

DETECTION AND PREVENTION OF ARP SPOOFING

A PROJECT REPORT

Submitted by

R.PARTHIBAN (810015104057)

In partial fulfilment for the award of the degree

Of

**BACHELOR OF ENGINEERING
IN
COMPUTER SCIENCE AND ENGINEERING**



**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
UNIVERSITY COLLEGE OF ENGINEERING
BHARATHIDASAN INSTITUTE OF TECHNOLOGY CAMPUS
ANNA UNIVERSITY, TIRUCHIRAPPALLI - 620 024.**

APRIL 2019

BONAFIDE CERTIFICATE

Certified that this project report titled “**Detection and Prevention of ARP Spoofing**” is a bonafide work of **R. Parthiban (810015104057)** who carried out the work under my supervision, for the partial fulfilment of the requirements for the award of the degree of Bachelor of Engineering in Computer Science and Engineering at University College of Engineering, Bharathidasan Institute of Technology Campus, Anna University, Tiruchirappalli. Certified further that to the best of my knowledge and belief, the work reported herein does not form part of any other thesis or dissertation on the basis of which a degree or an award was conferred on an earlier occasion.

SIGNATURE OF HOD

Dr. D. VENKATESAN

Assistant Professor & Head
Department of CSE-IT
University College of Engineering,
Campus,
Tiruchirappalli -620 024

SIGNATURE OF GUIDE

Mr. S. SURENDRAN

Teaching Fellow
Department of CSE
University College of Engineering, BIT
BIT Campus,
Tiruchirappalli - 620 024

Submitted for the CS6811 Project Viva-voce examination held on _____

Internal Examiner

External Examiner

DECLARATION

We hereby declare that the work entitled “**Detection and Prevention of ARP Spoofing**” is submitted in partial fulfilment of the requirements for the award of the degree in B.E , in University College of Engineering, BIT Campus, Anna University, Tiruchirappalli . It is record of the our own work carried out by us during the academic year 2017-2018 under the supervision and guidance of **Mr. S. SURENDRAN**, Teaching Fellow, Department of Computer Science and Engineering, University College of Engineering, Bharathidasan Institute of Technology Campus, Anna University, Tiruchirappalli. The extent and source of information are derived from the existing literature and have been indicated through the dissertation at the appropriate places. The matter embodied in this work is original and has not been submitted for the award of any other degree, either in this or any other university.

R. Parthiban
(810015104057)

I certify that the declaration made above by the candidate is true.

Mr.S.SURENDRAN
Teaching Fellow
Department of CSE/IT

ACKNOWLEDGEMENT

I would like to thank our honorable Dean **Prof. Dr. D. SENTHIL KUMAR**, Professor for having provided us with all required facilities to complete our project without hurdles.

I would also like to express our sincere thanks to **Dr. D.VENKATESAN**, Head, Department of Computer Science and Engineering, for his valuable guidance, suggestions and constant encouragement paved way for the successful completion of this project work.

I would like to thank our Project Coordinators **Mr. C. SANKARRAM, Mr. P. KARTHIKEYAN and Mr. C. SURESH KUMAR** of Department of Computer Science for their kind support.

I wholeheartedly thank and express our deep sense of gratitude to our project guide **Mr. S. SURENDRAN**, Teaching Fellow, Department of Computer Science and Engineering, Anna University, Tiruchirappalli, for his valuable guidance throughout the project.

I also extend our thanks to all other teaching and non-teaching staff for their encouragement and support.

I thank our beloved parents and friends for their full support in the moral development of this project.

TABLE OF CONTENTS

CHAPTER NO	TITLE	PAGE NO
	ABSTRACT	viii
	LIST OF FIGURES	ix
	LIST OF ABBREVIATIONS	x
1	INTRODUCTION	1
	1.1 OVERVIEW	1
	1.2 ADDRESS RESOLUTION PROTOCOL	3
	1.3 WORKING OF ARP	5
	1.4 ARP SPOOFING	7
	1.5 METHODS OF ARP SPOOFING	8
2	LITERATURE SURVEY	10
3	SYSTEM ANALYSIS	14
	3.1 EXISTING SYSTEMS	14

3.1.1	Limitations	15
3.2	PROPOSED SYSTEM	16
4	SYSTEM SPECIFICATIONS	17
4.1	SOFTWARE REQUIREMENTS	17
4.2	HARDWARE REQUIREMENTS	17
4.3	ABOUT THE SOFTWARE	17
5	SYSTEM DESIGN	21
5.1	SYSTEM ARCHITECTURE	21
5.2	MODULE DESCRIPTION	22
5.2.1	Implementation of ARP Spoofing	22
5.2.2	Detection of ARP Spoofing	23
5.2.3	Prevention of ARP Spoofing	24
5.3	EXPERIMENTAL RESULTS	24

6	CONCLUSION AND FUTURE WORKS	25
	6.1 CONCLUSION	25
	6.2 FUTURE WORKS	25
	APPENDICES	
	SAMPLE SOURCE CODE	26
	SAMPLE SCREENSHOTS	29
	REFERENCES	34

ABSTRACT

Address Resolution Protocol (ARP) has been in use since the advent of Open System Interconnection (OSI) Network Architecture. It has been working in Network layer for The conversion of Network Address i.e. Internet Protocol (IP) Address to Physical Address or Media Access Control (MAC) Address. However it does not include any Security measures against malicious attacks, in its design, an attacker can invade another Host by using ARP spoofing. ARP spoofing is a type of attack in which a malicious attacker sends falsified ARP messages over a Local Area Network .Therefore a strong need is felt to harden the security system. Since LAN is used in maximum organisations to get the different computers communicated. So an attempt has been made to enhance the work of ARP protocol to work in a more secure way. But the architecture of ARP is such that all the efforts made till have not been proven ultimate solution. A new approach for detection and prevention of ARP spoofing has been designed. This approach sets Media Access Control Address (MAC) of the Default Gateway static but logs all changes history. This software can protect us from MITM attacks on ARP cache.

LIST OF FIGURES

FIGURE NO.	TITLE	PAGE NO.
1.1	ARP packet format	3
1.2	Using ARP ,client acquires MAC Address with its IP address	5
1.3	ARP Spoofing –reply packet sent to victim	8
5.1	Architecture of Proposed system	21

LIST OF ABBREVIATIONS

ARP	Address Resolution Protocol
MAC	Media Access Control
IP	Internet Protocol
TCP	Transmission Control Protocol
LAN	Local Area Network
DHCP	Dynamic Host Configuration Protocol
DAI	Dynamic ARP Inspection
MITM	Man In The Middle Attack
IDS	Intrusion Detection System
DOS	Denial Of Service
DSA	Digital Signature Algorithm
GUI	Graphical User Interface