Enhanced Moving Target Defense Mechanisms to Handle Cyber Attacks

By

M. UMA

(10PH076)

Supervisor

Dr. G.PADMAVATHI

A Thesis Submitted to

Avinashilingam Institute for Home Science and Higher Education for Women, University, Coimbatore - 641 043

In partial fulfilment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

IN

COMPUTER SCIENCE

June 2014

ACKNOWLEDGEMENTS

First and foremost, I am extremely thankful to the **LORD ALMIGHTY** for his graces and blessings bestowed on me.

I would like to place on record my reverential gratitude to **Late Ayya Dr. T. S. Avinashilingam Avl.**, Founder and President and First Chancellor of Avinashilingam University for Women, Coimbatore for providing the temple of learning and also for his heavenly blessings. I also owe my sincere and humble gratitude to **Late Amma Dr. Rajammal P. Devadas Avl., M.A., M.Sc., Ph.D.** Former Chancellor, Avinashilingam University for Women, Coimbatore

I record my sincere thanks to **Late Anna Mr. T. K. Shanmuganandam, B.A.,B.L.,** Former Chancellor, Avinashilingam University for Women, Coimbatore for providing the platform to carry out the research.

I record my sincere thanks to **Dr. T. S. K. Meenakshi Sundaram,** Chancellor, Avinashilingam University for Women, Coimbatore for providing the infrastructure for the conduct of the research.

I express my sincere and heartfelt thanks to **Dr. Sheela Ramachandaran, M.Sc., PG. Dip., Ph.D.**, Vice Chancellor, Avinashilingam University for Women, Coimbatore for providing necessary facilities and resources for the successful completion of this research work.

I express my sincere thanks to **Dr. Saroja Prabhakaran, M.A., Dip. Ed, Ph.D.**, Former Vice Chancellor, Avinashilingam University for Women, Coimbatore for motivating me to carryout the research, the constant encouragement, timely help, care and advice throughout the research.

I extend my gratitude to **Dr. Gowri Ramakrishnan, M.Sc., M.Phil., Ph.D.,** Registrar, Avinashilingam University for Women, Coimbatore for providing the infrastructure for the conduct of the research.

I express my heartfelt thanks to Dr**. P. Santhanakrishnan**, Director, Research and Consultancy, Avinashilingam University for Women, Coimbatore, for giving an opportunity to do research work.

I express my sincere and heartfelt thanks to **Dr. R. Parvatham M.Sc., Dip.Ed., M.Phil., Ph.D.,** Former Dean, Faculty of Science, Avinashilingam University for Women, Coimbatore for her spontaneous and timely help and amenities provided for the successful completion of this research work.

I also record my thanks to **Dr. Mrs. Parvathi,** Dean, Faculty of Science, University for Women, Coimbatore for motivating me to carryout the research, the constant encouragement, care and advice throughout the research.

I feel extremely privileged and fortunate to have worked under the able guidance and professional supervision of my guide, **Dr. G.PADMAVATHI, M.Sc., M.Phil., Ph.D.,** Professor and Head, Department of Computer Science, Avinashilingam University for Women, Coimbatore. Her constant encouragements, motivation, valuable and constructive suggestions and untiring support have guided me to gain and explore deep knowledge in the research field.

She helped me to define my research goals and showed the way to achieve them. Her able guidance, systematic approach guided me to put my best possible efforts in completing my work and documentation. Her sympathetic friendly nature, timely counseling, willingness to help at anytime, anywhere and at any situation during the entire period of the study have molded this research into a reality.

I record my gratitude to all **Ph.D** and **M.Phil Research Scholars, Faculty members** of Department of Computer Science, **Researchers** working in sponsored projects and **Staff Members** of Computer Center, Avinashilingam University for Women, Coimbatore for their encouragement and support.

I also thank My Mother **Mrs.M.Malliga**, My Brother **Mr.M.Arunkumar**, My Grandma **Mrs.D.SriRengathammal**, My Uncle **Mr.Alpandi Kannan** and **Mr.T.Jeyaraman,** My cousin **Mr.R.Praveen Kumar**, **Mr.M.Rangaraj** and **Mr.D.Augustin**, My Sister **Mrs.M.Chitra**, My brother-in-law **Mr.Anantharaj Apisek**, My Nephew **Master.N.Swaraj Kanna**, **Master.Abinesh Peter Solomon** and **Master.Adriel Jebi**, My Niece **Miss.N.Yadavi**, My Friend **Mr.P.Prem Kumar**, **Ms.R.KalpanaBharathi** and **my entire family** for their patience, wishes, prayers, encouragement and constant support extended to me at all the times throughout my career. I also thank all my **Friends, Relatives** and My well wishers **Dr.S.Chidambaranathan** and **Mr.N.Kumar** for their support and encouragement.

M. UMA

ABSTRACT

Secure communication in networking is still an open challenge due to the rapid development in technology. The increased use of networking makes the communication vulnerable to active and passive attacks. The decisive aim of the security is to maintain Confidentiality, Availability, Integrity, Non- repudiation and Authentication. According to a 2012 survey, that every organization is experiencing with an average of 102 attacks every week.

Based on the literature review, it is observed that efficient defense mechanisms are essential to defend against known and unknown cyber attacks. Game changing approaches are suggested as a defense mechanism to handle such attacks. The three game changing approaches namely, Trusted Tailored Spaces, Moving Target Defense Mechanisms and Cyber Economics are suggested as Research and Development Essentials. Among the three, moving target defense mechanisms are not explored much and only a few of them are used to handle attacks.

Moving target is a dynamic concept as it confuses the attackers by moving the real target often based on time or event. In the National Cyber Leap Year Summit Participants Report 2009, there are 11 moving target defense mechanisms suggested. According to the co-chairs' report, four moving target defense mechanisms are taken for study in this research work.

The objectives of the thesis are to Improve the quality of service in terms of End-to-end delay, Latency, Packet delivery ratio, Throughput, Reduce the number of retransmissions of data packets, Save time, Improve the accuracy of detection, Appropriate security application and Enhance storage security.

Few solutions are studied and enhanced. The proposed traffic monitoring technique achieves increased efficiency in traffic monitoring, adaptability for various network sizes, reduced retransmission and time saving. Cyber attack detection is done using the enhanced dimensionality reduction technique and the

outcome is improved accuracy in detection of known cyber attacks. The percentage of detection rate is 94%

For unknown cyber attack detection, four moving target defense mechanisms are implemented and improvised. They are Smart Motion Adaptation/Management - Game Theory, Robust Cryptographic Authentication - Mouse Dynamics, Data Chunking and Decentralization and Decoys. The above moving target defense mechanisms are enhanced to achieve the objectives of the thesis.

The secured hash based game theory approach is proposed. The experimentation is conducted using the NS2 simulator and the performance is estimated in terms of reduced end to end delay, increased packet delivery ratio, throughput. The proposed method also ensures neighbor authentication. The cyber attack detection rate is 71%.

Enhanced mouse dynamics is another method which outperforms the existing method in terms of reduced authentication time, reduced false acceptance rate, reduced false rejection rate and increased accuracy in detection of unauthorized users. The detection accuracy is observed to be 73% .The proposed application is developed using JAVA 1.7 as front end and mysql as back end.

The improved data chunking using non-sequential storage has showed better performance than the existing method and it achieves development of an application, robust security and increased storage durability. It also achieves increased accuracy in detection of unknown cyber attacks. The percentage of detection rate is 79% when compared to Mark W. Storer method. The proposed application is developed using JAVA 1.7 as front end and mysql as back end.

The Integrated Time and Event Triggered approach is proposed and tested using Network Simulator NS2. Simulation results show that the proposed method performs better than the existing methods. The percentage of detection rate is 83%

It also achieves reduced end to end delay, increased packet delivery ratio and improved throughput.

From the experimental and simulation results, it is observed that the four proposed methods are robust against known and unknown cyber attacks.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACRONYMS

QoS	Quality **o**f **S**ervice
DoS	Denial of Service
SNMP	Simple Network Monitoring Protocols
RMON	Remote Monitoring
PCA	Principal Component Analysis
LDA	Linear Discriminant Analysis
ICA	Independent Component Analysis
CLP	Conditional Legitimate Probability
DDoS	Distributed Denial-of-Service
PCANNA	Principal Component Analysis Neural Network Algorithm
ROC	Receiver Operating Characteristic
FAR	False Acceptance Rate
FRR	False Rejection Rate
NDN	Named Data Networking
ICN	Information-Centric Networking
IPCA	Incremental Principal Component Analysis
HMM	Hidden Markov Model
DR	Data Representation
WLAN	Wireless Local Area Network
RMTI	Routing with Metric-based Topology Investigation
RIPv2	Routing Information Protocol
TTCAN	Time Triggered Controller Area Network
RODL	Round Description List
ET	Externally Triggered
IT	Internally Triggered
FOTG	Fault-Oriented Test Generation
SHARP	Sharp Hybrid Adaptive Routing Protocol

AODV	Ad hoc On-Demand Distance Vector
ECC	Elliptic Curve Cryptography
SVM	Support Vector Machine
SHA-512	Secured Hash Algorithm
AES	Advanced Encryption Standard
CDC	Content Defined Chunking
DSR	Dynamic Source Routing
TORA	Temporally Ordered Routing Algorithm
OLSR	Optimized Link State Routing Protocol
CBR	Constant Bit Rate
VBR	Variable Bit Rate
RIP	Routing Information Protocol
OSPF	Open Shortest Path First