

Universiti Teknologi MARA

**Secure Online Voting System for FTMSK
Student's Union with Blind Signature
Techniques**

Mohd Nurhafizi Bin Saidin

Thesis submitted in fulfilment of the requirements for
Bachelor of Computer Science (Hons)
**Faculty of Information Technology And
Quantitative Science**

December 2008

ACKNOWLEDGEMENTS

BISMILLAHIRRAHMANIRRAHIM

In the name of Allah, the most gracious and the most merciful.

Alhamdulillah, praise to Allah for His Almighty and Graciousness. With His utmost blessings, I was able to finish this written report within the time duration given.

I would like to express a very special gratitude and thankfulness to my supervisor Puan Norasiah Binti Mohammad who is giving me reliance and shrewd guidance that have profited me very much. She also gave lots of support to me in my hard time to journey through this knowledge quest. I would also like to thank my second supervisor Puan Radziah Binti Ali who always helping and guiding me towards the completion of this project final report.

My special appreciation and thanks for my subject lecturer, En. Syed Ahmad Aljunid for his encouragement and guidelines through this semester and the rest of my previous lecturers at faculty of information technology and quantitative science.

To my friends in the faculty, who are simply too numerous to indicate, thanks for your time, understanding, buttress and always give me motivation and support. May Allah will reciprocate you for all those kindness.

Last but not least, to my parents and my siblings, I would like to forward my obliged to them for their continuous support during my study period, their patience and benevolence.

Thank you.

ABSTRACT

With a rapid growth in computer networks, many people can access the network through the Internet and therefore an online voting system can be a viable alternative for conducting an election. Online voting system must attempt to achieve at least the same level of security as ordinary elections. We have developed an Online Voting System (OVS), online voting for a general election. One supports universal and absolute security with the use of physical ballots and the other claims that such security is not a necessity in all contexts. Online Voting System (OVS) employs cryptographic techniques to overcome the security issues in the election process. In this system, voter's privacy is guaranteed by using a blind signature for confidentiality. For this reason, a structural security framework for electronic voting systems is presented which can be used for their composition and analysis.

Keywords: online voting systems, security, confidentiality, blind signature

Table of Contents

Declaration	ii
Approval.....	iii
Acknowledgements	iv
Abstract	v
List of Figures	ix
List of Abbreviations	x
Chapter 1: Introduction	
1.0 Research Background.....	1
1.1 Problem Statement	2
1.2 Project Objective	2
1.3 Project Scope.....	3
1.4 Technique(s) Employed	4
1.5 Project Significant.....	4
Chapter 2: Literature Review	
2.0 Introduction.....	6
2.1 The Evolution of Voting System	7
2.2 Definition of Online Voting.....	9
2.3 Online Voting Process	11
2.3.1 Elections Stages	11
2.4 Threats to Online Voting Services.....	13
2.4.1 Potential Sources of Attack	14
2.4.2 Possible Methods of Attack.....	15

2.5	General Security Requirements for Online Voting	17
2.6	Security Mechanisms in Online Voting.....	20
2.6.1	Blind Signatures.....	21
2.7	Conclusions.....	23
Chapter 3: Methodology		
3.0	Introduction.....	24
3.1	Planning	26
3.2	Analysis	26
3.2.1	Data Collection	27
3.2.2	Data Analysis.....	29
3.2.3	Findings	30
3.3	Design	30
3.3.1	Logical Design.....	30
3.3.2	Detailed Design	31
3.4	Testing	31
3.5	Documentation	32
3.6	Summary	32
Chapter 4: Design and Implementation		
4.0	Introduction	33
4.1	System Requirements	33
4.1.1	Software Requirement	33
4.1.2	Hardware Requirement.....	35
4.3.1	Hardware Requirement.....	35
4.2	Development.....	36