

**SECURITY FRAMEWORK BASED ON REPUTATION MECHANISM
FOR PEER-TO-PEER SYSTEMS**

By

SUBBA RAO SINNANAIDU

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

March 2004

*To,
My mother and grandmother,
Great and Grand,
For Their Neverending
Love and Support...*

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

**SECURITY FRAMEWORK BASED ON REPUTATION MECHANISM
FOR PEER-TO-PEER SYSTEMS**

By

SUBBARAO SINNANAIDU

March 2004

Chairman : Professor Borhanuddin Mohd. Ali, Ph.D.

Faculty :Engineering

Peer-to-peer networks have emerged over the past several years as a new and effective way for distributed resources to communicate and cooperate. Peer-to-peer computing is the sharing of computer resources and services by direct system exchange. These information sharing environments are increasingly gaining acceptance on the Internet as they provide an infrastructure in which the desired information can be located and downloaded while preserving the anonymity. Some of the peer-to-peer networks such as Napster and Gnutella which support anonymity, open doors to possible misuse and abuse of the network resources. This is apparent in the spread of tampered resources, malicious program such as Trojan Horses and viruses by resource provider itself.

In this thesis, a Peer Security Framework (PSF) has been developed using reputation-based mechanism to address these problems. This is done by an approach where the servants can keep track and share the information about the reputation of their peers with other peers. The “reputation sharing” based on a distributed polling

algorithm in which the resource requestors can assess the reliability of respective provider before initiating the download. This approach nicely complements the existing peer-to-peer protocols and gives a limited disruption on current implementations. Furthermore, it maintains the current level of anonymity of requestors and providers as well as that of the parties sharing their views on other's reputations.

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

**KERANGKA KESELAMATAN BERASASKAN MEKANISMA REPUTASI
UNTUK SISTEM PEER-TO-PEER**

Oleh

SUBBA RAO SINNANAI DU

March 2004

Pengerusi : Professor Borhanuddin Mohd. Ali, Ph.D.

Fakulti : Kejuruteraan

Rangkaian rakan sebaya telah muncul sebagai satu kaedah yang baru dan berkesan untuk sumber-sumber teragih berkomunikasi dan berkerjasama. Pengkomputeran rakan sebaya merupakan perkongsian sumber dan perkhidmatan melalui pertukaran secara langsung. Senario perkongsian maklumat ini semakin mendapat sambutan dalam Internet kerana ia membekalkan suatu infrastruktur di mana maklumat yang dikehendaki boleh didapati tanpa mendedahkan pengenalan pembekal. Sesetengah rangkaian rakan sebaya seperti, Napster dan Gnutella yang menyokong anonimiti membuka ruang kepada penyalahgunaan sumber dan maklumat rangkaian. Keadaan ini lebih jelas dengan penyebaran sumber maklumat yang dimodifikasi serta program-program perosak seperti Trojan Horse dan virus oleh pembekal sumber tersebut.

Dalam tesis ini, kerangka keselamatan peer (PSF) telah direkabentuk dengan menggunakan mekanisma berasaskan reputasi untuk mengatasi masalah ini. Ini dapat dilakukan dengan mencadangkan suatu kaedah di mana server dapat

memantau dan berkongsi maklumat tentang reputasi rakan dengan yang lain. Perkongsian reputasi (Reputation Sharing) ini berasaskan algoritma polling teragih di mana pengguna dapat menentukan kesahihan maklumat tersebut sebelum memuat-turunkannya. Kaedah ini dapat disesuaikan dengan protokol rakan sebaya di mana ia dilaksanakan tanpa menjejaskan pelaksanaan sedia ada. Di samping itu, ia dapat mengekalkan tahap anonimiti pengguna dan pembekal serta pihak-pihak yang berkongsi pandangan tentang reputasi sesuatu pihak lain

ACKNOWLEDGEMENTS

First and foremost, I owe my gratefulness to almighty Lord for giving me the strength and willpower to complete this research.

I would like to express my earnest gratitude to my supervisor, Prof. Dr Borhanuddin Mohd. Ali for believing in me enough to help me grow throughout my research. He also provided me a lot of freedom to explore and investigate the research topics and ideas that I found interested. I'm really impressed with the mastery of different aspects with which he maintained.

I am no less grateful to my committee members, Tuan Syed Abd. Rahman Al-Hadad Syed Mohamed and Shaiful Jahari Hashim, who were kind enough to read and comment on my work.

Thanks to my parents especially my mother Mrs Somualamah, brother and sisters for having the faith and believe in me, that I could do it. Most of all, I thank my granny Mrs Simhachalam for offered advice and wisdom from the very beginning that helped to bring this research to completion.

Thanks also to Vijay Babu, for his encouragement and support. He was always available for providing useful direction and advice when I needed. I feel happy to have friend like him.

Special thanks also go to all the colleagues and fellow friends such as Choong Khong Neng, Deepalaxmi, Hisham Zuhdi and Jeevan Rao for their assistance through my research.

I certify that an Examination Committee met on 19th March 2004 to conduct the final examination of Subba Rao s/o Sinnanaidu on his Master of Science thesis entitled "Security Framework Based on Reputation Mechanism for Peer-to-Peer 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 relevant degree. Members of the Examination committee are as follows:

Sudhanshu Shekhar Jamuar, Ph.D.

Professor
Department of Electrical and Electronic Engineering
Faculty of Engineering
Universiti Putra Malaysia
(Chairman)

Borhanuddin Mohd. Ali, Ph.D.

Professor
Department of Computer and Communication Engineering
Faculty of Engineering
Universiti Putra Malaysia
(Member)

Tuan Syed Abd. Rahman Al-Hadad Syed Mohamed

Department of Computer and Communication Engineering
Faculty of Engineering
Universiti Putra Malaysia
(Member)

Shaiful Jahari Hashim

Department of Computer and Communication Engineering
Faculty of Engineering
Universiti Putra Malaysia
(Member)

GULAM RUSUL RAHMAT ALI, Ph.D.

Professor/Deputy Dean
School of Graduate Studies
Universiti Putra Malaysia

Date :

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

Borhanuddin Mohd. Ali

Professor
Faculty of Engineering
Universiti Putra Malaysia
(Chairman)

Tuan Syed Abd. Rahman Al-Hadad Syed Mohamed

Faculty of Engineering
Universiti Putra Malaysia
(Member)

Shaiful Jahari Hashim

Faculty of Engineering
Universiti Putra Malaysia
(Member)

AINI IDERIS, Ph.D.

Professor/Dean
School of Graduate Studies
Universiti Putra Malaysia

Date :

DECLARATION

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

SUBBA RAO s/o SINNANAIDU

Date :

TABLE OF CONTENTS

	Page
DEDICATION	ii
ABSTRACT	iii
ABSTRAK	v
ACKNOWLEDGEMENTS	vii
APPROVAL	ix
DECLARATION	xi
LIST OF FIGURES	xv
LIST OF ABBREVIATION	xvi
 CHAPTERS	
1	INTRODUCTION
1.1	An Overview 1
1.2	History of Peer-to-Peer 2
1.3	Peer-to-Peer Vs Client-Server 4
1.4	Internet Security Issues 4
1.5	Problem Statement 6
1.5	Objectives 6
1.6	Organization of the Thesis 7
2	LITERATURE REVIEW
2.1	Introduction 8
2.2	Peer-to-Peer Architecture 8
2.2.1	Advantages of Pure Peer-to-Peer Network 9
2.2.2	Disadvantage of Pure Peer-to-Peer Network 10
2.3	Hybrid Peer-to-Peer Network 12
2.3.1	Advantages of Hybrid Peer-to-Peer Network 13
2.3.2	Disadvantages of Hybrid Peer-to-Peer Network 13
2.4	Napster 14
2.4.1	Napster Architecture 14
2.4.2	Napster Search Scenario 15
2.4.3	Napster Security 16
2.5	FreeNet 17
2.5.1	Freenet Architecture 17
2.5.2	Freenet Search Scenario 18
2.5.3	Freenet Security 20
2.6	Groove 21
2.6.1	Groove Architecture 22
2.6.2	Groove Security 24
2.7	Gnutella 27
2.7.1	Gnutella Architecture 27
2.7.2	Gnutella Search Scenario 30
2.8	Conclusion 31

3	METHODOLOGY	
3.1	Introduction	32
3.2	Peer Security Framework (PSF)	32
3.3	Peer Security Framework Architecture	34
3.3.1	Resource Searching	36
3.3.2	Resource Selection and Polling	36
3.3.3	Vote Evaluation	37
3.3.4	Resource Download	38
3.4	Maintaining Servents Reputation and Credibility	38
3.4.1	Representing Reputations	39
3.4.2	Translating Local Reputations into Votes	39
3.4.3	Representing Credibilities	40
3.5	Securing Votes	41
3.6	Implementation of PSF	42
3.6.1	Hardware Requirement	42
3.6.2	Software Requirement	43
3.6.3	Functional Specification of The PSF	44
3.6.3.1	Search Session Service	45
3.6.3.2	Reply Session Service	49
3.7	Design of PSF	50
3.8.1	Protocol Design	50
3.8.2	Application Design	54
3.8	Conclusions	57
4	RESULTS AND DISCUSSION	
4.1	Introduction	59
4.2	Experimental Setup	59
4.2.1	Network Configuration	59
4.2.2	Machine Configuration	61
4.3	Functional Testing	62
4.3.1	System Connectivity	62
4.3.2	Application Connectivity	63
4.3.2.1	Search System	64
4.3.2.2	Download System	64
4.3.2.3	Sharing System	65
4.3.2.4	Settings System	66
4.3.2.5	Voting System	67
4.3.2.6	Reputation System	68
4.3.2.7	Credibilities System	69
4.4	Flow of Operation	70
4.5	Security Evaluation	78
4.5.1	Distribution of Tampered Information	78
4.5.2	Self Replication	80
4.5.3	Pseudospoofing	81
4.5.4	IP Stealth	81
4.5.5	Shilling	82

4.6	Conclusions	82
5	CONCLUSION AND FUTURE WORK	
5.1	Contributions of The PSF	84
5.2	Future Work	86
	REFERENCES	89
	APPENDIXS	
	APPENDIX A	94
	BIODATA OF THE AUTHOR	106