Chapter 23
Implementation and Evaluation of Steganography Based Online Voting System

Lauretha Rura
Swinburne University of Technology, Malaysia

Biju Issac
Teesside University, UK

Manas Kumar Haldar
Swinburne University of Technology, Malaysia

ABSTRACT

Though there are online voting systems available, the authors propose a new and secure steganography based E2E (end-to-end) verifiable online voting system, to tackle the problems in voting process. This research implements a novel approach to online voting by combining visual cryptography with image steganography to enhance system security without degrading system usability and performance. The voting system will also include password hashed-based scheme and threshold decryption scheme. The software is developed on web-based Java EE with the integration of MySQL database server and Glassfish as its application server. The authors assume that the election server used and the election authorities are trustworthy. A questionnaire survey of 30 representative participants was done to collect data to measure the user acceptance of the software developed through usability testing and user acceptance testing.

1. INTRODUCTION

One of the most important concerns in elections is to have an efficient and secure voting procedure. Even though it could be achieved by implementing an e-voting system, its ability to complete voting process faster than the paper ballot procedure alone does not guarantee its security. E-voting systems must be able to earn user's trust and confidence by providing enhanced security features without affecting us-

DOI: 10.4018/978-1-7998-1763-5.ch023

ability, efficiency and reliability. The system should offer some level of transparency to the user without allowing any breach of trust and privacy. To fulfil this condition, e-voting systems must provide both individual and universal verifiability. Individual verifiability is the ability of an e-voting system to offer vote verifiability to the voter through the implementation of vote receipt, whereas universal verifiability is the ability to offer election transparency to its users. Such systems are categorised under End-to-End (E2E) verifiable voting system (Adida, 2008). End-to-end verifiability represents a change in electronic voting, allowing a way to verify the integrity of the election by permitting the voters to use the system generated information, rather than trusting that the system has behaved correctly (Ryan, Schneider & Teague, 2015). In this paper, we propose an improved E2E verifiable voting system called as eVote software. This voting software could deliver a secure, reliable, convenient, and efficient voting system. As a research objective, we want to improve the quality of election procedure in an electronic voting system that relates to security and usability aspects, by using visual cryptography and image steganography in the system architecture. We also want to evaluate the developed online system through usability testing.

The outcome of evaluating an Internet voting system in the Canton of Zurich shows the need to rely on more advanced technology and centralised infrastructure (Beroggi, 2014). In the work (Azougaghe, Hedabou & Belkasmi, 2015) an electronic voting system based on homomorphic encryption to ensure privacy and confidentiality are proposed. The eVote software differs from previous online voting systems with the usage of cryptography and steganography to secure the data transmission during the election. The difference between cryptography and steganography lies in the way data is processed. Cryptography generates a ciphertext, while steganography produces a stego-object which is not perceptible by Human Visual System (HVS). In electronic voting, cryptography is a commonly used technique as it is a good defence against threats. In this paper, the authors introduce a novel approach to enhance E2E Voting System's security by combining visual cryptography with image steganography. Image steganography is chosen due to its capability to use data transmitted over the network. During the election voting process, the image steganography protects the existence of the message as a secret (Wang and Wang, 2004), offering a good solution for threats and risks that might occur. The combination of these two schemes is expected to produce an improved and secure approach (Morkel et al., 2005). Petcu & Stoichescu (2015) proposed a mobile biometric-based design that uses techniques such as Secure Sockets Layer encryption, certificate keys and security tokens. This paper is organised as follows. Section 2 discusses the E2E verifiable voting system and related works, section 3 is the proposed eVoting system, section 4 is the software testing and the usability analysis done, and section 5 is the conclusion and limitations.

2. E2E VERIFIABLE VOTING SYSTEM

Various E2E systems have been proposed and are widely used these days (Ryan et al., 2009; Chaum, 2004; Adida, 2008; Chaum et al., 2008; Hubbers, Jacobs, & Pieters, 2005). A verifiable voting system allows blind voters and voters in remote locations to cast fully secret ballots in a verifiable way (Burton, Culnane & Schneider, 2016). In principle, E2E voting system offers assurance to the voters over their cast vote. This is done by distributing vote receipt of encoded cast vote to each of the voters for verification purpose. To support this verification process, E2E systems implemented bulletin board which is a secure append-only broadcast media where each of the encoded votes would be posted once the voters completed the voting process. To verify their cast votes, they need to match the encoded value on their receipt against the values shown on the bulletin board. However, the vote receipt cannot be used as a