



UNIVERSITI PUTRA MALAYSIA

**PLATFORM PROPERTY CERTIFICATE FOR PROPERTY-BASED
ATTESTATION MODEL**

NAZANIN BORHAN

FSKTM 2011 1



**PLATFORM PROPERTY CERTIFICATE FOR
PROPERTY-BASED ATTESTATION MODEL**

NAZANIN BORHAN

**MASTER OF SCIENCE
UNIVERSITI PUTRA MALAYSIA**

2011



**PLATFORM PROPERTY CERTIFICATE FOR PROPERTY-BASED
ATTESTATION MODEL**

BY

NAZANIN BORHAN

**Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia,
in Fulfilment of the Requirements for the Degree of Master of Science**

January 2011



Dedicated to my dear parents



Abstract of thesis to be presented to the Senate of Universiti Putra Malaysia in
fulfilment of the requirements for the degree of Master of Science

**PLATFORM PROPERTY CERTIFICATE FOR PROPERTY-BASED
ATTESTATION MODEL**

By

NAZANIN BORHAN

January 2011

Chairman: Zuriati Ahmad Zukarnain, PhD

Faculty: Computer Science and Information Technology

Trusted Computing Group (TCG) provides a group of prominent computer manufacturers to improve a new technology called Trusted Computing (TC) which can provide a basis to the highest security level in hardware and software. The goal of TCG is to provide a mechanism for security and integrity of computing platforms. Remote attestation is one of the TC aspects which is the method that a system uses to authenticate to a remote party or for a remote party to verify the authenticity of the application. Among other methods of attestation, binary attestation is the TCG standard approach. However, binary attestation mechanism still lacks in flexibility, privacy and scalability and to overcome these problems Property-based Attestation was introduced. Two important issues should be considered in this context: the content of the property and the protocol that we should choose.

We proposed Platform Property Certificate based on the current certificates of a system (AIK and SSL certificates), in our study as the model's property. At the same



time, we propose a client-server attestation protocol that can apply this property by using an online Trusted Third Party to verify the trustworthiness of the certificates and measurements of the system. Performance evaluation method in this study is implementation with existing specification and hardware of TC and the criteria that are evaluated are privacy, flexibility and scalability that are compared in the proposed model with the TCG binary attestation model.

Comparison and analysis are based on an implemented binary attestation model that are designed to have the same input and output format of our own proposed model to check the results. Results shows that our property is efficient in the case of accepting and rejecting valid and invalid input and our property-based protocol overcomes the deficiencies of lack of flexibility, privacy and scalability in binary attestation mechanism. Therefore the model and the property fulfill the requirements of property-based attestation.



Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia sebagai memenuhi keperluan untuk ijazah Master Sains

**SIJIL SIFAT PLATFORM UNTUK MODEL PENGAKUSAKSIAN
BERASAKAN SIFAT**

Oleh

NAZANIN BORHAN

Januari 2011

Pengerusi: Zuriati Ahmad Zukarnain, PhD

Fakulti: : Sains Komputer dan Teknologi Maklumat

Trusted Computing Group (TCG) merupakan satu sumber yang sedia ada untuk meningkatkan teknologi baru iaitu *Trusted Computing* (TC) dimana boleh membekalkan asas kepada tahap keselamatan yang tertinggi dalam perkakasan dan perisian. Tujuan TCG yang terdiri daripada IT infrastruktur menyediakan satu mekanisme bagi keselamatan dan integriti untuk platform-platform pengiraan. Remote Attestation ialah satu aspek daripada TCG yang bermakna cara sistemnya diggunakan untuk mengesahkan satu parti yang jauh atau untuk parti yang jauh mengesahkan keaslian permohonan. Antara kaedah-kaedah akuan yang lain, Binary Attestation digunakan sebagai pendekatan piawai TCG. Tetapi mekanisme Binary Attestation masih mempunyai kekurangan-kekurangan dari segi Kelonggaran, Privasi dan Kebolehskalaan dan kami menggunakan Pengakusaksian Berasaskan sifat untuk menangani masalah ini. Dua isu penting harus dipertimbangkan dalam konteks ini: Kandungan dalam Sifat dan Protokol yang kita harus memilih.

Kami mencadangkan Sijil Sifat Platform berasaskan sijil-sijil lain daripada sistem (AIK dan SSL sijil), dalam kajian kita sebagai sifat model. Pada masa yang sama, kami mencadangkan sebuah protokol client-server atestasi yang dapat melaksanakan hotel ini dengan menggunakan talian "Trusted Pihak Ketiga" untuk mengesahkan kepercayaan sijil dan pengukuran sistem. Penilaian prestasi kaedah dalam kajian ini adalah pelaksanaan dengan spesifikasi yang ada dan peranti keras dari TC dan kriteria yang dinilai adalah privasi, fleksibiliti dan skalabilitas yang dibandingkan pada model yang dicadangkan dengan model atestasi TCG binari.

Perbandingan dan analisis didasarkan pada model atestasi dilaksanakan binari yang dirancang untuk memiliki input yang sama dan format output dari model yang dicadangkan sendiri kami untuk memeriksa hasilnya. Keputusan menunjukkan bahawa harta kita adalah cekap dalam hal menerima dan menolak masukkan yang sah dan tidak sah dan hotel protokol berasaskan kami mengatasi kekurangan kekurangan fleksibiliti, privasi dan skalabilitas dalam mekanisme atestasi binari. Oleh kerana itu model dan hotel memenuhi keperluan atestasi hotel yang berpusat.

ACKNOWLEDGEMENTS

First and foremost, I would like to thank Associated Professor Dr. Ramlan Mahmud, who gave me this opportunity and support to realize the project. His great insights and guidance have been reflected throughout all this thesis work. His kindness and friendliness has also made this work finished in the easiest way.

I sincerely thank Dr. Zuriati Ahmad Zukarnain, for her constant guidance and technical direction for completing this work. I owe her lots of gratitude for having shown me this area of research.

Special thanks are given to my parents, who always support in my hardest time. Without their unceasing encouragement, dedication and blessings, my dream could never come true.

I am also very grateful for my friends, who always care about me and are always on my side, in both shining and dark years.

It should be mentioned that this study was partially supported by MIMOS Berhad Malaysia.



I certify that a Thesis Examination Committee has met on 17 January 2011 to conduct the final examination of Nazanin Borhan on her thesis entitled “Platform Property Certificate for Property-based Attestation Model“ in accordance with the Universities and University Collage Act 1971 and the Constitution of the Universiti Putra Malaysia [P.U.(A) 106] 15 March 1998. The committee recommends that the student be awarded the Master of Science.

Members of the Examination Committee are as follows:

Abdul Azim B. Abd. Ghani, PhD

Professor
Faculty of Computer Science and Information Technology
University Putra Malaysia
(Chairman)

Nur Izura binti Udzir, PhD

Senior Lecturer
Faculty of Computer Science and Information Technology
University Putra Malaysia
(Internal Examiner)

Shamala a/p K Subramaniam, PhD

Senior Lecturer
Faculty of Computer Science and Information Technology
University Putra Malaysia
(Internal Examiner)

Rabiah binti Ahmad, PhD

Associated Professor
Faculty of Computer Science and Information Technology
University Technical Malaysia Melaka
(External Examiner)

SHAMSUDDIN SULAIMAN, PhD

Professor and Deputy Dean
School of Graduate Studies
Universiti Putra Malaysia

Date: 24 March 2011



This thesis was submitted to the senate of Universiti Putra Malaysia and has been accepted as fulfilment of the requirement for the degree of Master of Science. The members of the Supervisory Committee were as follows:

Zuriati Ahmad Zukarnain, PhD

Senior Lecturer

Faculty of Computer Science and Information Technology

University Putra Malaysia

(Chairman)

Ramlan Mahmud, PhD

Associated Professor

Faculty of Computer Science and Information Technology

University Putra Malaysia

(Member)

HASANAH MOHD GHAZALI, PhD

Professor and Dean

School of Graduate Studies

Universiti Putra Malaysia

Date:



DECLARATION

I declare that the thesis is my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously, and is not concurrently, submitted for any other degree at Universiti Putra Malaysia or other institutions.

NAZANIN BORHAN

Date: 17 January 2011



TABLE OF CONTENTS

	Page
DEDICATION	ii
ABSTRACT	iii
ABSTRAK	v
ACKNOWLEDGEMENTS	vii
APPROVAL	viii
DECLARATION	x
LIST OF FIGURES	xv
LIST OF TABLES	xvii
LIST OF ABBREVIATIONS	xviii
CHAPTERS	
1 INTRODUCTION	1
1.1 Introduction	1
1.2 Remote Attestation	3
1.3 Property-based Attestation	6
1.4 Problem Statement	7
1.5 Research Objectives	9
1.6 Research Contributions	9
1.7 Scope of the research	10
1.8 Organization of the Thesis	10
2 LITERATURE REVIEW	12
2.1 Introduction	12
2.2 Trusted Computing Main Features	13
2.2.1 Endorsement key	14
2.2.2 Memory curtaining	15
2.2.3 Sealed storage	16
2.2.4 Remote attestation	16
2.2.5 Trusted Third Party	16
2.3 Trusted Platform Module (TPM)	17
2.4 Software Based Trusted Platform Module	19
2.5 Platform Configuration Registers	21
2.6 TCG Style Remote Attestation (Binary Attestation)	23



2.7	Property-based Attestation	30
2.7.1	Delegation Based Attestation	32
2.7.2	Derivation Based Attestation	44
2.7.3	Enforcement Based Attestation	46
2.8	Definition of Property in Property-based Attestation model	48
2.9	Using Trusted Channels	52
2.10	Summary	55
3	RESEARCH METHODOLOGY	57
3.1	Introduction	57
3.2	Reviewing LR and Identifying the Problem	59
3.3	Identification of Data and Performance Measurements	59
3.3.1	Defining the Proposed Model	60
3.4	Designing the Proposed Model	62
3.4.1	Dataset and benchmark log file	63
3.4.2	Evaluation Method	65
3.5	Implementation of the proposed model	65
3.5.1	Testbeds Setup	66
3.5.2	Performance Evaluation Metrics	67
3.5.3	Running of the system	68
3.6	Results and Analysis	69
3.6.1	Validating the proposed model	69
3.7	Documentation of the study	72
3.8	Summary	72
4	PROPOSED PROPERTY-BASED ATTESTATION MODEL	74
4.1	Introduction	74
4.2	Property-based Attestation Architecture	74
4.2.1	Data flow and system architecture	75
4.2.2	The protocol for Decision Making	81
4.3	Components of the proposed Model	83
4.3.1	TPM Configuration	83
4.3.2	Loading process of the Trusted Platform	86
4.3.3	Attestation Function	88



4.3.4	Endorsement Key (EK)	89
4.3.5	Attestation Identity Key	89
4.3.6	AIK Generation	89
4.4	Algorithms of the Proposed Model	90
4.4.1	Certificate Managing Algorithm	91
4.4.2	Client Machine Algorithm	94
4.4.3	Server Machine Algorithm	95
4.4.4	Trusted Third Party Algorithm	96
4.4.5	Privacy CA Algorithm	97
4.4.6	Monitoring Agent	98
4.5	Summary	98
5	IMPLEMENTATION OF TESTBEDS	100
5.1	Introduction	100
5.2	Data Requirement	100
5.3	Performance evaluation Methods for PBA	101
5.4	Performance Evaluation Metrics	102
5.5	Implementation Testbeds	103
5.5.1	Testbeds Scenarios	103
5.5.2	Binary Attestation Model	105
5.5.3	PCR Update	108
5.5.4	Property-based Attestation Model	109
5.6	Running of the Systems	109
5.6.1	Program interfaces for Binary Attestation Model	110
5.6.2	PCR Update Program Interface	112
5.6.3	Program Interfaces for the proposed Model	112
5.6.4	Certificate Managing Program	113
5.6.5	Program on Client Machine	114
5.6.6	Program on Server Machine	115
5.6.7	Trusted Third Party Program	116
5.6.8	Privacy CA Program	117
5.6.9	Monitoring Agent Program	118
5.7	Expected Outputs of the tests	119
5.8	Summary	121

6	RESULTS AND DISCUSSION	122
6.1	Introduction	122
6.2	Results and Analysis	122
6.2.1	Model Testing	122
6.2.2	Result of the comparison test	126
6.2.3	Comparative Analysis	129
6.3	Summary	131
7	CONCLUSION AND RECOMMENDATION	133
7.1	Conclusion	133
7.2	Future works	135
	REFERENCES	137
	BIODATA OF STUDENT	141
	LIST OF PUBLICATIONS	142

