UNIVERSITI PUTRA MALAYSIA

PLATFORM PROPERTY CERTIFICATE FOR PROPERTY-BASED ATTESTATION MODEL

NAZANIN BORHAN

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 atestasiyang 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 spesifikasiyang ada dan peranti keras dari TC dan kriteria yang dinilai adalah privasi, fleksibiliti dan skalabilitas yang dibandingkan pada model yang dicadangkan dengan modelatestasi TCG binari.

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

ACKNOWLEDGEMENTS

First and foremost, I would like to thank Associated Professor Dr. Ramlan Mahmod, 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 Mahmod, 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