

LB/DON/29/2015

2E10 06/14

**DEVELOPING A STRATEGY AND AN OPEN MODULE  
FOR N-SBC TO ELIMINATE DDOS ATTACKS FROM  
SIP BASED NGN IP INTERCONNECTIONS**

Sanjeevane Nadeesha Weerasinghe

(08/8403)

LIBRARY  
UNIVERSITY OF MORATUWA, SRI LANKA  
MORATUWA

Dissertation submitted in partial fulfillment of the requirements for the degree Master  
of Science in Telecommunications

University of Moratuwa



108894

Department of Electronic & Telecommunication Engineering

University of Moratuwa

Sri Lanka

621.39 "13"

621.39(043)

February 2013

108894

**108894**

## DECLARATION

I declare that this is my own work and this dissertation does not incorporate without acknowledgement any material previously submitted for a Degree or Diploma in any other University or institute of higher learning and to the best of my knowledge and belief it does not contain any material previously published or written by another person except where the acknowledgement is made in the text.

Also, I hereby grant to University of Moratuwa the non-exclusive right to reproduce and distribute my dissertation, in whole or in part in print, electronic or other medium. I retain the right to use this content in whole or part in future works (such as articles or books).

Signature: ***UOM Verified Signature***

Date: 12/07/2014

The above candidate has carried out research for the Masters Dissertation under my supervision.

Signature of the supervisor: ***UOM Verified Signature***

12/07/2014.

## **ABSTRACT**

The Session Initiation Protocol (SIP) is the communication protocol of the future. Used for Voice-over-IP (VoIP), Internet Multimedia Subsystem (IMS) and Internet Protocol Television (IPTV), SIP's concepts are based on mature and open standards and its usage is increasing rapidly. However, with its acceptance as a mainstream communication platform, security concerns become ever more important for users and service providers.

Usage of SIP for communication is currently spreading into the last mile of mobile and fixed line carriers making them very much vulnerable to the protocols of the internet domain.

The posed threat can be understood by the increasing number of calls being initiated from the internet to mobile and fixed line devices. At the crux, in order to manage the threats coming in from the internet, operators usually go for tighter Security in the Session Border Gateway (SBC), the interface between internet and the operator's domain.

Furthermore, rogue attempts to infiltrate the Operator's domain is now becoming a common occurrence and leading to losses beyond billions of dollars of revenue. Irony is that Operator's sometimes does not understand the scale of the exploitation until much later in the billing cycle.

This thesis identifies the probable modes of attacks including DoS and DDoS, and provides a strategy and an implementation plan to identify these threats via pattern matching and heuristic logic which is built on learning algorithms. Target is to introduce a solution capable of learning and identifying patterns which leads to DoS, DDoS attacks and eliminate the rogue communication threads from ever entering the realms of the operator.

With this solution, general VOIP communications with Operators shall be more robust against DoS and Distributed DoS attacks and many other threats looming at the N-SBS level of an NGN network.

## ACKNOWLEDGEMENT

First and foremost, I would like to express my deepest gratitude to my supervisor, Mr. Kithsiri Samarasinghe, not only for his support, encouragement and guidance, but also for his patience and availability. Without his guidance and persistent help I would not be able to complete this work.

Furthermore I wish to express my sincere thanks to our M.Sc. coordinators Dr. Ajith Pasqual and Dr. Chandika Wavegedara for their untiring supervision and guidance throughout the research work.

Many thanks to my husband, for all his love, affection and understanding throughout my research work. I am also grateful to my wonderful family, to whom I owe everything I am.

Finally I would like to thank my team at Dialog for releasing me for research work when required.

## TABLE OF CONTENTS

DECLARATION .....	i
ABSTRACT .....	ii
ACKNOWLEDGEMENT .....	iii
TABLE OF CONTENTS .....	iv
LIST OF FIGURES .....	vii
LIST OF TABLES .....	viii
LIST OF ABBREVIATIONS .....	ix
<b>CHAPTER 1 : INTRODUCTION.....</b>	<b>1</b>
<i>1.1 Introduction and literature survey .....</i>	<i>1</i>
1.1.1 Motivation .....	1
1.1.2 Related works and GAP Analysis.....	2
1.1.3 My proposed strategy and implementation overview .....	3
<i>1.2 SIP .....</i>	<i>3</i>
1.2.1. SIP Overview .....	3
1.2.1.1 Introduction to SIP .....	4
1.2.1.2 SIP Methods.....	5
1.2.1.3 SIP Response Code Classes.....	6
1.2.1.4 Elements of a SIP Network .....	6
User Agents.....	7
Servers.....	7
1.2.1.5 Locating SIP Servers .....	8
1.2.1.6 Location Services.....	8
1.2.2 Functions of the SIP Protocol .....	9
1.2.2.1. Address Resolution.....	9
1.2.2.2 Session-Related Functions.....	10
1.2.2.3 Non-session Related Functions .....	13
<i>1.3. Threats to SIP .....</i>	<i>15</i>
1.3.1 Analysis on SIP Security Focusing DoS/DDoS .....	15
1.3.2 Overview of general SIP security Threats and Related Works.....	16
1.3.3 Introduction on SIP DoS/ DDoS.....	18
1.3.3.4 SIP DoS / DDoS by Message Payload Tampering .....	19
1.3.3.5 SIP DoS / DDoS by Message Flow Tampering.....	21
1.3.4 REGISTER Attack .....	21
1.3.5 INVITE Attack.....	22
1.3.6 BYE Attack .....	23
1.3.7 CANCEL Attack .....	24

1.3.8 UPDATE Attacks.....	26
1.3.9 REFER Requests.....	26
1.3.10 SIP DoS / DDoS by Message Flooding.....	27
<i>1.4 Counter measures</i> .....	27
1.4.1 Why conventional security methods fail.....	27
1.4.2 Exploitable SIP Resources (Mostly Targeted Resources).....	28
1.4.2.1 Memory.....	28
1.4.2.2 CPU.....	29
1.4.2.3 Network Bandwidth.....	30
1.2.5 SIP Flooding Attack Scenarios.....	30
1.2.5.1 DoS / DDoS Attacks Based on Exhaustion of Memory.....	30
1.2.5.2 Possible Countermeasures against Memory Exploitation Attacks.....	31
1.2.6 CPU Attacks.....	32
1.2.5.3 Countermeasures against CPU Attacks.....	32
<b>CHAPTER 2 : SIMULATION AND STRATEGY DEVELOPMENT .....</b>	<b>33</b>
2.1 Introduction.....	33
2.2 Further Research.....	34
2.2.1 NetFlow.....	34
2.2.1 Abnormal Traffic Detection.....	35
2.3 Simulation of Network threats.....	36
2.3.1 Simulating SIP communication environment using NS2.....	36
2.3.2 Simulating DoS/DDoS attack using NS2 and Analyse the impact.....	37
2.3.2.1 Simulating a “No Attack” Scenario.....	37
2.3.2.2 Simulating a DoS Attack.....	38
2.3.2.3 Simulating a Distributed DoS (DDoS) Attack.....	39
2.3.3 Analyzing the Packet Loss Ratio.....	40
2.3.4 Simulate DDoS attacks with different Queues and Analyze the Impact.....	40
2.3.4.1 Simulating the DDoS Attack with a RED Queue.....	41
2.3.4.2 Simulating the DDoS Attack with a FQ Queue.....	42
2.3.4.3 Simulating the DDoS Attack with a DRR Queue.....	43
2.3.4.4 Simulating the DDoS Attack with a SFQ Queue.....	44
2.3.4.5 Simulating the DDoS Attack with a FIFO (Drop tail) Queue.....	45
2.3.5 Analyzing the Packet Loss Ratio.....	46
2.4 Strategy Development.....	46
2.4.1 The Role of Session Boarder Controllers in these changing times.....	46
2.4.2 Threats Posed by attackers.....	47
2.4.3 End to end DDoS Attack Scenarios.....	48
2.4.3.1 SPIT or Spam.....	49
2.4.3.2 Flooding.....	49
2.4.3.3 Enumeration.....	49
2.4.3.4 Cracking.....	50
2.4.3.5 Fraudulent Calls.....	50
2.4.4 SBC Security Framework.....	50
2.4.5 Probable parameters we can use to detect network traffic.....	52
<b>CHAPTER 3 : SOLUTION IMPLEMENTATION.....</b>	<b>53</b>

3.1 <i>Implementation Framework components</i> .....	53
3.1.1 Overall System components of the Implementation framework.....	53
3.2.1 Technologies that need to be used to make it Telco Grade.....	59
3.2.2 Design Best Practices for Optimization of Delay and Latency.....	59
<b>CHAPTER 4 : IMPLEMENTATION ISSUES</b> .....	<b>61</b>
4.1 <i>Operator framework</i> .....	61
4.2 <i>Scalability Enhancements</i> .....	61
4.3 <i>Real-time algorithm mapping</i> .....	61
4.4 <i>Operational analysis</i> .....	62
4.5 <i>Pattern Enhancements</i> .....	62
<b>CHAPTER 5 : CONCLUSION</b> .....	<b>63</b>
5.1 <i>Conclusion</i> .....	63
5.2 <i>Future Works</i> .....	64
<b>REFERENCE LIST</b> .....	<b>65</b>

## LIST OF FIGURES

FIGURE 1-1: NORMAL REGISTER FLOW .....	22
FIGURE 1-2: NORMAL SESSION TERMINATION .....	23
FIGURE 1-3: SPOOFED SESSION TERMINATION .....	24
FIGURE 1-4: NORMAL CANCEL FLOW .....	25
FIGURE 1-5: CANCEL ATTACK .....	25
FIGURE 2-1: CISCO NETFLOW V 9.0 .....	35
FIGURE 2-2: SIMULATING SIP COMMUNICATION ENVIRONMENT USING NS2 .....	37
FIGURE 2-3: SIMULATING A "NO ATTACK" SCENARIO .....	38
FIGURE 2-4: SIMULATING A DOS ATTACK .....	38
FIGURE 2-5: SIMULATING A DISTRIBUTED DOS (DDoS) ATTACK .....	39
FIGURE 2-6: ANALYZING THE PACKET LOSS RATIO .....	40
FIGURE 2-7: SIMULATING THE DDoS ATTACK WITH A RED QUEUE .....	41
FIGURE 2-8: SIMULATING THE DDoS ATTACK WITH A FQ QUEUE .....	42
FIGURE 2-9: SIMULATING THE DDoS ATTACK WITH A DRR QUEUE .....	43
FIGURE 2-10: SIMULATING THE DDoS ATTACK WITH A SFQ QUEUE .....	44
FIGURE 2-11: SIMULATING THE DDoS ATTACK WITH A FIFO (DROPTAIL) QUEUE .....	45
FIGURE 2-12: ANALYZING THE PACKET LOSS RATIO .....	46
FIGURE 2-13: SBC SECURITY FRAMEWORK .....	51
FIGURE 3-1: IMPLEMENTATION FRAMEWORK .....	53
FIGURE 3-2: SHAPE OF TRAFFIC PATTERNS AT IP AND APPLICATION LAYERS .....	56



## LIST OF TABLES

TABLE 1-1: SIP METHODS .....	5
TABLE 1-2: SIP RESPONSE CODE CLASSES .....	6
TABLE 1-3: SECURITY ISSUES ON NETWORK AND APPLICATIONS.....	16
TABLE 1-4: CLASSIFICATION OF SIP DOS / DDoS ATTACKS.....	18
TABLE 2-1: NPROBE MATRICES .....	36
TABLE 3-1: ANALYSIS MATRIX .....	58
TABLE 3-2: SAMPLE ANALYSIS .....	58

## LIST OF ABBREVIATIONS

AAA	Authentication, Authorization and Accounting
CAS	Channel Associated Signaling
CPU	Central Processing Unit
DDOS	Distributed Denial Of Services
DNS	Domain Name Server
DOS	Denial Of Services
HTTP	Hyper Text Transport Protocol
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPTV	Internet Protocol Television
MMUSIC	Multiparty Multimedia Session Control
NGN	Next Generation Network
N-SBC	Network Session Boarder Controller
RTP	Real-time Transport Protocol
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SMTP	Simple Mail Transport Protocol
SPIT	Spam over Internet Protocol Telephony
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UAC	User Agent Client
UAS	User Agent Server
UDP	User Datagram Protocol
URI	Uniform Resource Identifier
VoIP	Voice over Internet Protocol