UNIVERSITI PUTRA MALAYSIA

INCORPORATION OF CERTIFICATION REVOCATION AND TIME CONCEPT INTO A TRUST MODEL FOR INFORMATION SECURITY SYSTEM

FATEMEH AZIMZADEH

INCORPORATION OF CERTIFICATION REVOCATION AND TIME CONCEPT INTO A TRUST MODEL FOR INFORMATION SECURITY SYSTEM

By

FATEMEH AZIMZADEH

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

September 2007

To my parents, my husband and my son.

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

INCORPORATION OF CERTIFICATION REVOCATION AND TIME CONCEPT INTO A TRUST MODEL FOR INFORMATION SECURITY SYSTEM

By

FATEMEH AZIMZADEH

September 2007

Chair: Professor Borhanuddin Mohd. Ali, PhD

Faculty: Engineering

In large open networks, handling trust and authenticity adequately is an important prerequisite for security policy. Trust issues influence not only the specification of security policies but also the techniques needed to manage and implement security policies for systems. Certification is one of the main components of trust models and is known as a common mechanism for authentic public key distribution. In order to obtain a public key, verifiers need to extract a certificate path from a network of certificates, which is called the public key infrastructure (PKI). There are two classifications of PKI; namely the centralized and decentralized PKIs. In this thesis, attention is paid the decentralized PKIs, such as Maurer's model. This model is comprised of two parts; the deterministic and probabilistic models. An important limitation in this model is that certification revocation is not considered. Revocation happens in

cases, among others, such as the loss of private key. Another limitation of Maurer's model is that it lacks time consideration, which is important as trust changes over time.

In this thesis, a novel trust model is developed, addressing the limitations of other models. Negative values such as revocation of certification have been incorporated, making a complete trust model that includes both positive and negative evidences. Particularly, certification is considered as positive evidence while certification revocation is considered negative. The time concept is then added to the model in order to address the change of trusts status over time. Hence, the complete trust model is able to incorporate certification revocation and time concept into both deterministic and probabilistic parts of a model.

Incorporating two new concepts into Maurer's model increases the generality and expressive power of the model. Novel extension of the trust model enabling it to capture all aspects of public key certification which includes trust, recommendations, confidence values for trust metric and authenticity of public keys, multiple certification paths, certification revocation and the time concept. Experimental results show that after incorporating the new concept, a decrease in confidence value in comparison to Maurer's model was observed, resulting to a more realistic model.

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

MEMASUKKAN PEMBATALAN PENSIJILAN DAN KONSEP MASA DALAM SATU MODEL KEPERCAYAAN UNTUK SISTEM KESELEMATAN MAKLUMAT

Oleh

FATEMEH AZIMZADEH

September 2007

Pengerusi: Profesor Borhanuddin Mohd. Ali, PhD

Fakulti: Kejuruteraan

Dalam rangkaian terbuka yang besar, pengurusan kepercayaan dan pembuktian secukupnya adalah satu syarat yang penting untuk polisi keselamatan. Isu-isu kepercayaan mempengaruhi bukan sahaja spesifikasi polisi-polisi keselamatan tetapi juga kaedah-kaedah yang diperlukan untuk menguruskan dan melaksanakan polisi-polisi sistem itu. Pengesahan adalah salah satu komponen utama model-model kepercayaan dan dikenalpasti sebagai satu mekaniksma yang umum untuk penyebaran pembuktian kunci awam. Untuk memperoleh satu kunci awam, para pengesah perlu mencabut satu laluan yang sah daripada satu rangkaian pengesahan yang dikenali sebaga infrastruktur kunci awam (IKA). IKA diklasifikasikan dalam dua bentuk, pemusatan dan bukan pemusatan. Di dalam tesis ini tumpuan ditujukan kepada IKA bukan pemusatan seperti model Maurer. Model ini dibahagi kepada dua bahagian; model

deterministik dan model kebarangkalian. Satu had yang penting dalam model ini ialah pembatalan pengesahan tidak dikira, walkhal pembatalan berlaku oleh kerana beberapa sebab, contohnya kehilangan kunci awam. Masalah pertimbangan kedua untuk model ini ialah pembadanan masa di dalam model ini, sementara kepercayaan berubah mengikut masa.

Dalam tesis ini, satu model kepercayaan dibangunkan dengan memasukkan nilai negatif seperti pembatalan pengesahan ke dalam satu model kepercayaan, kerana satu model lengkap adalah besertakan bukti-bukti positif dan negatif, sementara model Maurer adalah besertakan hanya nilai positif. Sebagai contoh pengesahan adalah bukti positif dan pembatalan pengesahan adalah bukti negatif, yang dipertimbangkan dalam model kita. Selepas itu konsep masa ditambahkan kepada model ini untuk menyelaraskan pertukaran status kepercayaan mengikut masa. Oleh itu model kepercayaan yang lengkap dapat memasukkan pembatalan pengesahan dan konsep masa ke dalam kedua-dua bahagian pengenalpastian dan kebarangkalian.

Memasukkan dua konsep yang baru ke dalam model Maurer meningkatkan peraturan umum dan kuasa yang bererti model tersebut. Ini disebabkan model baru ini memperangkap semua aspek-aspek pengesahan kunci awam, termasuk; nilai-nilai kepercayaan, pengesyoran, keyakinan untuk metrik kepercayaan dan pengurusan kunci-kunci awam, beberapa laluan pengesahan, pembatalan pengesahan dan konsep masa. Keputusan eksperimen menunjukkan selepas memperbadankan konsep-konsep baru, penurunan nilai keyakinan dalam

perbandingan model Maurer. Perkara ini selaras dengan hakikat, di mana masa pertimbangan dan pembatalan adalah tidak dapat dielakkan.

ACKNOWLEDGEMENTS

Acknowledgement is not a play of words, but an attitude of mind. If words are considered as the symbol of approval and tokens of appreciation, then let the words play the heralding role to expressing my gratitude.

First and foremost of all, I pay my obeisance and gratitude to the Allah for giving me the ability to carry out the research work and completing it.

I would like to express my sincere and deep gratitude to my supervisor, Prof. Dr. Borhanuddin Mohd. Ali. His unwavering support and advice throughout my two years of Master study enabled me to focus on what I needed to learn and complete my studies on time.

Special thanks to my co-supervisor, Associate Prof. Dr. Sabira Khatun for her helpful comments and suggestions in completing this thesis.

I would like to thank my friends and colleagues for their motivation, support and help accorded throughout my study in University Putra Malaysia. This is also extended to everyone who helped me directly or indirectly in making my graduate studies smooth journey

Last but not the least, I would like to express my gratitude and appreciation to my family for their guidance, encouragements, moral support and their patience in tolerating my idiosyncrasies throughout my course of study and research work.

I certify that an Examination Committee met on 07 September 2007 to conduct the final examination of Fatemeh Azimzadeh on her Master of Science thesis entitled “Incorporating Certification Revocation and Time Concept into a Trust Model for Information Security Systems” in accordance with Universiti Pertanian Malaysia (Higher Degree) Act 1980 and Universiti Pertanian Malaysia (Higher Degree) Regulations 1981. The Committee recommends that the candidate be awarded the Master of Science.

Members of the Examination Committee are as follows:

Abd Rahman Ramli, PhD
Associate Professor
Faculty of Engineering
Universiti Putra Malaysia
(Chairman)

Mohamad Khazani Abdullah, PhD
Professor
Faculty of Engineering
Universiti Putra Malaysia
(Internal Examiner)

M. Iqbal Saripan
Lecturer
Faculty of Engineering
Universiti Putra Malaysia
(Internal Examiner)

Rahmat Budiarto
Associate Professor
School of Computer Sciences
Universiti of Science Malaysia
(External Examiner)

HASANAH MOHD. GHAZALI, PhD
Professor and Deputy Dean
School of Graduate Studies
Universiti Putra Malaysia

Date:

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:

Borhanuddin Mohd. Ali, PhD
Professor
Faculty of Engineering
Universiti Putra Malaysia
(Chairman)

Sabira Khatun, PhD
Associate Professor
Faculty of Engineering
Universiti Putra Malaysia
(Member)

AINI IDERIS, PhD
Professor and Deputy Dean
School of Graduate Studies
Universiti Putra Malaysia

Date: 13 December 2007

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 at any other institution.

FATEMEH AZIMZADEH

Date: 6 November 2007

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

CA	Certification Authority
CREN	Corporation for Research and Educational Networking
CRL	Certificate Revocation List
CRS	Certificate Revocation System
CRT	Certificate Revocation Tree
IT	Information Technology
MIT	Massachusetts Institute of Technology
OCSP	On-line Certificate Status Protocol
PGP	Pretty Good Privacy
PKC	Public Key Cryptography
PKI	Public Key Infrastructure
QoI	Quality of Information
RCA	Root Certification Authority
RSA	Rivest- Shamir- Adleman
URL	Uniform Resource Locator

CHAPTER 1

INTRODUCTION

Trust has become a very important part of our lives. With the recent developments of networking technologies and especially the Internet, it can be assumed that the need to interact with other people face to face has decreased due to the remarkable growth in new online applications such as e-commerce, e-government, and digital libraries. Nevertheless, trust is still important if not between people, definitely between the electronic devices we use to interact with each other. However, networks and in particular the Internet, is inherently insecure. A hacker can corrupt data, steal sensitive information, or masquerade as another user. Public Key Infrastructure (PKI) is a prerequisite for security in networks and distributed systems.

Open networks allow users to communicate without any prior arrangements such as contractual agreement or organization membership. However, the very nature of open networks makes authenticity difficult to verify. Authentication cannot be based on public key certificates alone; it needs to include the binding between the key used for certification and its owner, as well as the trust relationships between users.

The Internet has become the network that makes many applications such as electronic mailing, peer-to-peer file sharing, internet phoning, online auctions,

online games, ad hoc networks and the like, possible. A common security problem faced by an internet user is that most or all other users of the network are unknown to them [1].

Communicating with an unknown user X brings up at least two crucial questions:

1. What is the real identity of X? Are they who they claim to be?

2. How reliable is X? Is it secure to use the services X offers?

The first question concerns the authenticity of the available information about X's identity, whereas the second question is about the trustworthiness of X as a service provider. In other words, (1) is about what X is, whereas (2) is about what X dose?

In large open networks, handling trust and authenticity adequately is an important prerequisite for security. The authenticity of the public key of a user can be established by using certificates. Because of e-commerce, several organizations are setting up public key infrastructures. For example, the Massachusetts Institute of Technology (MIT) and the Corporation for Research and Educational Networking (CREN) propose to set up a hierarchical authentication structure for secure source-sharing among higher education institutions [2].

Trust is important because the current information infrastructure is rife with boundaries: individuals work and connect from multiple machines,

organizations, roles and activities. On the other hand, public key cryptography is a technology that enables users to make effective trust judgments across such boundaries. The term “trust metric” can be defined as the measure of trust attached to something, while confidence value stands for the degree of certainty that a piece of evidence or hypothesis is true. In a probabilistic model, the trust metric is referred to as the confidence value.

Properly managing authenticity and trust in a distributed network is not trivial and most approaches are based on a corresponding formal model. There is a general distinction between the centralized and decentralized models. For the former, the responsibility of issuing various forms of credentials is taken over by a central authority. One can think of a credential as a digitally signed statement or attestation about what another user is or does.

A centralized model usually requires all network users to fully trust the central authority, whereas in a decentralized model, every user is a potential issuer credentials such as authentication, certification, recommendation or revocation. The centralized models can be regarded as special cases of decentralized ones.

1.1 Problem Statements and Motivation

Certification is a common mechanism for authentic public key distribution. In order to obtain a public key, verifiers need to extract a certificate path from a

network of certificates, which is called a public key infrastructure (PKI), An entity X uses a trust path (or chain of trust) in order to validate authenticity between himself/herself at the starting point of the chain and the entity Y in the final point of the chain so that each public key is certified by the previous entity in the path. The chain is called a path of trust.

Research [3] emphasis: “PKIs are complex distributed systems that are responsible for giving users enough information to make reasonable trust judgments about one another”. Since PKI provides trust and certificates, users who make trust decisions must do so using only initial trust beliefs about the PKI and some certificates (and other assertions), as well as revocation of certification they received from the PKI.

A PKI needs to issue digital certificates to individuals and organizations, manage the certificates during their life cycles, and publish information about the certificates; certificate revocation is a necessary part of the certificate process. Revocation means invalidating the public key before its expiration date. There are many reasons why a certificate may be revoked long before it expires, for example, a user might change organizations or lose his or her key pair. Figure 1.1 shows the rate of certification revocation in certain environments.

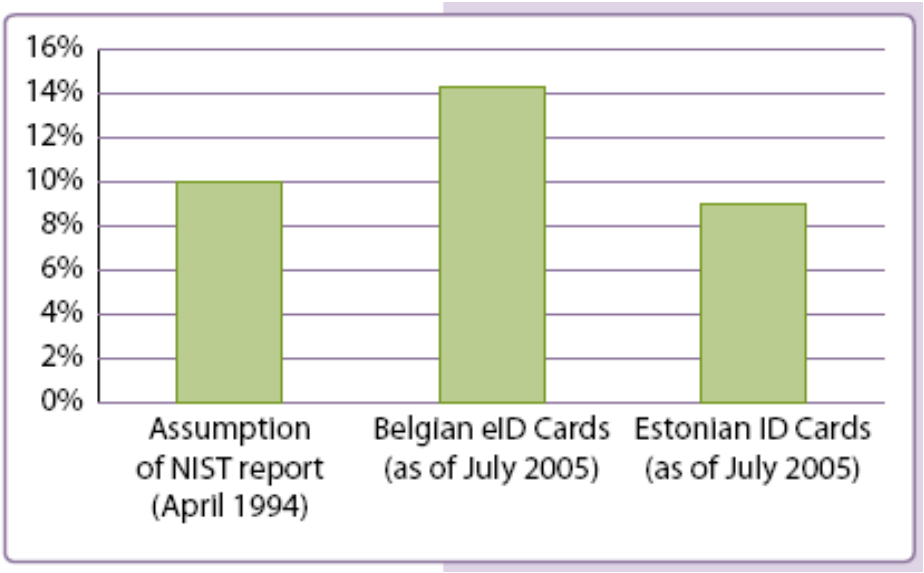

Figure 1.1: Certification Revocation Rates in Different Environments [4]

While revocation happens, it is not considered in the traditional model of trust. How can the verifier assure that the public key was not revoked at the time of signing (or verifying)? Previous works implicitly assume that there would be no revocation at all, or in a fully-trusted way there is always a fresh check verifying that the certificate is not revoked [5].

One aspect that research on trust and reputation systems strives to determine is a suitable digital representation of trust, commonly referred to as a trust model [6]. Tightly interwoven with trust models are the algorithms used to determine how this trust is updated according to different and usually discrete events such as certification revocation. For centralized trust models, central management is responsible for issuing revocation. For decentralized trust models, every user is a potential issuer of certification as well as revocation.

Trust issues influence both the specification of security policies, as well as the techniques needed to manage [7] and implement these security policies for systems. A theory of trust for a given system consists of a set of rules that specify the behavior (or functions) of the security mechanisms.

Trust changes over time. Even if no changes in factors that influence trust occur, the value of trust at the end of the period is not the same as that at the beginning of the period until such a time those users gradually become non-decisive or uncertain about the trust decision. [8]. This leads to the claim that trust decays over time, some happen like as refreshes of trust can change this process. Hence a complete model of trust needs to consider the concept of time. Consequently, the target is to develop a new model by upgrading Maurer's model considering certification, revocation and time concept.

1.2 Scope of Research

Maurer's model was chosen because this model is general in three ways. First of all, the model includes certification and recommendation, secondly, Maurer's model makes it possible to attach a confidence parameter, and thirdly the deterministic part of the model stands out. The model is simple, flexible, and can used to reason about PKI. This model is a decentralize model.