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

Sanjeevanee Nadeesha Weerasinghe

(08/8403)

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

Department of Electronic & Telecommunication Engineering

University of Moratuwa

Sri Lanka

February 2013

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 it is 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 then 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 crust, in order to manage the threats coming in from the internet, operators usually go for tighter Security in the Session Boarder 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 leaning 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

LIST OF FIGURES

List of tables

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