentication Code (MAC) or digital signature can protect integrity of stored data [1].

Advanced cryptographic techniques: end-to-end cryptographic voting techniques are designed to detect integrity breaches caused from alteration of casted votes. Some of these techniques also let voters to check if their votes are counted [1].

Utilizing voter side trusted hardware component: since personal and public computers always are in exposure of various types of security threats, a trusted hardware could be designed and distributed among voters as secure voting platform. In addition of e-voting, the trusted hardware also can be used as a multipurpose platform for e-commerce and other similar applications [1].

Malware detection and prevention systems: anti-malware programs by heuristic methods can detect presence of malicious programs based on their signatures. Despite these software are helpful programs but only are able to find known signatures and even sometimes they fail to remove found malwares. Distribution of updated anti-malware programs can enhance security but does not solve this issue [1].

Remote software verification: developed end-point scanning software help to scan computers in virtual private networks remotely to ensure they only run authorized software [14], [15].

Formal software verification method: this method lets to proof correctness of the developed codes mathematically. Since in this method every step should precisely be described as algorithm, this type of verification is very hard and costly. Only evaluation of particular applications, like military or avionic programs, by formal method is reasonable [16].

Bootable CD or DVD: to help voters to vote safely, the election officials can distribute bootable CDs or DVDs which contain required applications for safe vote casting among all of the voters. Voters can boot up their systems for casting safe votes by bootable disks to avoid danger of majority of security threats. This method is expensive, hard, and unsafe because mailing address of voters might not be updated, not all of voters receive their disks, not all of them may run correctly, and undistinguishable fraudulent CDs or DVDs might be distributed [1].

Virtual machines: to provide safe voting environment instead of CDs or DVDs, virtual machines can be utilized. The virtual machines take advantages of resources of host machines and does not require any configuration or driver. Danger of distribution of fraudulent images containing malicious codes and logistical difficulties of distribution of them are the main defects of this method [1].

Second channel: since security threats like malicious codes or viruses may endanger safety of casting votes, a secondary channel like telephone or SMS could be utilized for verification of casted votes. This method suffers from essential usability defects [1].

Unintelligible content for malwares: easy techniques like employing CAPTCHAs can help to ban malwares from alteration of votes. Since till now there is no malware kit which is able to

read CAPTCHAs, using CAPTCHAs would help to ensure no malware will vote instead of people [1].

4. Unresolved Problems:

Despite of all advances in security still there are severe defects like following items.

- PC security: many important threats like viruses, malwares, and botnets still endanger safety of personal computers for casting votes in secure environment.
- Software security: although many techniques are designed for testing and revealing left security bugs in developed codes, but there is no economic method which assures all bugs will be discovered. The left bugs could be exploited by attackers to influence election result.
- Defects of advanced cryptographic techniques: despite the modern cryptographic techniques enhance security level dramatically, but they are able to detect only certain types of attacks and also there is no way to restore original votes.

C. Availability

Proportion of time that a system must be partially or fully functional is called availability. Due to problems like overloading resources, malfunctions, or attacks the systems might become unavailable [12].

1. Properties:

Up-time: the time that system is available and in functioning mode for system operators, election officials, and voters [1].

- Reliability: possibility of desired system behavior if no external factors try to disrupt it [12].
- Recoverability: capability of restoring from system failure in reasonable time [1].
- Fault tolerance: system must be capable of delivering even lower level of functionality if a failure or attack happens [1].
- Fail safe: data los must be minimal if failure or attack happens [1].
- Scalability: capacity of the system must be expandable through adding extra resources without affecting system architecture [1].

2. Threats:

Following threats endanger availability of e-voting systems:

DoS attack: the most important threat to availability of an e-voting system is Denial of Service (DoS) attack which may target voters' computer, servers, or the election infrastructure [2], [17].

Large-scale DoS attack: an attack which targets large scale denial of service normally by

support of political parties or countries like what happened in Georgia (2008) or Estonia (2007) [18]. This attack aims to prevent voters to vote by attacking on registration databases, servers, or the infrastructure.

Domain Name System (DNS) attack: attack on content of look up table of DNS will redirect voters to a bogus website if chosen method is internet voting. Another similar attack is installing a program to change proxy of internet browser of voters to redirect them into desired address which in fact is kind of man-in-the-middle attack [2].

Targeted suppression and disruption: this attack is the same as Denial of Service attack when it only targets particular jurisdiction or demographic. Running this attack will ban people of particular area from casting their votes and will affect whole election result.

Client side disruption: large scale denial of service attack will threaten availability of server and communication channel, while this attack prevents the client systems from voting by techniques like installing malware on clients [1].

3. Solutions:

There is no comprehensive solution against denial of service attacks but following points will help to detect, prevent, and recover from attacks.

Redundancy and over-provisioning: duplication of resources to be used at attack time is called redundancy, and over-provisioning is devoting higher capacity severs and infrastructure to keep system functionality if DoS attack happens [1].

Availability active attack detection: process of availability detection is easy and voters will lose their access if DoS attack happens. Best protection is early detection and fast reaction [1].

Active attack defense: the most common DoS defense is over-provisioning and second choice is filtering sent attack packets.

4. Unresolved Issues:

Because of similarity of architecture of e-voting systems, particularly internet voting systems, with other online systems they suffer from almost same threats.

- Dos attack still is the most important cause of unavailability. Some technical defenses are introduced but no one of them can fully protect the system [1].
- Cloud computing is an ongoing field, but not enough mature to resolve current issues [19].

III. CONCLUSION

This study helps e-voting system researchers, designers, and developers to have comprehensive security criteria list of modern e-voting systems in hand to design their systems based on the

latest definitions and criteria in 2012. Unresolved counted issues introduce the remained threats and open research subjects for those deals with security of these systems.

REFERENCES

[1] National Institute of Standards and Technology (NIST) (2011), *Security Considerations for Remote Electronic UOCAVA Voting (NISTIR 7770)*. United States: National Institute of Standards and Technology.

[2] Norwegian Ministry of Local Government and Regional Development (2011). *E-vote 2011 Security Objectives*. Norway: Norwegian Ministry of Local Government and Regional Development.

[3] Georgia Tech Information Security Center (2008). *Emerging Cyber Threats Report for 2009*. Georgia: Georgia Tech Information Security Center.

[4] Internet Engineering Task Force (IETF) (2008). *The Transport Layer Security (TLS) Protocol Version 1.2*. Fremont: Internet Engineering Task Force (IETF).

[5] Chaeikar, S. S. (2010). *Interpretative Key Management (IKM), A Novel Framework*, Proceedings of 2010 Second International Conference on Computer Research and Development, Kuala Lumpur, Malaysia, 2010.

[6] Chaeikar, S. S. (2010). *Node Based Interpretative Key Management Framework*, Proceedings of The 2010 Congress in Computer science, Computer engineering, and Applied Computing (The 2010 International Conference on Security and Management SAM'10), WORLDCOMP'2010, Las Vegas, USA, July 2010.

[7] Chaeikar, S.S. Manaf, A. M. & Zamani. M. (2012). *Comparative Analysis of Master-Key and Interpretative Key Management (IKM) Frameworks.* Cryptography and Security in Computing, Dr. Jaydip Sen (Ed.), ISBN: 978-953-51-0179-6, InTech, Available from:http://www.intechopen.com/books/cryptography-and-security-in-computing/comparative-analysis-betweenmaster-key-and-interpretative-key-management-ikm-framework-to-provide-u

[8] Fujioka, A., Okamoto, T., and Ohta. K. (1992). *A Practical Secret Voting Scheme for Large Scale Elections*. Advances in Cryptology - AUSCRYPT '92. 1992. Berlin, 244-251.

[9] Cranor, L. F. and Cytron, R. K. (1997). *Sensus: A Security-Conscious Electronic Polling System for the Internet*. *Proceedings* of the Hawai`i International Conference on System Sciences, 7-10 January. Wailea, Hawaii, USA, 561-570.

[10] Benaloh, J., Tuinstra, D. (1994). Receipt-Free Secret-Ballot Elections. *Proceedings of the 26th ACM Symposium on Theory of Computing.* May. New York, USA, 544-553.

[11] Cramer, R., Gennaro, R., and Schoenmakers, B. (1997). *A secure and optimally efficient multi-authority election scheme*. European Transactions on Telecommunications. 8,481-489.

[12] Peralta, R. (2003). *Issues, non-issues and cryptographic tools for Internet-based voting*. Secure Electronic Voting. 7, 153-164. Springer.

[13] John Hopkins University, Department of computer science (2004). *Requirements for an Electronic Voting System*. Baltimore: John Hopkins University, Department of computer science.

[14] McConnell, S. (2004), *Code Complete*. (Second Edition), United States: Microsoft Press.

[15] Fink, R.A., Sherman, A.T., and Carback, R. (2009). TPM Meets DRE: Reducing the Trust Base for Electronic Voting Using Trusted Platform Modules. *Information Forensics and Security, IEEE Transactions*. 4(4), 628-284.

[16] Paul, N., Tanenbaum, A. S. (2009). *The Design of a Trustworthy Voting System*. Proceedings of Annual Computer Security Applications Conference. 7-11 December. Honolulu, HI, 507-517.

[17] ISO/IEC, Common Criteria for Information Security Evaluation (2009). *Part 3: Security assurance components. Version 3.1, Rev. 3*. Switzerland: ISO/IEC, Common Criteria for Information Security Evaluation.

[18] Alvarez, R. M. (2005). Precinct Voting Denial of Service. *NIST Threats to Voting Systems Workshop*. 5 October. Washington DC, Appendix 29.

[19] John Markoff (2008). *Before the Gunfire, Cyberattacks*. The New York Times, Retrived February 14, 2012, from http://www.nytimes.com/2008/08/13/technology/13cyber.html.