APPLICATION OF TRUSTED COMPUTING IN INTERNET VOTING

MOHD ZAID WAQIYUDDIN BIN MOHD ZULKIFLI

A thesis submitted in partial fulfillment of the
requirements for the award of the degree of
Master Computer Science (Information Security)

Faculty of Computer Science and Information System
Universiti Teknologi Malaysia

NOVEMBER 2009

To my beloved family and friends

ACKNOWLEDGEMENT

I would like to forward my appreciation to my thesis supervisor, Dr. Rabiah Ahmad, for her guidance and support.

ABSTRACT

Over the years, improvements in technology and security, along with our increasing comfort with the Internet, have seen many applications and services being delivered online. Despite this, the adoption of Internet voting has been remarkably slow, mainly due to the unique requirements of elections, its scale and the disastrous consequences of failure. In the academic world however, many interesting techniques and protocols have been discovered that could help improving the security and robustness of Internet voting. Unfortunately, most of the designs often make very demanding assumptions or otherwise, are very limited in their effectiveness. This paper looks at Trusted Computing technology as a means to satisfy some of the assumptions, and to see its effects in improving the overall security of Internet voting architecture. This paper also looks at the possibility of Trusted Computing making certain Internet voting technologies unnecessary or redundant.

ABSTRAK

Hari demi hari, kemajuan teknologi dan keselamatan menyebabkan banyak servis dan aplikasi disalurkan melalui Internet berbanding cara tradisional. Faktor penyebab lain ialah kebanyakan pengguna semakin serasi dengan Internet dan komputer. Walaubagaimanapun, penggunaan komputer dan Internet dalam undian pilihanraya masih terlalu kurang. Antara faktornya ialah kriteria keselamatan yang unik, yang mesti dipenuhi. Saiz aplikasi dan risiko juga besar. Bagaimanapun, dalam dunia akademik, banyak kemajuan dari segi teknik dan protocol komunikasi telah dicipta untuk meningkatkan tahap keselamatan aplikasi pengundian pilihanraya melalui Internet. Kajian thesis ini melihat kepada pengaplikasian teknologi "Trusted Computing" untuk mengukuhkan tahap keselamatan aplikasi pengundian melalui Internet.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Overview

In democratic countries, general elections are held periodically to allow citizens to vote for representatives for a ruling government. Elections are normally held every three to five years.

Internet voting system aims to facilitate this process by automating certain parts or stages and enabling voting over Internet while guaranteeing the level of security that is at least equivalent to the traditional voting system.

One major difference between the traditional voting system and Internet voting system is that the voters can vote from anywhere with Internet connection which greatly affect the security implementation of various parts or stages of the process. Geography independent voting gives convenience and encourage higher voter turnout, but also introduces complication with security and privacy, considering the vulnerable nature of the Internet. This necessitates an Internet voting system to be carefully designed to maximize confidence in security while minimizing potential for fraud and manipulation.

Some examples of electronic voting systems, not necessarily Internet-enabled, are Nurmi (1999), Fujioka (1992), Davenport et. al (1995/7), Radwin (1995), Cranor (1996), Cramer et. al and Du Rette (1999). Each of these satisfies some or all of the features often needed in an electronic voting system such as double vote prevention, ballot confidentiality, universal verifiability, multiple authority and non-manipulability.

An Internet voting system is aimed at reducing cost and workload required for conducting a large scale election i.e. national general election. For example, in Malaysia during the 2004 general election, the workforce employed consisted of a total of 172,799 personnel from various categories, whereas the budget allocated was RM100 million. Internet voting system is expected to reduce the budget needed with elimination or reduction of paper printing, reduced workforce allowance, payment of overtime worker and traveling expenses. Another major motivation for Internet voting is also to encourage more participation from voters especially among the youngsters by offering convenience and voting medium that they are familiar with.

Despite the various voting systems designed and studied, the challenge remains to gain user confidence and eventually acceptance of the technology. The concerns are primarily integrity and privacy. There are also additional requirements associated with electronic voting, in that; measures must be taken to prevent vote buying and extortion by making the users unable to prove who they had voted for.

This study intends to take advantage of trusted computing platform being developed by Trusted Computing Group (initially Trusted Computing Platform Alliance or TCPA), to give better integrity and privacy assurance of Internet voting systems. Each entity in an Internet voting system such as voters' client machine, registrar, administrator, validator and tallier and their relationship are studied to leverage on available TCPA functions provided. This in result will give a higher level of trust to an Internet voting system as a whole.

As an example, distribution of ballot can be controlled so that it can only be decrypted at specific platforms, i.e. tallier by encrypting the ballot with the public

part of the Endorsement Key (EK) belonging to the tallier machine. This capability is made possible with Trusted Platform technology.

Trusted Platform technology can similarly be utilized to ensure that voters connecting to the electronic voting central system are running genuine client software and also used to manage protected storage for storing cryptographic keys, ballots and other sensitive data.

It is the goal of this project to study the usage of Trusted Platform Module (TPM) capabilities to improve the security i.e. integrity and privacy of Internet voting system as a whole.

1.2 Background of the Problem

1.2.1 Internet Voting

Stable and tested network technology and its ubiquitous deployment in many countries have opened up possibility for a nation-wide Internet voting system. This is supported by the advancement of cryptography techniques to ensure that issues involving privacy and integrity can be sufficiently dealt with. An electronic voting system can be designed to overcome the problems of traditional voting and thus becomes a viable alternative method to traditional system.

The advantages of Internet voting system have been emphasized in many literatures. These include convenience for voters hence encouraging higher turnout, minimizing human errors, and reducing management cost.

Additionally, with employment of cryptographic techniques in Internet voting system, secrecy and other properties, verifiability and authenticity can be obtained, which may not be provided in the traditional system.

Malaysia general election in 2004 had seen few complications which would not have arisen with correct implementation of Internet voting system. For instance, there was congestion in Selangor due to confusions as the state election director opened up new polling centers without consulting the national election commission. This resulted in voting time being extended by two hours, an unprecedented action in Malaysia election history. In electronic voting system, due care must be exercised to ensure that unapproved changes or actions will not be carried out. Similar problem transpired in state seat N.17 Sungai Lembing where faulty printing of ballot papers occurred after the printing company decided to change the printing plate without the approval from central committee. The ballot papers had mismatched the logo and the party.

There are also issues with double voting in election. Subariah et. al (2000) said, mechanisms must also exist to check that a voter has not already cast a vote in order to prevent double voting. However, the Estonian implementation guideline challenges this requirement, arguing that multiple voting is permissible if only one vote is counted in the final tally. Estonian implementation uses this as a strategy to further discourage vote buying.

Core properties of an Internet voting system can be summarized as the following:

Table 1.1 : Core properties of an Internet voting system

Confidentiality	No one, including the election authorities can link any ballot to the voter who cast it, and no voter can prove that he or she voted in a particular way (voting protocol must ensure this).
Integrity	No one can change the ballot without being discovered, not possible for valid vote to be eliminated from the final tally, not possible for invalid vote to be counted in the final tally.

Authentication	Voter must be eligible voter, and who he claims to be. Some form of credential or ticket must be given to a voter to be used during authentication when voting.
Verifiability	Voter can check that his vote was properly received and taken into account in the final tally. Auditing can be done at later date to verify at a later time that the election was properly performed.

Lorrie and Ron (1996) listed additional properties which are often desired but not always achieved, which are convenience (ability to cast votes quickly with minimum equipment and special skills), and mobility. Trusted Computing does include other devices besides PC i.e. PDA, mobile phones etc, hence is not a hindrance to these desired properties.

This study recognizes that one of the main challenges faced by implementation of Internet voting system is in trusting each entity in the architecture. In other words, there should be a guarantee that each of these entities is what it claims to be and does only what it claims to do. There must be assurance that there is no additional or unnecessary software operating on these machines. Voters must only use the client software approved by the election authorities, or web browsers for web based voting to ensure that the software not modified or compromised by malicious parties.

This study defines trusted Internet voting system as Internet-enabled remote voting system in which each entity and all its operations can be trusted. The viable solution for this is in embedding Trusted Platform Module (TPM) into the motherboard, implemented in each entity. Communication between entities must be based on trusted paradigm, each end point must be trusted and communication performed based on the policy set.

Lorrie and Ron (1996) claimed that their designed system, Sensus, did not address the specific instance of privacy property, where it did not prevent voters from proving how they voted by allowing another party to observe them while they

are casting their votes. They did not believe that this problem can be addressed without sacrificing mobility or convenience.

1.2.2 Trusted Platform Module

Trusted Computing was initiated in realization of the fact that software alone is not enough to be secure against attack. Inclusion of hardware is needed for more robust security architecture. Conventional crypto co-processors only protect itself from logical and physical attack but do not protect processing on the ordinary CPU.

The Trusted Computing Group (TCG) technical committee had a number of design goals for the Trusted Platform Module (TPM), as follow:

1. Securely report the environment that booted.
2. Securely store data.
3. Securely identify the user and system (without encountering privacy concerns).
4. Support standard security systems and protocols.
5. Support multiple users on the same system while preserving security among them.
6. Be produced inexpensively.

Trusted Computing is expected to effectively offer services such as a mechanism for the platform to show that it is executing the expected software, a mechanism for the platform to prove that it is a trusted platform while maintaining anonymity (if required). Trusted Computing also provides utilities for securing encryption keys, and protection against theft and misuse of secrets held on the platform.

1.3 Problem Statement

Literature has listed many architecture and implementation of Internet voting system, but there remains a challenge to ensure that these systems can be trusted. Customized hardware support has been recognized as a solution for trusted architecture but this introduces more complications to the system design such as interoperability problem between equipment from different vendor.

With initiative from Trusted Computing Group to research and develop the trusted platform technology, it is now ready to be applied to a multitude of applications, including Internet voting system. The challenge now is to successfully make the available studies and design of electronic voting system to integrate with Trusted Platform technology and accurately measure the security level and functionality of the resulting hybrid.

1.4 Project Objectives

The objectives of this project are outlined as below:

1. Identify what functionalities and capabilities of Trusted Computing that are useful for Internet voting system.
2. Demonstrate basic uses of Trusted Computing in securing certain parts of an Internet voting system.
3. Assess the functionalities and the security of the system against certain types of attack and weaknesses.

1.5 Project Aim

The aim of this project is to first identify functionalities and capabilities of Trusted Computing Platform that can be utilized in an implementation of Internet voting system. These functionalities are expected to complement existing voting protocols, rather than replacing them as a solution for a secure Internet voting system for large scale election. The project also aims to demonstrate basic uses of Trusted Computing in implementing trust into certain entities within an Internet voting architecture.

1.6 Project Scope

The following scope applies to the study:

1. The notion of trust is based on Trusted Computing Platform promoted by Trusted Computing Group.
2. Internet voting system is designed only for computing platform equipped with TPM devices.
3. The Trusted Platform Module (TPM) being used for demonstration is software based emulator instead of the actual physical hardware.

REFERENCES

Abdul Aziz Bari and Farid Sufian Shuaib (2006). *Constitution of Malaysia, Text and Commentary*. 2nd Edition. Prentice Hall.

Avi Rubin. *Security Considerations for Remote Electronic Voting over the Internet.* AT&T Labs

Bruce Schneier (1996) *Applied Cryptography*. 2nd Edition. John Wiley & Sons, Inc.

Byoungcheon Lee, Colin Boyd, Ed Dawson, Kwangjo Kim, Jeongmo Yang and Seungjae Yoo. (2003) *Providing Receipt-freeness in Mixnet-based Voting Protocols*

David Challener, Kent Yoder, Ryan Catherman, David Safford, Leen-dert Van Doorn. (2008) *A Practical Guide to Trusted Computing*. IBM Press. 2008.

Election Commision Malaysia (2004). *Report of the General Election Malaysia*

Fujioka, A., Okamoto, T., and Ohka, K. (1993) *A Practical Secret Voting Scheme for Large Scale Elections.*

G. Lowe. (1996) *Breaking and fixing the Needham-Schroeder public key protocol using FDR.* In Tools and Algorithms for the Construction and Analysis of Systems, volume 1055 of Lecture notes in computer science, pages 147166 Springer.

IBM Research. *Direct Anonymous Attestation (DAA)*

. http://www.zurich.ibm.com/security/daa/

Joe Mohen, Julia Glidden (2001) *The Case for Internet Voting*. Communications of the ACM January 2001/Vol.44,No.1

Joy Marie Forsythe (2005) *Encrypted Receipts for Voter-Verified Elections Using Homomorphic Encryption.* Massachusetts Institute of Technology.

Lorrie Faith Cranor and Ron K. Cytron. (1996) *Design and Implementation of a*

Practical Security-Conscious Electronic Polling System. Washington University.

Mark A. Herschberg (1997) *Secure Electronic Voting Over the World Wide Web.* Massachusetts Institute of Technology.

Office for Democratic Institution and Human Rights. Republic of Estonia Parliamentary Elections (2007) *OSCE/ODIHR Election Assessment Mission Report*

Subariah Ibrahim, Mazleena Salleh and Maznah Kamat. (2000) *Electronic Voting System: Preliminary Study.* Universiti Teknologi Malaysia.

Sebastien Canard, Herve Sibert. (2001) *How to Fit Cryptographic E-Voting into Smart Cards.* Fundamenta Informaticae XXI 1001-1012. IOS Press.

Thomas Tjostheim and Geir Rosland. *Remote Electronic Voting Using Verifiable Chain Encryption*. Fundamenta Informaticae XX(2006) 1-15. IOS Press.

Wolter Pieters. (2006) *Acceptance of Voting Technology: Between Confidence and Trust.*

Xenakis and Macintosh. (2005) *Procedural Security and Social Acceptance in E-Voting* (HICSS'05).