The copyright of this thesis vests in the author. No quotation from it or information derived from it is to be published without full acknowledgement of the source. The thesis is to be used for private study or non-commercial research purposes only.

Published by the University of Cape Town (UCT) in terms of the non-exclusive license granted to UCT by the author.

University of Cape Town

Using Decoys to Block SPIT in the IMS

by

S.M. Akramus Salehin

BSc(ENG) Electrical and Computer Engineering (1st Class Hons)

A thesis submitted to the

Department of Electrical Engineering

The University of Cape Town

in fulfillment of the academic requirements

for the degree of

MSC(ENG) ELECTRICAL ENGINEERING

Supervisor: Mr. Neco Ventura

January, 2007

University of Cape Town

Statement of originality

I declare that the work presented in the thesis is, to the best of my knowledge and belief, original and my own work, except as acknowledged in the text, and that the material has not been submitted, either in whole or in part, for a degree at this or any other university.

University of Cape Town

S.M. Akramus Salehin

.....

January, 2007

Acknowledgments

Firstly, I would like to thank my supervisor, Mr. Neco Ventura, for his guidance and assistance during the thesis. Secondly, I would like to thank Mr. David Waiting for proof reading the thesis and his valuable comments. Last but not least, I would like to thank all members of the Communications Research Group (CRG) and Chan Group for their support and encouragements.

University of Cape Town

Abstract

Spam has been a serious problem for e-mail causing frustration and annoyance to the customers. This problem is growing at a very fast rate with no signs of abating. In recent years, studies have shown that 80-85% of e-mails sent were spam. Another form of spam that has just surfaced is VoIP (Voice over Internet Telephony) spam. Currently, VoIP has seen an increasing numbers of users due to the cheap rates. With the introduction of the IMS (IP Multimedia Subsystem), the number of VoIP users are expected to increase dramatically. This calls for a cause of concern, as the tools and methods that have been used for blocking e-mail spam may not be suitable for real-time voice calls. In addition, VoIP phones will have URI type addresses, so the same methods that were used to generate automated e-mail spam messages can be employed for unsolicited voice calls.

Spammers will always be present to take advantage of and adapt to trends in communication technology. Therefore, it is important that IMS have structures in place to alleviate the problems of spam. Recent solutions proposed to block SPIT (Spam over Internet Telephony) have the following shortcomings: restricting the users to trusted senders, causing delays in voice call set-up, reducing the efficiency of the system by increasing burden on proxies which have to do some form of bayesian or statistical filtering, and requiring dramatic changes in the protocols being used. The proposed decoying system for the IMS fits well with the existing protocol structure, and customers are oblivious of its operation. Further, the decoying method causes no delays in voice call set-up.

An evaluation framework is implemented for proof of concept and analysis of performance of the decoying system. This framework included two decoy UEs and two spammers. Moreover, several users acting as either receivers or senders is established to provide background voice calls. The decoying system performed

University of Cape Town

well under low load and high conditions. Further, the proposed solution blocked the spammers irrespective of the spammers' call rates. A stress test is performed proving that the decoying system causes little overheads to the system, and there is little delay in banning the spammers. Additionally, the decoying system did not cause any delays in call set up.

University of Cape Town

Contents

Statement of originality i

Acknowledgments ii

Abstract iii

List of Figures ix

List of Tables xi

List of Abbreviations xiii

1 Introduction 1

1.1 Background Information 1

1.2 Thesis Objectives 6

1.3 Scope and Limitations 7

1.4 Thesis Outline 8

2 Literature Review 11

2.1 Introduction 11

2.2 IMS 12

2.2.1 Subscription Information 14

2.2.2 Security Procedures 15

University of Cape Town

2.2.3 Delays in Session Initiation 16
2.2.4 Discussion on IMS 17
2.3 Spam 18
2.3.1 Email Spam Filtering Methods 18
2.3.2 Spam Legislation 21
2.3.3 Comparison of Email Spam and SPIT 21
2.3.4 Profitability of SPIT in the IMS 22
2.3.5 Related Work on Blocking SPIT 23
2.4 Chapter Discussion 25

3 Proposed Decoying Solution for SPIT **27**
3.1 Introduction 27
3.2 Design Requirements 27
3.3 Decoying to Block SPIT 30
3.3.1 Honeypot Architectures 32
3.4 Detailed Operation of the Decoying System 34
3.4.1 Retrieving URI of Sender 35
3.4.2 Routing of Message from Decoy UE to Sender's HSS . . . 37
3.4.3 Interface between Decoy UE and HSS 38
3.4.4 Modification of Service Profiles on the HSS 40
3.4.5 Algorithm for Minimising False Positives 41
3.4.6 Modification of System for Insecure Wireless Networks . . 43
3.5 Operation of Spammers in an IMS Domain 44
3.5.1 Scenario: IMS Procedure to Make a Voice Call 45
3.5.2 Scenario: Voice Call from Spammer to Decoy 46
3.5.3 Scenario: Voice call from Spammer Blocked 47
3.6 Mobility Requirements 47
3.7 Chapter Discussion 48

University of Cape Town

4 Implementation of an Evaluation Framework **49**

4.1 Introduction 49

4.2 Objectives and Requirements of the Evaluation Framework 50

4.3 Decision on Test Bed Implementation and Tools Used 53

4.4 Overview of the Test Bed 56

4.5 Detailed Implementation of Test Bed Components 59

4.5.1 Registration and Authentication 59

4.5.2 Background Traffic Generation 61

4.5.3 Spammers 63

4.5.4 Decoy UEs 64

4.5.5 Interface Between Decoy UE and HSS 65

4.5.6 HSS 66

4.5.7 S-CSCF 68

4.6 Chapter Discussion 69

5 Evaluation of Results and Analysis **71**

5.1 Introduction 71

5.2 Analysis of Methods to Filter SPIT 72

5.2.1 Historical Call Pattern Analysis 72

5.2.2 Reputation Networks and Trust 73

5.2.3 Multi-Stage Filters 75

5.2.4 Challenge-Response Methods 75

5.2.5 Proposed Decoying Method 76

5.2.6 Discussion 76

5.3 Proof of Concept Tests 77

5.3.1 Functions of the Decoy UE 78

5.3.2 Modifications to the HSS 79

University of Cape Town

5.3.3 Modifications to the S-CSCF 80
5.4 Performance Tests 83
5.4.1 Tests under Low Load 84
5.4.2 Tests under High Load 91
5.4.3 Stress Test 95
5.5 Chapter Discussion 99

6 Conclusions and Recommendations 101
6.1 Conclusions 101
6.2 Contributions Made 103
6.3 Future Work and Recommendations 104

Bibliography 106

A Details on the IMS 112
A.1 IMS Design Requirements 112
A.2 IMS Components 114
A.3 IMS Interfaces 116
A.4 IMS User Identities 117

B Installation Notes for Tools Used for the Evaluation Framework 119
B.1 SIPp 119
B.1.1 Adding patches 119
B.2 Iptel SER Installation 120
B.2.1 Adding MySQL Support 120

C Accompanying CD-ROM 122

University of Cape Town

List of Figures

2.1 Media policy operation with service profiles. 15

2.2 Operation of a multi-stage filter. 25

3.1 Operation of the proposed decoying system. 31

3.2 Blacklist messages sent via the S-CSCF. 32

3.3 Implementing virtual honeypots. 34

3.4 Structure of the SIP INVITE header before traversing the P-CSCF. 35

3.5 Modification of the P-CSCFs due to the Privacy header. 36

3.6 Message structure of the Spam-Id command. 39

3.7 Two additional databases required in the HSS for the decoying system. 42

3.8 Algorithm for minimising false positives, implemented on the HSS. 42

3.9 Operation of decoy UE in WLAN networks for the IMS. 43

3.10 Web crawler fetching email addresses and HTTP links for future sources of HTML documents. 45

3.11 Flow of the Initial SIP INVITE from UE#1 to UE#2. 45

4.1 Complete layout of the test bed. 58

4.2 Output from SIPp during registration of a receiver. 59

4.3 Format of REGISTRATION and 401 messages captured from the sip-router using ngrep. 60

4.4 SIP signalling done by the sender in the test bed. 61

University of Cape Town

4.5 SIP signalling done by the receiver in the test bed. 62
4.6 Operation of a decoy UE. 64
4.7 INVITE message structure in the evaluation framework, highlighting the URI of sender. 65
4.8 RSA keys stored on the decoy host. 66
4.9 Iptel SER architecture supporting databases on one host. 67
4.10 Table "grp" in the database displaying users allowed to initiate audio transmissions. 68
4.11 Flow chart showing program algorithm for processing decoy messages. 69
4.12 Messages exchange when a banned user initiates a voice call. . . 70

5.1 Generation of a social network. 74
5.2 Output from the decoys when they are hit by a spammer. 79
5.3 Table "grp" modification when a sender hits only one decoy UE. . 79
5.4 Table "grp" entries when sender hits two different decoy UEs. . . . 80
5.5 SIPp output showing user making voice calls. 81
5.6 SIPp output for a banned user trying to make voice calls. 81
5.7 Ngrep output from sip-router letting user know that he/she is banned. 82
5.8 Time required to ban a spammer sending voice spam with frequency of 1 call per 30 seconds. 84
5.9 Performance of decoys in blocking spammers under low load conditions. 90
5.10 Messages received by the two decoys in scenario 7. 90
5.11 Performance of decoys under high load conditions. 95
5.12 Operation of decoys during the stress test. 99

A.1 IMS components and interfaces. 116

University of Cape Town

List of Tables

2.1 Charging methods used by VoIP service providers [41]. 23

3.1 Mapping of diameter AVP parameters from Cx parameters. 39

4.1 Components needed for the test bed and their functions. 52

5.1 Configuration of the two decoy UEs on one host. 78

5.2 Total number of legitimate calls sent by the 8 senders under low load. 86

5.3 Total number of failed calls under low load. 87

5.4 Average response times under low load. 88

5.5 Distribution of response times in milliseconds (ms) under low load. 88

5.6 Average call duration under low load. 88

5.7 Statistics on spam messages under low load. 89

5.8 Delays in blocking spammers under low load conditions. 89

5.9 Total number of legitimate calls sent by the 8 senders under high load. 92

5.10 Total number of failed calls under high load. 92

5.11 Average response times under high load. 93

5.12 Distribution of response times in milliseconds (ms) under high load. 93

5.13 Average call duration under high load. 94

5.14 Statistics on spam messages under high load. 95

University of Cape Town

5.15 Delays in blocking spammers under high load conditions. 95
5.16 Total number of legitimate calls sent by the 8 senders during the stress test. 96
5.17 Total number of failed calls during the stress test. 97
5.18 Average response times during the stress test. 97
5.19 Distribution of response times from 0 to 50 ms during the stress test. 97
5.20 Distribution of response times, 50 ms and above, during the stress test. 98
5.21 Average call duration during the stress test. 98
5.22 Statistics on spam messages for the stress test. 99
5.23 Delays in blocking spammers for the stress test. 99

A.1 Functions of the IMS interfaces. 117

University of Cape Town

List of Abbreviations

AAA - Authentication, Authorisation, and Accounting
AKA - Authentication and Key Agreement protocol
API - Application Programming Interface
AS - Application Server
AVP - Attribute Value Pair
CK - Cipher Key
CSCF - Call Session Control Function
DHCP - Dynamic Host Configuration Protocol
DNS - Domain Name Server
DoS - Denial of Service
EXosip2 - EXtended osip 2
FTP - File Transfer Protocol
GSM - Global System for Mobile Communications
HSS - Home Subscriber Server
HTML - Hypertext Markup Language
HTTP - Hypertext Transfer Protocol
I-CSCF - Interrogating - Call Session Control Function
IK - Integrity Key
IMS - IP Multimedia Subsystem
ISC - IMS Service Control
ISIM - IMS Identity Module
ISP - Internet Service Provider
NDS - Network Domain Security
OSA - Open Services Architecture
PBX - Private Branch Exchange
P-CSCF - Proxy - Call Session Control Function

University of Cape Town

PDP - Packet Data Protocol
PIN - Personal Identification Number
PMG - Progressive Multi Gray-Levelling
PPA - Push Profile Answer
PPR - Push Profile Request
PTT - Push to Talk
QoS - Quality of Service
RNM - Reputation Network Manager
RTP - Real Time Transport Protocol
SAA - Server Assignment Answer
SAR - Server Assignment Request
S-CSCF - Serving - Call Session Control Function
SER - SIP Express Router
SIM - Subscriber Identity Module
SLF - Subscription Locator Function
SPIT - Spam over Internet Telephony
ssh - secure shell
TDM - Time Division Multiplexing
UE - User Equipment
UICC - Universal Integrated Circuit Card
UMTS - Universal Mobile Telecommunications System
URI - Uniform Resource Identifier
URL - Uniform Resource Locator
WAP - Wireless Application Protocol
WLAN - Wireless Local Area Networks
XML - eXtensible Markup Language

University of Cape Town

Chapter 1

Introduction

University of Cape Town

1.1 Background Information

The Internet is a worldwide collection of networks allowing individuals or institutions to connect to any point within this network without regard for geographical or national boundaries. Since its inception as a research project in 1969 called ARPANET, the Internet has continued to grow at an alarming rate. This is because the traffic traversing this global network has been doubling every year since 1997 [1]. Academia, government agencies and financial institutions have benefited from using this global network. Moreover, the benefits brought about by the Internet include ubiquitous access using the IP protocol suite, the ability of the user to manage his/her profile, an open service creation framework for content based services, a fast service deployment environment and many others. However, the openness of the Internet is a cause for concern in terms of the level of security that is provided. As a result, the Internet Society was started in 1991 in order to address the issues regarding security and privacy on the net.

Privacy concerns have been magnified by the increasing popularity of the net that allows databases to collect information, autonomously, about individuals [2]. Tools such as firewalls, access protection and file encryption are common in order to tackle this issue of data mining. Furthermore, malicious viruses and worms are prevalent on the Internet. One is susceptible to various security hazards including probes, scans, packet sniffing, denial of service and exploitation of trust

when connected to the net. Although the Internet was started for research purposes, recently collected statistics reveal that commercial use accounts for 58% of Internet traffic [3]. These commercial activities on the net have created a greater requirement for security than ever before.

The Internet is spreading to the mobile environments as well. Wireless Application Protocol (WAP) [4] was started as a framework and protocol that successfully brings Internet content to cellular phones and wireless devices. This widespread adoption of the Internet has increased the need for security measures. A study done by the CERT Coordination Centre on its network reported 100 malicious attacks in 1988. This value rose to 2 500 in 1995 [5]. It can be seen that there is a direct correlation between growth of the Internet and the increasing number of malicious attacks. The advantages of using the Internet are enormous, however, there is a need to appreciate the security risks involved with such an open architecture.

Electronic mail commonly known as email evolved side by side with the Internet. A rudimentary form of email existed from the days of time sharing computers. Programs capable of exchanging text messages were executed on these machines in several labs in the U.S. Today, several millions of email messages traverse the net every single day. Commercial users are forecasted to be receiving about 160 messages per day in 2006 [6]. This low cost, long distance means of communication has gained popularity side by side with the Internet. Consequently, the security concerns of the Internet are also present for email. Viruses and malicious code have been propagated using email [7]. Moreover, email messages can be compromised since the messages are not encrypted and must pass through intermediate computers on the way to the destination.

One of the problems in using email is the large of numbers of spam messages received each day per user. Spam is defined as unsolicited and junk mail [8] and must be differentiated from legitimate marketing messages. This problem is not abating, but the number of spam messages are increasing exponentially every year. Statistics obtained in September, 2005 illustrate that 67,6% of email was spam [7]. This means that there are 4 spam messages for every 6 email messages. One of the reasons why there is so much spam is that it is profitable. Spamming is a low cost means of mass marketing where a large number of people can be reached. And,

University of Cape Town

automated spamming software can be installed easily on computers with Internet access, to harvest email addresses, and send unsolicited bulk emails, saving the spammer time. Therefore, even a small percentage of people reading the spam or purchasing the goods advertised makes spamming a profitable venture [9].

Analogous to email as a popular packet based means of communication, VoIP (Voice over IP) is being adopted by a number of businesses and individuals. VoIP is the packetised transmission of analog voice after it has been digitised. Recent innovations in codecs and network technology have improved the quality of IP telephony. And, the adoption of VoIP is a result of its numerous advantages over traditional PSTNs. Not only are VoIP long distance calls cheaper but also offer extra features such as mobility, number portability, integration with email, multimedia features, and many others. Skype is one of the most popular VoIP services available today with over a million customers [10]. Other such VoIP services include Google Talk, Yahoo Messenger, and other SIP based applications. In a study conducted on developing countries, analyst reports predict that VoIP and mobile services will become the prevalent means of voice communications [11]. On the operator side, bandwidth is saved since VoIP is packet switched whereas PSTNs are circuit switched; and operating costs are reduced since voice and data are transmitted over a single converged network. The two most widely accepted protocols for VoIP are H.323 and SIP (Session Initiation Protocol) [12]. In recent times, SIP has enjoyed greater favour due to its openness and flexibility, although earlier VoIP systems were based on the H.323 protocol. However, there are downsides to using VoIP services as well.

VoIP is exposed to new threats such as Spam over Internet Telephony (SPIT). Analogous to email spam, SPIT are unsolicited bulk calls that are either taken by the user or left in voice mail. SPIT causes a greater inconvenience to the user since it is a real time service unlike email spam. Email spam waits in the inbox until the user is ready to read it. In contrast, voice calls need to be answered straight away. SPIT is causing concern for security experts and VoIP service providers. This problem can lead to Denial of Service (DOS), degradation of voice quality, and cause delays in call set-up. On the business perspective, time will be wasted handling spam calls and filtering out voice mail with marketing messages. The popular trend to VoIP coupled with inexpensive global calls will make it a lucrative technology for mass marketers. Even the most conservative

University of Cape Town

forecasts by Gartner [13] imply that by 2010, 5% of all spam will be SPIT.

VoIP users are set to increase significantly with the advent of the all-IP networks. Market conditions and technological progress is leading to a converged all-IP network in order to achieve reliability, cost-effectiveness, and satisfy customer demands for new services. The IP Multimedia Subsystem (IMS) [14] is an all-IP network architecture that has been standardised by the 3GPP and 3GPP2. IMS merges cellular networks with the Internet and existing circuit switched phone systems. Introduction of the IMS will make VoIP popular, this is a cause for concern since the tools and methods that have been used to block email spam may not be suitable for real time voice calls. In addition, VoIP phones will have URI type addresses, so the same methods that have been used for generating email spam messages can be used for unsolicited voice calls.

There are various legislation that are against email spam. These include the CAN-SPAM act of 2003 [15], the Criminal Spam Act of 2003, the Cybercrime Act and several others [16]. Legislation has always been several steps behind technological progress. Similar to email spam, it will probably be years from now that laws will be placed on unsolicited voice calls. However, legislation has not been effective in dealing with email spam. To add to this, IMS uses SIP for session establishment. SIP has no mechanisms that deals with SPIT [17]. IMS is still being developed, therefore, there is still time to act on this problem before SPIT becomes as severe as email spam.

Spammers will always be present to take advantage of and adapt to trends in communication technology. Therefore, it is important that IMS have structures in place to alleviate the problems of spam. Recent solutions proposed to block SPIT [18, 19, 20, 21, 22] have the following shortcomings: restricting the users to trusted senders, causing delays in voice call set-up, reducing the efficiency of the system by increasing burden on proxies which have to do some form of Bayesian or statistical filtering, and requiring dramatic changes in the protocols being used. The decoying system proposed in this dissertation, for the IMS, fits well with the existing protocol structure and customers are oblivious of its operation. Further, the decoying method causes no delays in voice call set-up.

It has been highlighted that the Internet grew rapidly as a result of its openness. However, malicious attacks and viruses also spread due to this growth and lack of

University of Cape Town

security. Likewise, email grew in parallel to the net but was severely affected by spam. VoIP is in its infancy, if a lesson has to be learnt from history then VoIP is likely to be misused with SPIT as it becomes more popular. On the other hand, IMS introduces a converged system, and just like growth of the Internet resulted in adoption of email, similarly growth of IMS will result in VoIP popularity. IMS also adopts the philosophy of openness, just like the net, for faster creation and deployment of new services. But, IMS has standardised strong authentication and authorisation mechanisms in place, giving it a head start in securing VoIP. A method to block SPIT on IMS is possible using decoys that solves the performance shortcomings of many other methods of spam filtering. Large ISPs have always had decoy email accounts to catch spammers, however this was not effective due to lack of authorisation and authentication for emails. In addition, spammers had many disposable email accounts. This is not possible for IMS where users are charged for services, hence must pay for creating new subscriber profiles. Consequently, a banned account on the IMS framework will result in loss of capital and time in order to acquire a new account. This makes a decoying scheme effective, simple, and easy to deploy on an IMS infrastructure.

The introduced decoying system is a modified form of honeypot architecture designed specifically for catching automated spammers. Honeypot systems have several advantages and are being favoured to perform network intrusion detection and log activities of malicious attackers. There are many types of honeypot systems being researched [**?** 23, 24] to detect malicious attacks. The honeypot method is simple, allowing for data collection on the types of attacks, and are resource efficient as compared to other security measures that are succumbed by large number of attacks or bandwidth. Central logging systems also suffer from being overwhelmed by large number of attacks. However, a distributed decoying system would not have this shortcoming and still incorporate all the advantages of a honeypot system.

In summary, email grew side by side with the net. The openness favoured by these systems led to large accounts of security incidents as their adoption increased. For email, number of spam messages grew rapidly. Similarly, VoIP is gaining popularity and adoption of IMS will favour VoIP greatly. If SPIT is be limited, action needs to be taken in the early stages. Incorporating recent proposed VoIP systems have severe performance drawbacks on an IMS architecture. Therefore,

University of Cape Town

a decoying system for SPIT blocking is proposed having all the advantages of a modified honeypot system.

1.2 Thesis Objectives

This thesis proposes a simplistic, robust, novel decoying scheme so as to block SPIT. The design issues analysed for this scheme include a way to deploy this system with little change to the IMS infrastructure or signalling. The changes needed on the IMS will be discussed in terms of their efficiency. A detailed look at how the decoying system will interact with IMS components will be outlined, and the security aspects of this proposed interface will be a major concern in this design proposal.

The IMS is a globally mobile system, and this fact incorporates a stringent criteria that must be handled by any incorporated spam blocking solution on such a system. Analysis of the suitability of recent solutions of VoIP SPIT blocking will be done on the mobility framework of the IMS. In addition, the decoying system proposed will also be evaluated under this mobile environment.

Decoying systems deployed on an IMS system should be able to fully utilise the standardised authentication and authorisation measures that are included on an IMS framework. The current VoIP spam blocking methods assume that there is no secure authentication and authorisation. A system designed acknowledging the IMS authentication and authorisation can be simplistic and have better performance benefits than previously suggested solutions to VoIP spam. The introduced decoying system design aims to fully apply these security measures present in the IMS.

This study performs an evaluation into the different methods of email blocking techniques, and their suitability for VoIP in an IMS environment. Also, discussion on the recent solutions to VoIP spam blocking techniques is conducted. The analysis focused on these existing methods in order to evaluate their shortcomings and devise a simplistic method that can reduce these factors.

Several quantitative performance factors are considered in deploying a spam blocking solution. Analysis of recent VoIP spam filtering techniques in terms of these

University of Cape Town

quantitative factors is considered. Further, an evaluation test bed is implemented as proof of concept of the proposed spam blocking method. Furthermore, performance analysis of the decoying method is conducted under different network conditions to prove the robustness of the design. Also, the decoying method's performance on this evaluation framework is compared with theoretical analysis of the other VoIP spam blocking methods.

1.3 Scope and Limitations

The IMS is a converged all IP network integrating different heterogeneous access networks that include WLANs, WiMAX, cellular networks and so on. The proposed decoying scheme is considered for an overall IMS core architectural framework and protocols. A detailed consideration of the use of this decoying system for the different access networks is beyond the scope of this research. However, a consideration to networks like WLANs where transmissions are not secure are taken into account. A modification of the proposed scheme is outlined in order to be effective in such non-secure environments.

The research does not delve deeply into the details of posting the addresses of decoys on websites. It is assumed that decoy addresses will be present on adequate number of sources where an automated harvester is most likely to collect these addresses. The details of posting such a decoy address where a person can tell that it is a decoy address will not be discussed in detail. But, several solutions or methods to do this will be illustrated in the design.

The IMS incorporates several different types of SIP signalling depending on how Quality of Service (QoS) is guaranteed. The study conducted did not analyse the proposed scheme working in all the signalling scenarios, but looked at the operation of the decoying system on a simplified, general IMS SIP signalling architecture. The different forms of signalling are bound to cause different performance factors on the network with regard to voice call set up and transmission. As a result, no evaluation of the introduced method of blocking SPIT in terms of the different SIP signalling is provided.

The evaluation framework implemented to test the proposed scheme is not fully IMS compliant. The clients used to send voice traffic traffic do not follow the

University of Cape Town

exact signalling protocol of the IMS. These clients do perform authentication and authorisation and transmit SIP based voice calls. In addition, several components of the IMS architecture were implemented on one host due to resource constraints. As such several IMS interfaces were omitted in the test bed implemented.

Several heterogeneous networks are interworked by the IMS architecture. A packet originating from an Ethernet network can end up in a wireless network through the IMS core. This heterogeneous nature is not taken into account in implementing the evaluation framework. The complete evaluation framework was done on a Ethernet LAN.

Analytical comparison of the introduced scheme is compared to several, recent proposed systems that tackle VoIP spam. However, a comparison by implementing existing systems on IMS is beyond the scope of the study. Also, most of these systems were not designed for the IMS architecture.

The evaluation framework included only one domain, with nodes only present on a home network. This small scale test bed is sufficient for the purposes of this study, which include proof of concept and performance tests. However, it should be highlighted that most adverse effects of spam occur during periods of peak traffic and implementing a large number of voice clients is not possible.

The IMS prevents spoofing of user identities with its strong authentication mechanisms. However, the evaluation framework assumes that no identity theft or spoofing occurs without providing such a strong security measure present in the IMS.

The IMS is introduced as a globally mobile system. Any proposed evaluation test bed should incorporate these mobility features. The implemented test bed does not take into account this mobility requirement, and so no performance evaluation of the decoying system's effectiveness in a mobile environment is done. However, a theoretical analysis based on this criteria is presented.

1.4 Thesis Outline

The remainder of the document is organised as follows:

University of Cape Town

Chapter 2 looks at an overview of the IMS. A working knowledge of this system is needed to base our design around the components present in the IMS. Mechanisms of the IMS to perform authentication and authorisation is introduced in this chapter. Next, an account of the various forms of spam, spam's profitability, and the solutions to spam blocking in context of email systems and VoIP systems is conducted. An outline of the differences in email spam and SPIT is discussed as well. Also, the difficulties in blocking real time spam for VoIP in comparison to email spam is researched. This chapter is meant to provide a foundation of the ideas presented in the next sections of this study.

Chapter 3 starts off by looking at the requirements of SPIT blocking systems for an IMS architecture. An introduction to the decoying system is done together with its implementation details on IMS. Changes in the protocols of the IMS that is necessary is explained. This section also looks at the different types and functionalities of honeypot systems, taking into account where they have been effective and where they have failed.

Chapter 4 deals with how an evaluation test bed is implemented for proof of concept of the proposed design as well as to determine the performance of the decoying system on an IMS architecture. A description of the implementation test bed and different configurations that can be tested on this framework is presented. Each component of the test bed is explained together with details on how they were designed and developed. The various software and hardware used is outlined, additionally the customised software written or any modifications done is explained.

Chapter 5 starts off with a theoretical analysis of the recent VoIP spam blocking methods as compared to the proposed decoying method. The suitability for IMS in terms of mobility and performance is presented. Additionally, several shortcomings of VoIP spam blocking systems are explained and expectations of the decoying system to overcome some of these shortcomings are outlined. Also, results obtained from the evaluation test bed are presented and analysed.

Chapter 6 presents a set of conclusions derived from the results and theoretical analysis done in the previous chapter. A summary of the concluding remarks on the various issues encountered in the previous chapters are illustrated. Further, this chapter gives some recommendations to improve the system and the evalua-

University of Cape Town

tion test bed. Areas of research relating to this discipline that will be of interest in the near future is outlined.

University of Cape Town

Chapter 2

Literature Review

University of Cape Town

2.1 Introduction

The previous chapter introduced the history of the Internet and email. This was brought to light to demonstrate the significance of security as adoption increased. In addition, email was illustrated to be severely affected by spam. Identically, VoIP technology is a new technology gaining popularity that can also be affected by this issue of spam. Further, IMS was introduced in the previous chapter as a proponent that will increase VoIP popularity.

IMS is an all IP framework for network convergence. This proposed convergence solution will merge data and voice networks. In order to gain an understanding of the workings of the IMS, the mechanisms and protocols employed by this IMS is discussed in this chapter. Moreover, additions to any system cannot be done without first evaluating the mechanisms that are already present. This research focuses on blocking SPIT in the IMS architecture, therefore this IMS architecture is introduced, and its working is used as a foundation for ideas and analysis that will be proposed in later chapters.

Email spam problem has been present for decades and lots of research has been performed to classify and understand spam in emails. Furthermore, several email spam filtering techniques have been proposed and implemented. This chapter will also provide a formal discourse on these issues presented. Moreover, voice spam and email spam have different characteristics, these characteristics will be

presented together with explanations to the challenges faced in blocking SPIT. This will allow appreciation of different SPIT blocking methods that are under research. Related work on SPIT blocking techniques under research will also be presented.

2.2 IMS

The idea of allowing network standardisation to include fast service creation and rich service features was started by 3GPP release 99 of the UMTS specification that incorporated the Open Services Architecture (OSA). The inclusion of an all IP network together with convergence appeared only in 3GPP release 4. The IMS, however, was formally introduced in 3GPP release 5, and release 6 made further improvements to security and integrated the WLAN access domain. 3GPP release 7 is currently under revision, but stage 2 of this release is available [14].

In subsequent releases following release 5, IMS is seen as an essential element to the IP core network. It can be questioned why IMS is so important and what benefits can it bring. IMS is mainly based on SIP [12] and DIAMETER [25] but includes several other protocols. These protocols are combined to enable rich multimedia services including Push to Talk (PTT), presence, conferencing, messaging, and so on. These vast services are seen as a benefit to the users. Also, the service providers can increase their revenue by providing more and better services. Integration of voice and data has cost benefits of maintaining one network for both services rather than two separate networks.

The IMS design requirements include several criteria as discussed in appendix A.1, however a requirement for SPIT prevention is not provided. The other requirements of security and privacy can be utilised in spam blocking algorithms and so requires further discussion.

This study aims to include additions to the IMS framework so as to block SPIT senders. These additions incorporated should take into account all the various IMS requirements such that all these requirements can still be fulfilled by IMS after being modified with the proposed SPIT blocking system. Further, none of these requirements should be limited by an efficient SPIT blocking method.

University of Cape Town

The IMS being a layered architecture ensures that any additions or modifications in the signalling layer or services layer can be independent of the access layer. Hence, consideration of the several access networks will not be significant in this study. Moreover, implementing most SPIT blocking algorithms on the services layer ensures easier incorporation to the IMS. The proposed SPIT blocking algorithm done in this dissertation must ensure that it does not affect service capabilities especially the performance requirements for real time voice communication.

The thesis objectives stated that minimum modification and utilisation of IMS procedures and components is to be done in designing the decoying system. The IMS includes several entities such as the Proxy-Call Session Control Function (P-CSCF) which is the first point of contact into the IMS. The Interrogating-Call Session Control Function (I-CSCF) is used for routing and topology hiding. The Serving-Call Session Control Function (S-CSCF) performs service authorisation and the Home Subscriber Server (HSS) is database containing user service profiles. An understanding of the functions of the different IMS components is necessary because the decoying system is a distributive solution with several components of the IMS carrying out different functions of the proposed system. For more details on the IMS components the reader should refer to appendix A.2.

The SPIT blocking solution requires the use of the interfaces present in the IMS to transfer information from the decoy to other entities in the IMS. It is economical to reuse the interfaces already present. Further, if any additional interfaces are required then these additional interfaces can utilise the same protocol and methods of the existing interfaces. This will allow a easier adoption of the introduced decoying system. Appendix A.3 presents the main interfaces in the IMS framework and a detailed discussion of the interfaces used in the design will be presented in the next chapter.

There are several proposals on filtering VoIP spam and most of these require modifications to voice call session establishment. In order to be able to analyse these VoIP solutions for the IMS, this study will present the IMS session establishment procedures and give an analysis on its performance efficiency.

The proposed decoying system aims to utilise the authentication, authorisation, and security measures present in the IMS. These security measures will be dis-

University of Cape Town

cussed in terms of their operation and effectiveness. Further, the decoying system will rely on the enforcement of subscription profiles, hence the operation of the IMS on enforcing subscription data is outlined and discussed in this section.

2.2.1 Subscription Information

The decoying system that is proposed in this dissertation relies on retrieving user identities from SIP messages received. This retrieved identity is then used to modify the service profile of the user. For this reason, there is significance in presenting the user identities present in the IMS, how service profiles are mapped to these identities, the properties of the service profiles, and how service profiles are enforced. Further, the scheme proposed aims to modify the service profiles with as little change to the IMS methods as possible, hence IMS methods regarding identities and service profiles are introduced.

There are two main IMS user identities, private and public user identities. Both these identities are stored on the IMS Identity Module (ISIM) and cannot be changed by the user. For more information on IMS user identities, the reader should refer to appendix A.4.

IMS Service Profiles

A user can have many public user identities that are linked to one private user identity. In turn, different public user identities can be linked to different service profiles in the HSS.

During registration, service profiles are downloaded by the S-CSCF from the HSS by using the private user identity. It is worth mentioning that service profiles can be queried using the public user identity as well. This is done by ASs in order to receive notification on service profile changes from the HSS.

Service profiles contain public user identities, core network service authorisation, and initial filter criteria. The public user identities in the IMS include a barring indicator, which if set prevents this identity from initiating IMS services. Banning accounts using this barring field is too harsh for our proposed system, which aims to only prevent further voice calls.

University of Cape Town

The core network service authorisation performs media policy authorisation and can be used to check if a user is allowed to make voice calls, video calls, etc. The HSS stores integer values corresponding to the media profile which is transferred to the S-CSCF that must map these integers back to the media profiles. This operation is illustrated in figure 2.1. For the case shown in the figure 2.1 removing the integer "4" from the network service authorisation would prevent the user from making further voice calls.

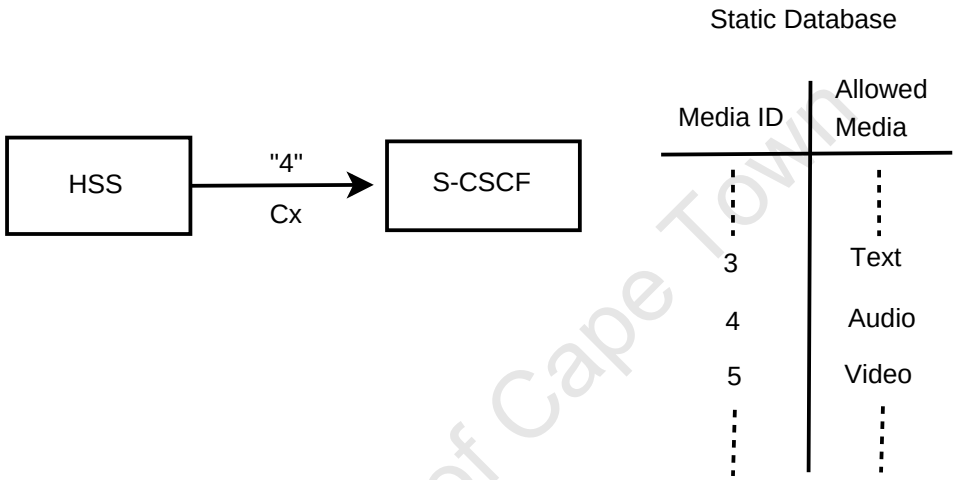


Figure 2.1: Media policy operation with service profiles.

The initial filter criteria causes service triggering, and subsequently the SIP messages are routed to the specified AS. Removing the filter criteria for voice applications can also prevent the user from accessing voice services requiring ASs.

2.2.2 Security Procedures

Any system that relies on banning user accounts should first evaluate the measures that are in place preventing users from providing fake identities. The authentication system for the IMS is presented together with a discussion on its effectiveness. This part on security procedures is performed with the purpose of proving that identity spoofing and theft are very difficult in an IMS architecture.

IMS access security [26] is based on UMTS Authentication and Key Agreement Protocol (AKA) [27]. The ISIM stores the secret key (K) and AKA algorithms. Access to the ISIM is limited, the ISIM takes AKA parameters as input and gives

University of Cape Town

out generated AKA parameters. Therefore, the secret key (K) is never exposed. Furthermore, the ISIM prevents physical access, and the user requires a PIN code to activate the ISIM.

Identity spoofing and theft are difficult since malicious users require both the ISIM and the PIN [28]. The AKA authentication requires the S-CSCF to send an authentication request with a random challenge (RAND) and a network authentication token (AUTN) during registration. The ISIM verifies the network by checking the AUTN and responds with an authentication response (RES) calculated using K and the RAND. The S-CSCF verifies the RES to authenticate the user. Also, this authentication procedure creates session keys - cipher key (CK) and integrity key (IK) - that are used for securing connection between the User Equipment (UE) and P-CSCF.

The IMS security mechanism is independent of the access security and does not consider if an access network has done any authentication or not. This can reduce efficiency in that in cases where both the IMS and the access network perform security associations. On the other hand, this IMS security methodology based on the ISIM is hard to apply to broadband networks [29]. In IMS release 6, interworking with WLAN was adopted, although authentication of user is done by IMS methods, subsequent integrity and encryption has to be performed by WLAN security mechanisms [29]. This can cause a problem if WLAN security is weak, and this problem will be discussed further in the next chapter.

The IMS security procedures ensure that identity theft is very difficult. Further, the IMS security methods are derived from GSM cellular networks using SIM cards. It has been shown that physical access to stolen SIM cards in order to spoof identities requires about 150 thousand queries and may take up to 8 hours [30].

University of Cape Town

2.2.3 Delays in Session Initiation

The purpose of discussing the delays in SIP signalling for IMS is to allow analysis of the research that proposes modification or additions to the SIP session establishment to carry out SPIT filtering. This part of the thesis presents a summary of the procedures required in IMS session initiation. Subsequently, the time re-

quired from session initiation to when media can be transferred over the session is discussed.

A session initiation involves several processes: routing of first INVITE to the recipient, media authorisation, media negotiation, and resource reservation. Routing uses the domain name system (DNS) [31] to locate the P-CSCFs, S-CSCFs, and the I-CSCFs. The S-CSCF, according to the service profile of the user, authorises the user in using the asked media for communication. Media negotiation involves the two UEs negotiating the type of media and set of codecs. Accordingly, both the UEs must ensure resource reservation before media transfer can occur. However, resource reservation may take time or even fail.

The delays associated with a SIP session establishment for the IMS include delays due to processing of messages, delays due to database look up, delays caused by DNS, and delays in ensuring resource reservation [32]. Processing delays involving message parsing and header processing occurs in the proxies and is considered to be low. In contrast, the delays caused by DNS can be large in the case of national calls and even larger considering international calls [32]. Resource reservation can be cumbersome and introduce a significant amount of delay to call set up. However, the database look up delays are considered of lower magnitude to both the DNS and resource reservation delays, but further studies need to be done to prove this [32].

The impact of delays caused by DNS and resource reservation can increase call set up time. These delays will be particularly noticeable in making international calls. It is seen that session establishment in the IMS involves several time consuming processes, addition of a process to filter SPIT in the session establishment mechanism would further aggravate this situation.

2.2.4 Discussion on IMS

The IMS framework has no insecure proxies that can be used by spammers to fool their identity. Further, the authentication system using ISIM is difficult to compromise. This fact ensures that where a decoying system failed for email, it will be more effective in the IMS architecture. IMS components and interfaces is discussed since the decoying system aims to make as few modifications to the

University of Cape Town

IMS architecture as possible and utilise the present functions. Also, if account deactivation is done for voice calls, an identity to refer to the account is needed. Therefore, this part of the thesis on IMS discusses the several IMS identities. In addition, the mechanism that enforces these service profiles were presented so that the reader can understand how the system will behave once a user service profile has been modified.

2.3 Spam

In the previous chapter, it was highlighted that more than 65% of all emails were spam [7], and a forecast by Gartner states that by 2010, 5% of all spam will be SPIT [13]. Email spam is bad economically for the Internet Service Providers that have to provide spam filtering solutions. Moreover, email spam causes waste of bandwidth and congestion for email servers. However, installing these spam filtering solutions leads to legitimate messages being discarded. Additionally, businesses lose money because employees have to sift out the legitimate messages from the spam.

Section 2.3.1 of the thesis looks at the solutions to the email spam problem that is available today. VoIP spam is still new, and solutions to filter SPIT can take a few lessons from email spam filtering techniques. Section 2.3.2 will discuss the effectiveness on legislation to reduce email spam and whether same types of legislation can be effective for VoIP spam. The next section compares email spam properties and SPIT properties. Moreover, a discussion on which email spam can be used for filtering SPIT is presented. Email spam is profitable, and there are several factors why it is so prevalent. The next part of the thesis discusses if these same factors will play a part in making SPIT popular in the future for the IMS. Subsequently, section 2.3.5 analyses the various SPIT filtering methods that have been proposed.

2.3.1 Email Spam Filtering Methods

There are several personal email spam filters and ISP based spam filters. These filters are prone to false positives (discarding legitimate messages as spam) and false

University of Cape Town

negatives (classifying spam as legitimate messages). These email spam filtering techniques are presented as follows:

Source Based Filtering

Source based filtering involves blacklisting sender's email address or sender's IP [33]. Blacklists are lists containing email addresses that are known for sending spam. A message from a user on these lists will be rejected. Nevertheless, blacklists have not been very effective because many legitimate users have been added to blacklists, spammers usually have many disposable addresses or may use another person's email account, and blacklist programs such as SpamCop are fooled by forwarded messages.

Blacklisting IPs have not been effective as well since spammers exploit open relays to circumvent this system. Because spammers change their IPs regularly, this method is only effective for a short period of time.

Whitelists

A user may keep a database containing a list of senders from whom emails are to be accepted. This method is too restrictive and does not allow the user to receive legitimate messages from new senders. Whitelists can also be employed by ISPs [34]. Messages from users on this list are allowed to pass through the ISP's servers. However, maintaining these lists by the ISPs have been a cumbersome task with more than a thousand users requesting to be added each day.

Greylists

This technique is based on the principle that automated spammers rarely resend emails. Greylisting involves maintaining a whitelist of allowed senders and a blacklist of blocked senders. This method defers delivery of messages containing sender IP, sender address, and recipient address that has not been previously seen together. However, this scheme can considerably delay legitimate messages and causes overheads on the recipients system. A proposed implementation of greylisting [35] checks the sender IP and email address obtained from the SMTP

University of Cape Town

greeting and that from the email message, if there are any irregularities then the message is rejected. The spammer receives notification that the email was blocked and additional information can be obtained from a specified URL. The downside is that this scheme cannot guarantee timely delivery of emails and can produce false positives.

Challenge-Response Methods

In this method, the ISPs keep a record of permitted users; and an email from a new user is stored and delivered when a challenge email sent by the ISP is answered by the sender. This challenge-response method stops all emails from automated senders and from senders using fake email addresses. However, this method causes deadlock when both the receiving and sending system uses this method. Additionally, challenge-response mechanisms fails for legitimate automated messages and emails sent from mailing lists.

Filtering Emails based on their Content

Word filters are one type of content filtering methodologies that identify key words in emails that are normally present in spam. The databases that contain these words need to be updated regularly if this method is to be effective. Also, spammers can fool these systems by misspelling words, and these systems suffer from a large number of false positives. For example, a physician can include the word "Viagra" in a legitimate email, but a word filter sees "Viagra" and classifies the message as spam.

Rule based filters are a learning algorithm system that assigns a rank to key words in emails. If the sum of these ranks exceed a set threshold the message is classified as spam. Rule based filters must be trained using a set of legitimate and spam messages. SpamAssasin is a popular rule based system. However, just like word filters rule based systems must be updated constantly to be effective.

Another content filtering approach uses Bayesian filters. This method uses a statistical scheme and must be trained just like rule based systems. The probability that a message containing word M is spam S is equal to the probability that the word M appeared in the training spam messages, multiplied by the probability of

University of Cape Town

spam messages, and divided by the probability of the word M in all the training messages ($P(S|M) = \frac{P(M|S)*P(S)}{P(M)}$). According to this equation, Bayesian filters are learning algorithms with their effectiveness increasing as the length of time they are used increases. As a result, Bayesian spam filters are one of the most effective filtering tools with a high spam recognition rate and low false positives [36, 37].

2.3.2 Spam Legislation

CAN-SPAM Act [15] does not prohibit spam but rather contains regulations for senders. Under this act, senders can send email messages with marketing information as long as opt out mechanisms are present. Analysis of the CAN-SPAM Act shows that it was established mainly to set rules for sales people who send marketing, bulk emails and not to prohibit spam [38]. Furthermore, this act allows spammers to send emails legally as long as they adhere to the rules set. If such legislation is set for SPIT, then the effectiveness will be limited.

The main reason why legislation has not been effective for emails because emails traverse national borders, so a global spam legislation is thus needed. Further, spammers are able to adjust in order to circumvent the act. Spammers can use legitimate addresses to send email and prevent messages from being tracked to the source by using open proxies. Lawsuits and investigations against spammers can take several years [39]. However, legislation is only part of the solution for email spam and needs to be coupled with effective spam filtering techniques. The same scenario will apply to voice spam, but it will probably be several years before laws prohibiting SPIT are enacted.

2.3.3 Comparison of Email Spam and SPIT

Voice spam is difficult to classify using content filtering methods as speech recognition software cannot recognise words very well. Also, voice spam can be sent in several languages. This language problem occurs in email as well. Moreover, email messages are stored in servers and spam filtering methods can be applied, however this same store and check principle cannot be applied to voice calls. Voice calls are not classified as a best effort service like emails and any SPIT blocking

University of Cape Town

solution implemented needs to consider the performance effects in terms of call set up and latency. In addition, voice spam is a larger nuisance than email spam, since the user has to take voice calls immediately as compared to spam emails that reside in inboxes until the user is ready to read them.

The mentioned email spam filtering techniques except for content filtering are applicable for filtering voice spam, however, it should be noted that the downsides of these methods will also be present in filtering voice spam. Content filtering is not applicable for SPIT filtering because voice calls are real time and currently available voice recognition software cannot recognise words very well. Bayes and rule based filtering are very effective for filtering email spam but cannot be used for voice spam, hence new methods are being researched; these are discussed in section 2.3.5.

University of Cape Town

2.3.4 Profitability of SPIT in the IMS

Spam is prevalent due to two factors time and cost. Spammers waste insignificant amount of time to send millions of email messages to different recipients. This is achieved by using automated web crawlers to harvest email addresses from websites, and then programs installed on hosts can be set up to send bulk emails. The various tools available are presented and analysed by Cournane and Hunt [40]. Similarly, IMS SIP URIs can be parsed from websites using web crawlers. The format of the SIP URI is similar to email addresses. The tools for harvesting SIP URIs are already present, and further pre-recorded voice messages can easily be sent from computers. Therefore, many unsolicited voice calls can be automatically sent within a short period of time in the IMS. However, email spammers have exploited open relays to hide their identities, this will not be possible in the IMS which has strict security procedures as explained in section 2.2.2.

To send an email, one needs an Internet connection. The connection to the Internet is normally charged at a flat rate, so sending one email costs the same as sending a thousand emails. The IMS has not been fully deployed yet, so one can only predict the type of charging for voice in the IMS. The IMS architecture incorporates a flexible charging mechanism that allows the service provider to choose the type of charging for their services. To predict how voice will be charged in the IMS, this study presents how VoIP is charged by the major providers. Table

2.1 shows the charging schemes employed by several VoIP service providers. With the exception of Vodafone, the charging method is either flat rate or free. If these service providers move to the IMS, then the charging schemes are not likely to change. Hence, the factor of cost will also be present in the IMS, and so SPIT will be profitable in the IMS.

Table 2.1: Charging methods used by VoIP service providers [41].

Service provider	Location	Charging scheme
At&T	U.S.	$29.99 unlimited within the U.S.
Broad Voice	U.S.	$24.95/month for unlimited calls to 31 countries.
Cable Vision	U.S.	$34.95 for unlimited calls within the U.S.
Free	France	Free VoIP calls within France.
Vodafone	Germany	20 euros per month for 1000 minutes.
KPN	Netherlands	Free.
Wanadoo	U.K.	4 pounds per month.

University of Cape Town

2.3.5 Related Work on Blocking SPIT

The proposed decoying system aims to reduce SPIT in the IMS, therefore this section discusses the related work done to filter voice spam.

Historical Call Pattern Analysis

Progressive Multi Gray-Levelling (PMG) is a SPIT filter based on historical call pattern analysis that has been proposed by Shin and Shim [18]. This method calculates a short term grey level and a long term grey level of a user based on the user's historical call pattern passing through a VoIP proxy. A threshold is set, and if the sum of the short and long term grey levels exceed this level the user is classified as a spammer and all outgoing voice calls are blocked for a specified time. This method is based on the behaviour of a spammer who generates a large number of calls in a short period of time.

The short term grey level is calculated for short periods so rises and falls quickly. If the caller stops making voice calls for a short period of time, this level reverts

back to zero allowing the user to initiate voice calls. This can be exploited by automated spammers very easily by having on and off periods. However, to reduce this short coming a long term grey level is included that rises and falls slowly. This level rises faster for a user that has been previously classified as a spammer than a normal user. However, even with this feature the spammer is not blocked completely. Further, this method requires the proxy to keep a database for every user counting the calls made within a time frame. This introduces extra overhead to the call set up process which for the IMS is already quite cumbersome as shown in section 2.2.3. PMG is a method suited to non-mobile terminals. In the IMS, UEs can change proxies hence the historical data for a spammer will not be present on this new proxy server and the method fails.

Reputation Systems

A reputation concept can be used to build trust and ban spammers. In this method, users rate each other using a pre-defined criteria, and this rating is stored in the contact list containing allowed senders. All the contact lists are combined to form a large social network in a reputation manager [20]. The reputation manager calculates the reputation, if the reputation exceeds a certain threshold then the message is rejected. The IMS is a global system, it will be impossible to merge all contact lists to one reputation manager. Further, a reputation manager presents a central point of failure under high loads. The overheads concerning calculating the reputation using complex equations will be high and cause delays to voice call set up.

Challenge-Response Methods

Madhosingh [19] proposes that users of VoIP classify users in whitelists, blacklists and greylists - users not in the whitelists or blacklists. Users in the greylist are required to pass a human verification Turing test before the call is forwarded to the recipient. This method has been adapted for the IMS, incorporating a SPIT AS to perform the Turing test [22]. This is an effective method capable of completely dealing with automated voice spammers. However, IMS is still in its infancy and requires a SPIT protection system that will not overload the proxy servers during

University of Cape Town

peak periods. Also, such methods can reduce the openness of the IMS and limit users to only a few regular contacts. This system although effective can also cause annoyance to the users.

Multi-Stage Filters

Multi-stage filters are a combination of reputation systems and historical call pattern analysis methods. Therefore, the shortcomings of both these methods are present in multi-stage filters. This method implements a learning algorithm with a feedback loop to adapt from previous situations as illustrated in figure 2.2. Dantu and Kolan [21] introduced this system and included user feedback and presence. The presence adapts the system to user mood such as available, do not disturb, and so on [21]. The multi-stage filter is implemented in the proxies. This method is computationally intensive and causes overheads to the call set up process.

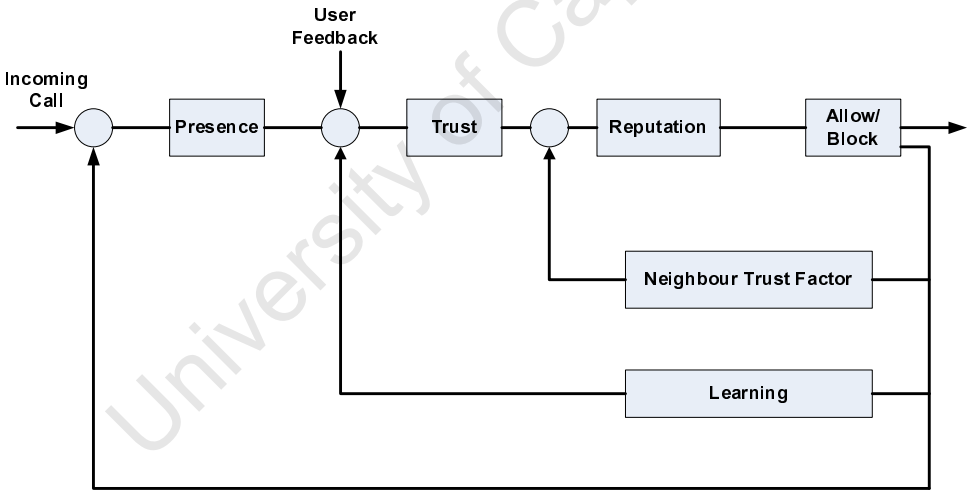


Figure 2.2: Operation of a multi-stage filter.

2.4 Chapter Discussion

The last part of this chapter on spam explained the prevalence and problem of spam for email, also expressing the importance to act on the problem of SPIT before SPIT becomes as prevalent as email spam. This part also introduced spam

University of Cape Town

filters for both emails and SPIT, and discussed the effect of legislation on spam. A case for the profitability of SPIT in the IMS was presented. The first section on IMS introduced the requirements of the IMS that must not be disturbed by adding a SPIT blocking solution. Moreover, the functions of IMS components and interfaces were discussed since a distributed algorithm needs to have knowledge of these functions. The decoying system utilises IMS authentication and service enforcement, hence these mechanisms of the IMS were discussed. This chapter presented the important parts of IMS for the decoying system together with motivating a requirement for SPIT blocking in the IMS and looking at previously proposed solution for email and voice spam. The shortcomings of the proposed solutions for spam was discussed in order to highlight in later chapters how the decoying system will reduce or overcome some of these shortcomings. The next chapter will introduce the proposed decoying system in detail.

University of Cape Town

Chapter 3

Proposed Decoying Solution for SPIT

University of Cape Town

3.1 Introduction

The previous chapter introduced the IMS protocols and mechanisms relevant to the study. Furthermore, related work on spam filtering techniques for both email and VoIP were presented. Motivation to the profitability of SPIT in the IMS was highlighted in the previous chapter, and so there is a need for an effective SPIT blocking solution for the IMS. This chapter will present in detail the proposed decoying solution to block SPIT.

3.2 Design Requirements

Before designing a system, the functional requirements should be well understood and documented. In consideration of this, and that the IMS is a standard for network convergence with various requirements that it meets, the SPIT solution should aim to disrupt these mechanisms present in the IMS as little as possible. Furthermore, the requirements highlight what functionalities are needed. This SPIT problem involves automated programs that can be executed on hosts to collect SIP URIs and send unsolicited voice calls to the addresses collected. The

aim of the solution is to block these users and ban their accounts, thus preventing them from making any further voice calls using the same account. Further requirements and functionalities of the proposed decoying scheme is presented as follows:

- The IMS is an architecture that allows mobile nodes to roam freely from one access network to another. So different access networks can allocate different addresses to the same user. The proposed SPIT blocking solution should be able to deal with spammers that move obtaining different addresses in different access networks. Moreover, IMS allows personal mobility whereby a user can access the subscribed IMS services from different terminals. Hence, the proposed SPIT blocking solution should be able to block a spammer even if the spammer changes terminals or access networks.

- The convergence of data and voice on a single core network increases the amount of processing and the number of packets received by the IMS core entities. The volumes of traffic would be particularly high during peak periods. A proposal for SPIT prevention will undoubtedly cause overheads in the IMS entities. However, a simple algorithm would require less processing on the core entities.

- There are various interfaces that are already defined within the IMS specification. Further, several network operators are in the process of migrating to the IMS. Extreme changes to the IMS introduced after this deployment will not be eagerly met by these operators. In light of this view, the proposed SPIT blocking solution will add components to the system but aim to modify or change the IMS interfaces as little as possible. Furthermore, the SPIT solution should incorporate the existing interfaces and mechanisms present. Easier deployment or adoption can thus be justified if this requirement can be met, also the cost of implementing the SPIT solution will be lower. An economical solution will be a greater benefit and be more likely to be implemented by many IMS network operators.

- The IMS has security mechanisms preventing unauthorised access and identity spoofing. Also, an authentication mechanism involving ISIM is present. In view of this, the proposed spam blocking algorithm should not create any

University of Cape Town

security hazards in the secure IMS network. Additionally, if communication between IMS entities are required then this should be as secure as possible.

- In periods of high traffic, the core entities of the IMS, the CSCFs, are performing a large number of packet processing. Any SPIT blocking solution that is to be effective under high loads needs to consider spreading the processing away from these entities as much as possible. Centralised processing scheme to block SPIT not only causes performance bottlenecks but can increase the likelihood of single points of failure. A distributed system is more effective for high traffic systems and will have a lower probability of failure. In addition, if processing is minimised in the core then there will be less packets dropped and less calls rejected during peak hours.

- To set up a voice session in an IMS domain, requires several signalling messages to locate the recipient and grant QoS resources. Therefore, introducing further signalling during call set up for the sake of SPIT prevention will adversely affect the performance of the system and cause even greater delays in call set up. The SPIT prevention technique should aim to leave the already cumbersome signalling as it is and not introduce any modifications for call set up.

- Some VoIP and email spam filtering techniques require user input and fine tuning. Most of these systems, however, are only as effective as the parameters input by the users. This causes problems since users may not be fully aware of the optimum settings of the system. In consideration of this, the proposed spam blocking for the IMS aims to be independent from user input. Furthermore, the users should be oblivious of the operation of the SPIT filtering method.

- The SPIT blocking solution must be independent of the access networks such that a generic solution can be placed in the many different access networks of the IMS. This allows the design of the SPIT blocking solution to work without dealing with specifics of the underlying access networks.

In summary, the main criteria for the design dwells on a system that will cause the least amount of overhead as well as require as little modification to the IMS

University of Cape Town

protocols as possible. In keeping with this, this study proposes, in the next section, a solution to block SPIT that accounts for all these criteria mentioned.

3.3 Decoying to Block SPIT

This section will give a brief overview of the proposed design. Detailed procedures in the decoying system are highlighted in the later parts of this chapter. The previous chapter looked at the various email and VoIP solutions that have been proposed. However, analysis of these solutions reveal weaknesses in performance under high load. Further, most, if not all, assume a non-secure environment with no authentication procedures present. The decoying solution described briefly is a SPIT blocking mechanism that will take advantage of the IMS authentication measures, and be simple enough to cause few performance overheads.

Firstly, a quick look at how spammers will operate in the IMS domain is necessary. The automated spammers comprising of a web crawler and bulk IMS voice call generator will be run on an IMS terminal. This spammer terminal will collect IMS SIP URIs from web pages, forums, Usenet news groups, mailing lists, chat rooms and so on. Subsequently, these automated programs will send pre-recorded voice calls to all the SIP addresses retrieved. Spammers of email preferred collecting addresses from websites over any other sources. This is proved in a study conducted in 2003 that show that 97% of spam were sent to addresses that were posted on web sites, and 2% of spam were sent to addresses from news groups [42]. In following this trend, SPIT senders are more likely to collect addresses from public websites.

Decoy addresses will be posted on the sources used by the automated spammers to collect the addresses, with special emphasis on posting these addresses on public websites. No human user should ever use these decoy addresses and thus no legitimate call to the decoy UEs should be made. These decoy addresses can be posted so that humans can tell that they are decoy addresses, but automated harvesters cannot. This can be done by putting the decoy addresses at odd places such as in the middle of content of the web page, next to pictures that indicate that this is a decoy address, and decoy addresses can be blended in with the background of the web page.

University of Cape Town

These decoy addresses correspond to actual Decoy UEs present in several IMS access networks. The functions of the decoy UEs can be implemented on the P-CSCF or the S-CSCF. However, one of the design requirements include creating as little overhead as possible on the core entities. Hence, the design implements the functions of the decoys on hosts present in the IMS access networks.

Upon receiving any voice call, the decoy UE will parse the SIP header to retrieve the address of the sender. Then, the decoy UE will send this address together with the decoy serial number to the sender's HSS. This HSS needs to store this entry, such that another entry from a different decoy for the same sender will lead to the sender's account being blocked. Next, if this sender tries to make a voice call, the S-CSCF will reject the call according to the service profile received from the HSS. If the offending user changes access networks or terminals but still uses the same service profile, then the call should still be blocked.

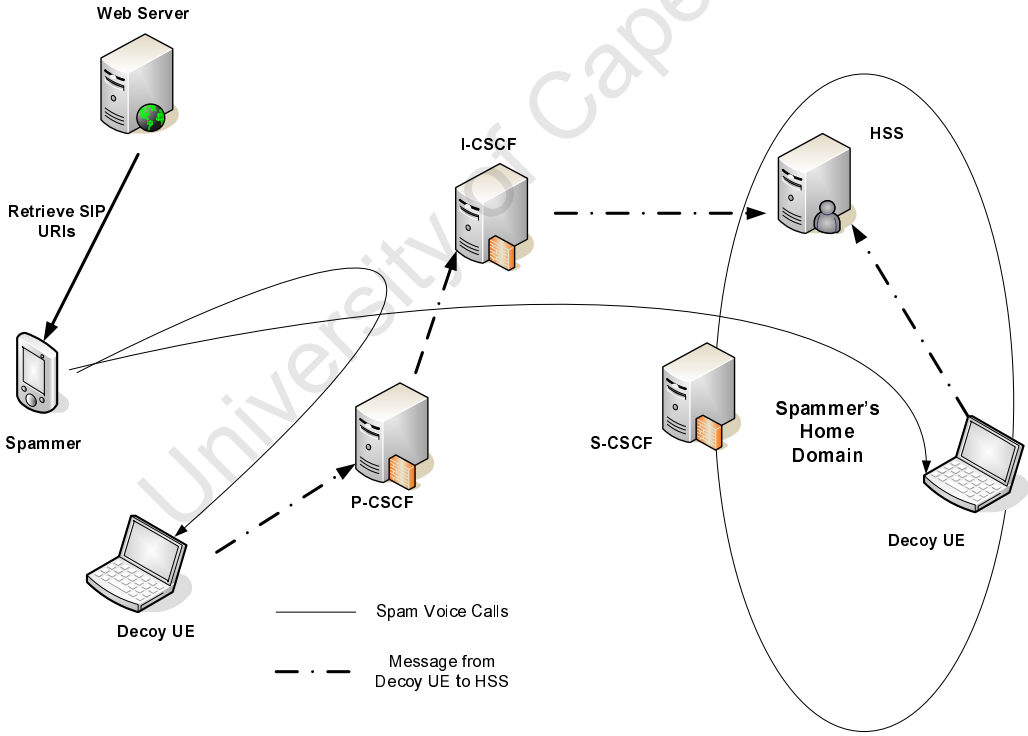


Figure 3.1: Operation of the proposed decoying system.

The message sent by the decoy UE to the HSS needs to traverse various IMS entities. This leads to two scenarios as shown in figure 4.6. If decoy is present in the spammer's home domain then the Decoy simply sends a message directly

to the HSS. However, if the Decoy is not present in the spammer's home domain, then the message must pass through the P-CSCF and the I-CSCF before reaching the HSS. This interface should be designed to be secure and cause little overhead to the system. Another way of transferring the message from the decoy UE to the HSS involves going via the sender's S-CSCF and not the I-CSCF. This is illustrated in figure 3.2. Between these two methods mentioned, this dissertation will analyse in section 3.4.2 which method is more efficient.

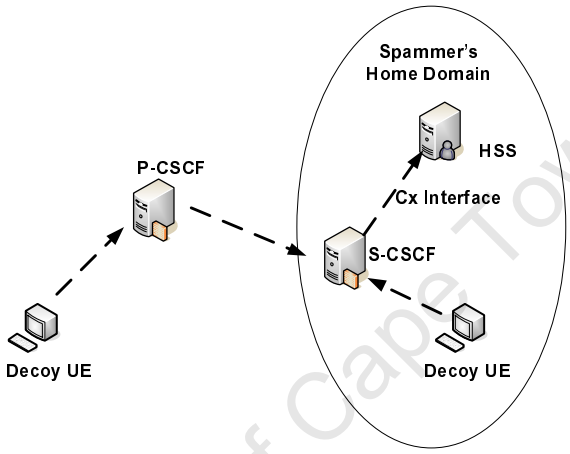


Figure 3.2: Blacklist messages sent via the S-CSCF.

The modification of this system to take account of false positives involves refreshing the decoy records on the HSS every single day. Therefore, for those users who have made one call to a decoy, their entry in the HSS's records is deleted at midnight everyday. This ensures a lower probability that a user will get banned for mistakenly phoning a decoy once. In the case of insecure wireless networks where addresses can be obtained by man in the middle snooping techniques, a modification to the proposed decoying system is presented in section 3.4.6.

University of Cape Town

3.3.1 Honeypot Architectures

This part of the dissertation will introduce honeypot systems. The proposed decoying scheme is a honeypot based system with the sole purpose of blocking SPIT. However, honeypot systems have been previously researched for other functions. This section discusses the uses of honeypots, the types of honeypots, and the limitations and advantages of honeypots.

A system composed of several honeypots is called a honeynet. Honeypots simulate an environment with the purpose of being compromised, thus allowing the network administrator to analyse an attacker's behaviour [43]. There are two types of honeypots: low interaction honeypots and high interaction honeypots [44]. Low interaction honeypots e.g. *honeyd*[1] emulates a service such as FTP and so the interaction of the attacker with such a system is limited. These systems can be detected when the attacker executes a command that the emulation does not support. On the other hand, high interaction honeypots involve deploying real operating systems that the attacker can interact with fully. However, high interaction honeypots can be compromised and be used as a launchpad for further attacks. But, high interaction honeypots allow collecting a larger amount of data about the behaviour of attackers than low interaction honeypots.

The advantages of honeypots include less time to analyse logs since only attacks towards the honeypots are recorded. On the other hand, honeypots only capture a subset of the activity i.e. those directed towards them, hence for honeypot systems to be effective, honeypots should be deployed in large numbers. However, honeypots are flexible systems and can be easily modified for new generation traffic such as IPv6 traffic.

Honeypots have been deployed for several purposes. The main use of honeypot systems is to collect data about hackers' activities in order to take action to protect the network against intrusions [45]. Honeypot schemes proposed for spam involve understanding how spammers operate. This honeypot method is used to collect data about new spam messages so as to improve spam filters [46]. The use of honeypot systems to blacklist users was proposed by Khattab et al [24]. They used roaming honeypots to locate malicious users performing Denial of Service (DoS) attacks.

Another development for honeypots systems introduced the concept of virtual honeypots. Several honeypot schemes employ this concept [46, 23]. Virtual honeypots can be simulated from one physical host, and therefore, one physical machine can be used to deploy several decoys as illustrated in figure 3.3.

[1]honeyd is a software to implement honeypots.

University of Cape Town

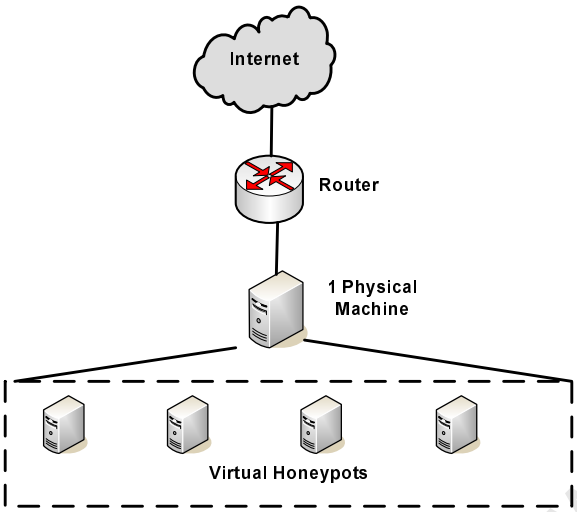


Figure 3.3: Implementing virtual honeypots.

University of Cape Town

Proposed Design as a Honeypot System

Honeypots are tools that have been used for analysing behaviour of malicious users. This thesis proposes a scheme for deploying decoy UEs in the IMS access networks, acting as modified honeypot systems. However, for spam prevention, honeypot systems have been used for analysing spam messages. In this case, the proposed scheme not only allows analysis of spam but also proactively informs the network to blacklist the sender, preventing further spam from the same source.

The different types of honeypot systems were introduced previously in section 3.3.1. The decoying system proposed only emulates a client for IMS voice services, hence it is a low interaction honeypot system with no chance of being used as a launchpad for further attacks. Moreover, several virtual decoys can be deployed using one physical host. This method saves capital and resources.

3.4 Detailed Operation of the Decoying System

The previous sections gave an overview of the proposed design and the requirements that need to be fulfilled. Also, the considerations made in various honeypot systems were analysed. This analysis resulted in modification of the initial design in some aspects. This section looks at the decoying system in detail. An outline

of how the decoying system fits into the IMS architecture is presented. The protocols and methods of the IMS that are utilised by the system is discussed and the modifications required will be proposed. The decoying system is separated into four functions.

The first function is invoked when the decoy UE receives a voice call and, the decoy examines the SIP header to retrieve the sender's address. The second function involves the Decoy UE sending the sender's URI and the decoy serial number to the sender's HSS. The third function is performed by the HSS. Upon receiving information from the decoy UE, the HSS modifies the profile of the sender and may subsequently prevent the sender from making voice calls in the future. The last function involves an algorithm implemented by the HSS to reduce false positives. A further discussion on the modification of the decoying system for insecure wireless networks is presented and analysed.

University of Cape Town

3.4.1 Retrieving URI of Sender

There are several URIs that are included in the SIP INVITE message. First thing to consider, will the decoying system retrieve the public or the private user identity. The private user identity is not included in the INVITE message and so cannot be retrieved by the decoy. Therefore, the public user identity is retrieved by the decoy UE and can be used to modify a user's service profile.

```
INVITE sip:joe@sip-router.com SIP/2.0
FROM: "friend" <sip:dick@siphone.com>; tag veli
TO: : "friend" <sip:joe@ser.com>
P-Preferred-Identity: <sip:dick@sipexpress.com>
Privacy: None
```

Figure 3.4: Structure of the SIP INVITE header before traversing the P-CSCF.

The identities included in the INVITE message from the sender is illustrated in figure 3.4. The inclusion of the optional P-Preferred-Identity header includes a registered public user identity. On receiving this INVITE message, the P-CSCF will insert a P-Asserted Identity header which includes a registered and authenticated public user identity. Further, the P-CSCF will remove the P-Preferred-Identity header.

Next, the P-CSCF will forward the INVITE message to the sender's S-CSCF. Using this P-Asserted-Identity header, the S-CSCF will check authentication and authorisation of service for the sender. Then the S-CSCF will route the SIP INVITE to the receiver's home network. Subsequently, the receiver's P-CSCF will check the Privacy header. If this Privacy header is set to "id" then the P-Asserted-Identity will be removed before forwarding the message to the receiver.

If the decoy UE is to retrieve the public user identity from the INVITE message then the P-Asserted-Identity has to be present. This leads to a complication in the case of the privacy field. A modification to the P-CSCF forwarding SIP messages to the decoy UEs is necessary. This modification will allow these P-CSCFs to ignore the Privacy header to all messages sent to the decoys. Therefore, the P-CSCFs require a static database of decoy UEs that they are serving. The algorithm implemented on the P-CSCFs together with the static database is illustrated in figure 3.5.

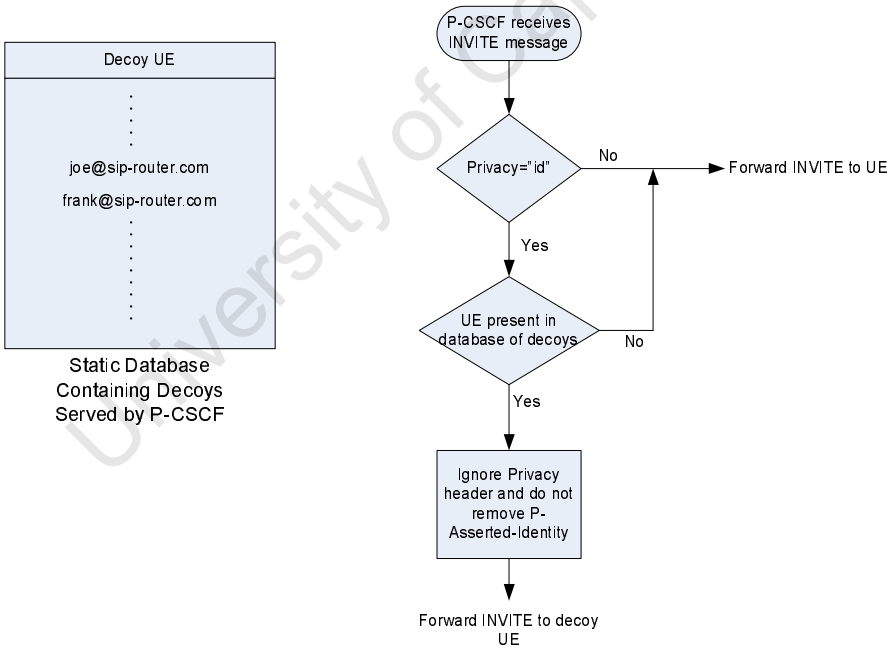


Figure 3.5: Modification of the P-CSCFs due to the Privacy header.

The decoy UE retrieves the P-Asserted-Identity from the INVITE message. This retrieval requires no decryption hence no heavy overhead will be incurred. Moreover, the software implemented in the decoy UE will parse the INVITE header

University of Cape Town

and separate the P-Asserted-Header.

3.4.2 Routing of Message from Decoy UE to Sender's HSS

This section will look at how the initial INVITE message is routed to the recipient to give an understanding of how the blacklist message can be routed to the sender's HSS. Also, a choice is made whether to go via the I-CSCF or the sender's S-CSCF for sending blacklist messages from the decoy UE to the sender's HSS. The advantages of both these methods will be outlined.

The address of the outgoing P-CSCF is obtained from PDP context activation or DHCP. The SIP INVITE is forwarded from the sender to the outgoing P-CSCF which forwards this message to the sender's S-CSCF. The address of this S-CSCF is obtained during registration and contained in the Service-Route header. The sender's S-CSCF then sends the host part of the recipient's address to the Domain Name Server (DNS). Consequently, the DNS sends back the address of the I-CSCFs corresponding to the receiver's home network.

The sender's S-CSCF chooses an I-CSCF and forwards the invite message. The I-CSCF queries the local HSS for the receiver's assigned S-CSCF and sends the message to this S-CSCF. The recipient's S-CSCF replaces the receiver's SIP URI with the address the receiver is currently registered with, and the message is sent to the incoming P-CSCF. This P-CSCF address was received in the Path header during registration of the receiver UE. The incoming P-CSCF will then send the INVITE message to the recipient's UE.

It is worth mentioning that whichever method of routing the blacklist messages is chosen, the delays due to DNS queries should be minimised. More information on DNS delays was presented in section 2.2.3. As shown in the routing of the initial INVITE message, all CSCFs insert their addresses on top of the Via header. Furthermore, the Record-Route header includes addresses of all CSCFs other than the I-CSCF because the I-CSCF is no longer required in the route. In consideration of both the Record-Route header and the Via header, both methods of sending the blacklist messages will involve no DNS queries.

The interface to the HSS from both the S-CSCF and the I-CSCF is based on the IMS Cx interface. Further information on IMS interfaces is discussed in section

University of Cape Town

2.2. The routing of the blacklist messages is chosen via the S-CSCF since this will involve modification of one Cx interface, that between the S-CSCF and the HSS. The final decision to route via the S-CSCF is shown in figure 3.2. Going via the I-CSCF requires an extra modification when the decoy is present in the spammer's home domain. This scenario requires a direct HSS to decoy UE interface. However, this interface can be avoided by going through the S-CSCF thus requiring less modifications to the IMS structure.

3.4.3 Interface between Decoy UE and HSS

The goal of the interface between a decoy UE and the spammer's HSS is to convey information that will successfully lead to preventing the spammer from making further voice calls using the same public user identity. It is significant to note that there may not be a one to one relationship between service profiles and public user identities. Hence, banning one public user identity from making calls may prevent other public user identities from making voice calls as well. In this scheme, this scenario is not an issue since the public user identities belong to the same private user identity and will affect the spammer and no other user.

In the IMS, IP security between different domains is provided by Network Domain Security (NDS)/IP [47] which uses a pre-shared secret parameter type of authentication and encryption between the IMS core elements. These core elements include the P-CSCF, S-CSCF, I-CSCF, AS, HSS, and SLF. Secure communication between these are handled by NDS/IP mechanisms.

The route of the blacklist message is from the decoy UE to the P-CSCF and then to HSS via the S-CSCF or straight from the decoy UE to the HSS via the S-CSCF, as shown in figure 3.2. There are no IMS security mechanisms present for the diameter communication from the decoy UE to the P-CSCF or from the decoy UE to the S-CSCF. Therefore, these CSCFs must keep a database of the private user identities and a shared secret key for each decoy that they are serving. This database is the same database used in overcoming the problem due to the Privacy headers as discussed in section 3.4.1.

The diameter interface between the CSCFs and the decoy UEs will be encrypted using TLS and IPSec.The information that the decoy UE is required to send the

University of Cape Town

spammer's HSS includes the decoy serial number and the spammer's public user identity. The blacklist messages require a command code that is not used in the Cx interface. Since command codes from 300 to 305 are already in use [48], the blacklist message with command name of Spam-Id will use command code of 306. The diameter message format of the Spam-Id command is illustrated by figure 3.6 and table 3.1 shows the mapping of the diameter Attribute Value Pair (AVP) parameters from the Cx parameters for this Spam-Id message. More details on these mappings can be found in 3GPP specification TS 29.228 [49].

```
<Spam-ID> ::= <Diameter Header>
        <Session-Id>
        {Vendor-Specific-Application-Id}
        {Auth-Session-State}
        {Origin-Host}
        {Origin-Realm}
        {Destination-Host}
        {Destination-Realm}
        {User-Name}
        [Supported-Features]
        {Public-Identity}
        {Integrity key}
        {Confidentiality key}
        [AVP]
        [Proxy-Info]
        [Route-Record]
```

Figure 3.6: Message structure of the Spam-Id command.

Table 3.1: Mapping of diameter AVP parameters from Cx parameters.

Cx parameter	AVP name
Public Identity (Spammer)	Public-Identity
Private Identity (Decoy)	User Name
Shared secret key for CSCF	Integrity-Key
Decoy Serial Number	Confidentiality-Key

The routing information required to send the blacklist messages can be obtained from the Record-Route header in the SIP INVITE message received from the spammer. Information from this header is used in the Destination-Host and Destination-Realm AVPs to forward the blacklist message to the spammer's S-CSCF. Subsequently, the S-CSCF will forward the Spam-Id to the HSS of the spammer. The Record-Route will include the P-CSCF address as the first hop

University of Cape Town

for the message from the decoy UE. The virtual decoy UEs will each have their own serial number and shared secret key for diameter interface with the P-CSCF. The P-CSCF will not be able to distinguish between a virtual decoy UE from a physical decoy UE.

The Spam-Id command is replied by the Spam-Id-Answer message, with command code of 307. Any errors or timeouts will cause the decoy UE to resend the Spam-Id command. However, if the HSS does not support blacklisting then a diameter error containing feature not supported will be returned according to IMS procedures. This will pass through the P-CSCF which will update its firewall rules to block any calls from the spammer's public user identity. This will at least ensure that the decoy UE domain is protected from the spammer. However, this does not create a global blacklisting of the spammer.

3.4.4 Modification of Service Profiles on the HSS

This research has dealt with the issues of retrieving the spammer's public user identity and delivering the blacklist message to the spammer's HSS. The information that the HSS needs from the blacklist message includes the public user identity of the spammer and the decoy serial number.

There are two ways that the spammer's account can be banned. For details on the structure and properties of service profiles refer to section 2.2.1. The first way includes setting the barring indicator for the spammer's public user identity. However, this method will prevent the spammer from accessing any of his/her IMS services and so is too restrictive. The second method involves modifying the core network service authorisation and/or the initial filter criteria.

This research employs the second solution that removes entries from the core network service authorisation responsible for granting audio rights. Furthermore, if voice services are deployed using ASs then initial filter criteria relating to voice services will also be removed. The banning of a user from making voice calls can have problems when considering emergency calls. However, in the IMS, emergency call numbers are embedded on the ISIM [50]. These emergency calls do not require a service profile check or authorisation. Hence, banning a user from making voice calls by removing audio rights will still allow emergency calls.

University of Cape Town

The structure of the core network service authorisation and initial filter criteria is not standardised and is vendor specific. Therefore, each vendor may have a different software to perform this modification on their HSS. For example, if integer "4" from the core network authorisation corresponds to audio media authorisation, then removing "4" from the core network authorisation will prevent the spammer from making further voice calls using the same public user identity. For more information on service profiles, the reader should refer to section 2.2.1.

The HSS will also need to incorporate databases to hold the information from decoys. This database can be separate or merged with the database of service profiles. However, a separate database is more efficient since look ups will be faster. This is because this database will be smaller than the database of all the users. The reason for this is based on the assumption that a subset of the users will be spammers.

University of Cape Town

3.4.5 Algorithm for Minimising False Positives

The last section dealt with the issue of modifying service profiles to ban users from making further voice calls. However, the issue that every spam prevention technique suffers from false positives was not discussed. In order to reduce false positives, service profiles are only modified if two or more different decoy UEs are hit by the same spammer, using the same public user identity. Further research on the optimum number of decoys that need to be hit before an account is banned needs to be done. For the purpose of this study, hitting two different decoys is assumed to be sufficient to ban a user.

The last section highlighted that a separate database is needed to keep account of the decoy messages. This design proposes two different databases to keep this information. One database will contain all public user identities that have already been banned, and the other will contain users that have hit only one decoy. The structure of these databases is illustrated in figure 3.7.

The database containing the users that have hit one decoy is refreshed every 24 hours to reduce false positives. The time of 24 hours is chosen arbitrarily, and further research on an optimum refresh period needs to be conducted. However, this is beyond the scope of this study. The overall algorithm for minimising false

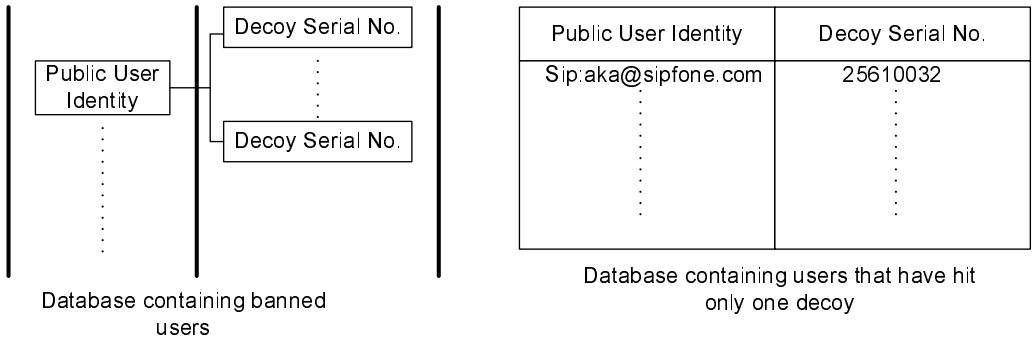


Figure 3.7: Two additional databases required in the HSS for the decoying system.

positives is shown in figure 3.8. Moreover, a permanent database of banned user profiles is required to follow up queries from banned users. This database will also contain all serial numbers of decoys that the banned user has hit.

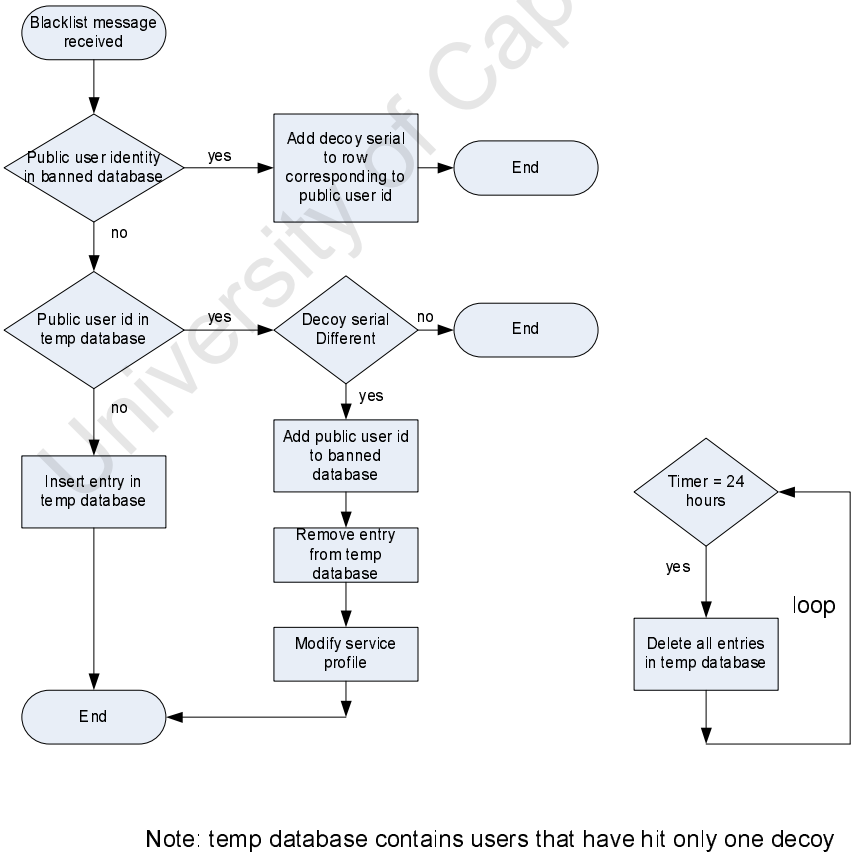


Figure 3.8: Algorithm for minimising false positives, implemented on the HSS.

University of Cape Town

3.4.6 Modification of System for Insecure Wireless Networks

In IMS release 6, WLANs were integrated into the IMS. A problem of security still persists for WLANs in the IMS domain. Although authentication of users employ IMS methods, the security association between UE and P-CSCF is maintained by mechanisms present in the WLAN standards [**?** 51]. This brings up a new scenario in the deployment of the proposed decoying system. Firstly, blacklist messages from decoy UE to P-CSCF may be intercepted by malicious users. And secondly, a new way to harvest SIP URIs by eavesdropping or intercepting SIP messages in the form of man-in-the-middle attacks needs to be catered for.

In order to ensure that the blacklist messages are not intercepted, the decoy UEs present in the WLAN networks will include a separate Ethernet connection to the P-CSCF. The sole purpose of this Ethernet link will be the secure communication of blacklist messages. This is illustrated in figure 3.9.

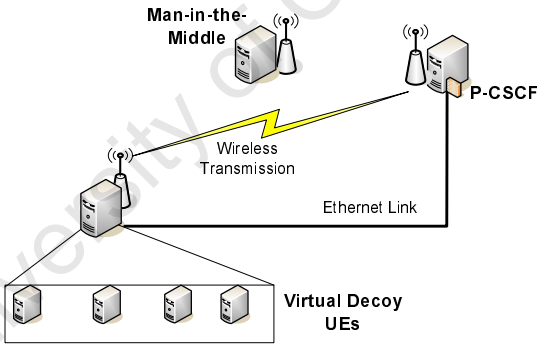


Figure 3.9: Operation of decoy UE in WLAN networks for the IMS.

The major aim of this thesis is to propose a decoying system to block SPIT and prove its effectiveness. However, a new issue whereby spammers can harvest messages by intercepting WLAN transmissions will not be dealt with in detail. Furthermore, an active decoy UE is proposed to deal with this scenario.

The decoying scheme proposes two kinds of decoy UEs, active decoy UEs and passive decoy UEs. Passive decoy UEs wait for voice calls but do not generate their own voice calls. On the other hand, active decoy UEs, only present in WLAN access networks, generate voice calls to other decoy UEs in their WLAN network.

University of Cape Town

Further study is required to propose an efficient scheduling and call rate for these active decoys. This issue will not be covered in this thesis. In this system, the decoy messages will be intercepted by spammers who will harvest SIP URIs of the decoys. As a result, these spammers will hit these decoys and so will be banned.

3.5 Operation of Spammers in an IMS Domain

This section gives an overview of the operation of the spammers. Subsequently, this behaviour will be adapted for sending SPIT over an IMS framework.

Most email spammers obtain their addresses from public websites. A study done by the Center for Democracy and Technology illustrates that 97% of spam were sent to addresses obtained from public websites. Furthermore, 2% of email spam sent were to addresses obtained from newsgroups [42]. Therefore, email spammers use web crawlers to fetch HTML documents. Then, the crawler parses the HTML documents to retrieve email addresses and links to other websites. These harvested email addresses are stored in a database as a list of potential customers. The operation of the web crawler is shown in figure 3.10.

After obtaining the list of email addresses, the automated software can schedule email messages to be sent to all the addresses in the database. The harvesting of SIP URIs for the IMS can re-use email web crawlers since the sources remain the same HTTP documents, and the syntax of the SIP URIs are similar to email addresses.

SPIT senders can easily obtain a list of IMS public user identities. Next, bulk call generators for voice are needed to send SPIT to all addresses harvested. One such tool that can be modified for this bulk call function for the IMS is SIPp [52].

The next subsection will discuss the signalling and procedures required to make a voice call from one user to another in the IMS. Then an outline of the procedures that follow once a spammer hits a decoy UE is presented. Lastly, this section presents the IMS procedures and signalling that occur once a banned spammer tries to initiate voice calls. These subsections present the operation of the decoy system for voice calls in an IMS domain.

University of Cape Town

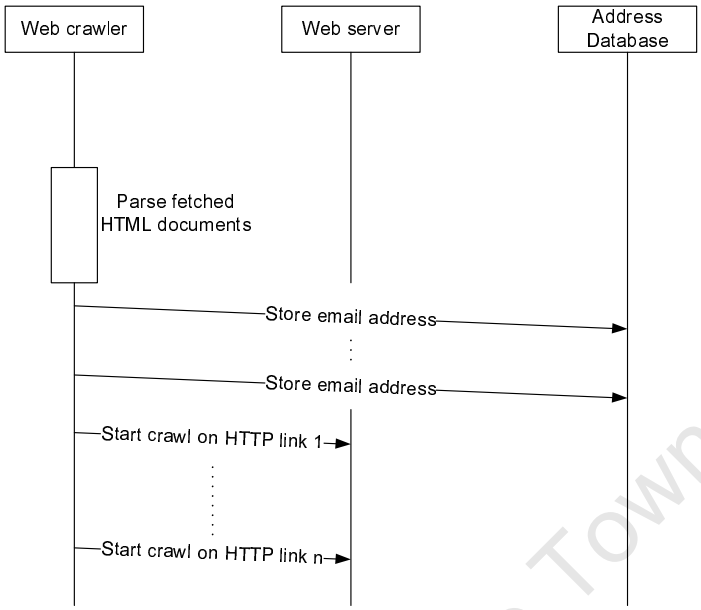


Figure 3.10: Web crawler fetching email addresses and HTTP links for future sources of HTML documents.

3.5.1 Scenario: IMS Procedure to Make a Voice Call

For this scenario, this thesis assumes a voice call from UE#1 to UE#2 who are both registered. The signalling flows are illustrated in figure 3.11.

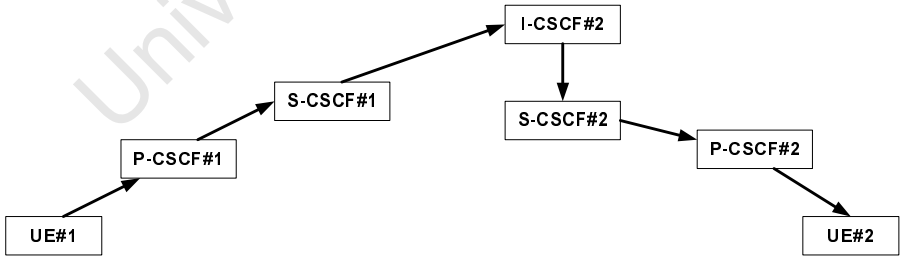


Figure 3.11: Flow of the Initial SIP INVITE from UE#1 to UE#2.

The initial INVITE from UE#1 is sent to S-CSCF#1 via P-CSCF#1. This route was determined during registration. However, S-CSCF#1 performs a DNS query to locate I-CSCF#2, entry point to the home network of UE#2. Further, I-CSCF#2 queries the HSS for address of S-CSCF#2 to forward the INVITE

University of Cape Town

message. The route to UE#2 from S-CSCF#2 has been established during registration. Therefore, the S-CSCF forwards the INVITE to UE#2 via P-CSCF#2 without any external queries.

For this thesis, it is important to highlight that S-CSCF#1 downloads the service related data from UE#1's HSS. For this task, the S-CSCF#1 uses the Cx interface and the Server Assignment Request (SAR) command. The HSS replies with a Server Assignment Answer (SAA) command that contains the service profile of UE#1. This service profile is used by the S-CSCF to ensure that UE#1 has the right to make voice calls. The core network service authorisation part of the service profile is used for this media authorisation function. Subsequently, the two UEs must agree on the media and the codecs and the network performs resource reservation before a voice message can be received by UE#2.

3.5.2 Scenario: Voice Call from Spammer to Decoy

Once a voice call is made to a decoy UE, the decoy UE parses the INVITE message retrieving the public user identity of the sender. This identity is sent to the sender's HSS using the Spam-Id command as discussed in section 3.4.3. The decoy UE keeps a log of the public user identities for future reference. Consequently, the sender's HSS, on receiving the Spam-Id command, updates its databases as discussed in section 3.4.6. However, the voice call to the decoy UE is allowed to continue to completion.

In the case that this is the second decoy UE that this particular sender has hit using the same public user identity, then this user is blacklisted. Blacklisted means that the integer corresponding to voice calls in the core network authorisation is removed from the service profile. This change in service profile causes the HSS to send a Push-Profile-Request (PPR) message to the S-CSCF indicating the new service profile. A Push-Profile-Answer (PPA) message is sent back by the S-CSCF. This mechanism of notifying change in service profiles is already present in the IMS and is not a modification by the decoying system.

University of Cape Town

3.5.3 Scenario: Voice call from Spammer Blocked

Once a blacklisted spammer decides to initiate a voice call, the S-CSCF will check the service profile to check if audio messages are allowed by this subscriber. The spammer will fail this check and a SIP 488 (Not Acceptable Here) is returned by the S-CSCF. This scheme is already part of the IMS.

It is important to highlight that the decoying system only installs the decoy UEs, sends blacklist messages to HSSs, and these HSSs then modify their databases accordingly. However, the other transactions mentioned in this section for the various scenarios are already present in the IMS framework. These functions help to block the spammers and so complete the decoying system.

3.6 Mobility Requirements

The IMS framework was designed for mobility. Therefore, the decoying system should be designed to work in such a mobile environment. This section discusses the mechanisms of IMS mobility and if the decoying system will be effective for a mobile user.

The IMS supports three types of mobility: personal mobility - users can access IMS services independent of the network and the terminal used, terminal mobility - users can access IMS services while the terminal is moving, and session mobility - this ensures that the session continues when the point of attachment of the terminal changes. For IMS, mobility is catered for by re-registration i.e. when a terminal moves to a new P-CSCF, the terminal issues a new registration attaching the public user identity to a new contact address. Furthermore, users can change terminals by removing the ISIM from one terminal and placing it in another. This allows the same service access from different terminals. Not only that, IMS permits one or more terminals to be registered using the same public user identity.

The decoying system continues to work well even if the spammer changes terminals or moves to a new access network with a different P-CSCF. As long as the spammer is registering using the same public user identity, then all further calls can be blocked with the proposed decoying system. In addition, the decoying system is capable of blocking calls from all terminals registered with the same public user

University of Cape Town

identity. Since the decoying system blocks calls based on the principle that public user identities are linked to service profiles, and mobility scenarios do not change the public user identity, so the decoying system requires no modification for mobile spammers.

3.7 Chapter Discussion

With regard to the design requirements mentioned in section 3.2, the design fulfils all these requirements. The decoying system is effective for mobile scenarios, does not tear down any IMS interfaces but adds a few more features, and decoys can be placed in any access network. For the decoying system to be effective, it utilises the strong authentication procedures present in the IMS. Furthermore, service subscriptions will cost money in the IMS, hence disposable accounts will not be present for the spammers as is the case for emails.

The proposed decoying system requires no modification of user terminals, and users are unaware of its presence. Moreover, the decoying system does not rely on any user input or feedback. As to the assessment of the overheads caused by the decoying system, this is investigated in later chapters. For this reason and proof of concept, an evaluation framework will be presented in the next chapter.

University of Cape Town

Chapter 4

Implementation of an Evaluation Framework

University of Cape Town

4.1 Introduction

The previous chapter introduced the proposed decoying system, and how this system works in an IMS framework. Detailed descriptions of the protocol and interface modifications required for deployment of the proposed system, with the aim of reducing SPIT, was presented as well. The primary purpose of this chapter is to outline in detail how a test bed framework is set up for proof of concept of the decoying system. Furthermore, detailed implementation procedures is described, and a discussion of the limitations of the test bed is presented.

This test bed framework further aims to illustrate that the decoying system causes low overheads and works well in situations when the network load is high. Additionally, the various components of the test bed framework is discussed in detail, with emphasis on the decisions made given alternate choices. It is significant to state that several choices of software and implementation algorithms are also discussed in this chapter.

4.2 Objectives and Requirements of the Evaluation Framework

The objectives of implementing a test bed are outlined below:

- The primary aim of the test bed framework is to prove that the decoying algorithm proposed is capable of blocking SPIT senders. This evaluation framework should incorporate two decoy UEs that when hit by any spammer, modifies the spammer's account. Moreover, the framework implemented should allow observation of calls being blocked from senders who have hit both decoy UEs.

- The decoying system described in the previous chapter includes additions to the IMS framework. These additions include an interface from the decoy UEs to the HSSs and a software program to be installed on the HSS, capable of modifying service profiles. The evaluation framework emulates the procedures present in the IMS HSS and S-CSCF. Therefore, the feasibility of incorporating the mentioned additions to the IMS can be shown by the workings of the evaluation framework.

- As compared to other SPIT filtering techniques, the decoying system is designed to cause low overheads on the IMS core entities. Another purpose of the evaluation framework is to deduce that incorporating a decoying system on the IMS does not adversely affect voice services during periods of high traffic. Moreover, the evaluation framework should facilitate the testing of the decoying system under different loads.

- There is a large number of email spam messages present in todays networks. This fact can lead to the assumption that spammers send a large quantity of spam messages within a short amount of time. Many of the SPIT filtering techniques under research may fail in conditions where the rate of spam is just too high. The decoying system should be robust enough to deal with spammers at even the high rates. To test this claim, the evaluation framework should allow the rates of spammers to be set to different values and observation of the performance of the decoying system to be recorded.

University of Cape Town

- The evaluation framework is meant to be a contribution of this thesis and should be able to be used for performance evaluations of other SPIT filtering techniques. Therefore, the spammer implemented should behave as a spammer in all aspects; it should collect addresses from a website and schedule pre-recorded voice messages to be sent to these harvested addresses. In addition, a need for background voice traffic to analyse the performance of the SPIT blocking technique is necessary together with a means to collect data.
- Another aim of the evaluation framework is to allow comparison of the network resource utilisation in terms of three different networks; a network with only legitimate senders, a second network with voice spammers, and a third network with both spammers and a decoy system. This network utilisation can be gauged using the number of legitimate messages, the number of failed calls, and the call duration which includes the time to set up the call. For the three different networks mentioned, the evaluation framework should allow recording of the mentioned data and so permit a quantitative comparison to be performed.

Chapter 5 will give a detailed discussion on the tests performed using the implemented evaluation framework.

Several of the requirements of the evaluation framework were mentioned in the discussion on the objectives of the framework. These mentioned requirements include the need to establish background voice traffic; data collection that enables derivation of failed calls, number of legitimate calls, and call duration; and a complete spammer architecture. However, several requirements were not mentioned and so requires discussion. In this discussion, some of the limitations of the test bed, mentioned in chapter 1, will be mentioned again.

To begin with, the evaluation framework requires several different components, highlighted in table 4.1 together with the functions these components need to perform.

Table 4.1 shows that two decoy UEs and two spammers are required for the test bed architecture. There is no particular reason for two spammers but just to incorporate tests involving multiple sources of voice spam in the decoying system. For the case of two decoy UEs, this is important since a spammer must hit two different decoys in order to be blacklisted.

University of Cape Town

Table 4.1: Components needed for the test bed and their functions.

Component	Functions
IMS SIP Proxy / Router	Routing of voice calls.
IMS HSS	Database of service profiles.
Voice traffic senders and receivers	Senders send IMS voice messages to the receivers.
2 Decoy UEs	Act as a receiver, parse SIP INVITE messages for public user identify of sender, and send blacklist messages to the HSS.
2 Spammers	Harvest address from website and send pre-recorded voice calls to these addresses.
Web server	Host website containing SIP URIs of all the receivers and the two decoy UEs.

University of Cape Town

For the sake of completeness and to cover every possible factor in call set up, the senders and spammers are required to send actual voice messages to the receivers. This would ensure greater processing and allow inclusion of times required for codec negotiation in the call duration times.

Mobility is an important factor in the operation of the decoying system. However, as discussed in the previous chapter, changing the P-CSCF does not change the public user identity. Therefore, the decoying system will be as effective in the mobile as in the non-mobile case. In consideration of this, the test bed will not be required to test the decoying system with mobile spammers.

The test bed aims to prove the decoying concept and gauge its performance benefits. For this reason, implementing an IMS framework with several proxies is not required. For the tests required to be performed, implementation of one proxy and HSS will be sufficient.

It is not necessary to implement the different SIP signalling present in the IMS for call set up, and those required for QoS provisioning. The aims of the tests to be performed on the evaluation framework does not deal with QoS, hence a complete IMS signalling is not required for the UEs.

The decoying system relies on the assumption that users cannot spoof identities, and identity theft is extremely difficult for the IMS due to the ISIM module. However, implementing a hardware based ISIM authentication is beyond the scope of

this thesis, and so it is assumed that no identity spoofing can take place for the evaluation framework. However, authentication of users are required in the evaluation framework. So, registration should be incorporated in the UEs, allowing the UE to verify its identity using a password.

There are several tests that are required in order to establish the robustness of the system under different network loads. To establish different loads, it is imperative that there be a mechanism in place that will allow the number of voice messages sent per second to be changed for the senders and the spammers.

Lastly, the implemented framework should include two decoy UEs capable of retrieving public user identities. Moreover, a secure communication should be present between the decoy UEs and the HSS to transmit blacklist messages. The HSS should also include a program to process these blacklist messages and block accounts of spammers.

It is worth mentioning that the design included a mechanism to erase the temporary database containing list of users who have hit only one decoy UE after 24 hours. This is not necessary for the test bed since the tests run will span a time frame less than 24 hours. Further, it is beyond the scope of this research to validate the refreshing of this temporary database after 24 hours.

University of Cape Town

4.3 Decision on Test Bed Implementation and Tools Used

Although, hardware test beds are limited in scale due cost and limitations of resources, hardware test beds are better tools than simulation framework in demonstrating and proving a novel idea. Furthermore, hardware test beds consider all the real world factors, whereas simulations tend to include those factors that are regarded as important. This reason can sometimes lead to simulations overlooking factors that can have an effect on the results obtained.

This research introduces a novel scheme for SPIT blocking in the IMS. For this reason, it would be more beneficial to have a small scale prototype than a simulation. Further, the aim of the evaluation framework is for proof of concept which

is better illustrated using real hardware than a simulation environment. Implementing a test bed provides another benefit in that results from a test bed are easier to transfer to a commercial setting since a prototype is present.

For this research, therefore a real hardware implementation is more beneficial than a simulation architecture. The IMS is a new concept and there are few open source tools that allow simulations of this IMS framework. Moreover, quantitative results obtained from a hardware test bed are closer to performance of a system in a real world network than for the case of those obtained in simulations.

Firstly, it is important to mention the functions of the tools that are required for implementing this hardware test bed. This hardware test bed requires a tool that can generate SIP voice calls. Another tool is required that can be used to implement a modified SIP proxy with a database. This study aims to choose tools that are open source and so can be modified to suit the needs of the decoying system. Several of the implementation required in this research will be performed using custom written programs. The next parts of this section will propose alternatives for the two tools mentioned, and a suitable decision will be made with regard to the requirements of the test bed as discussed in section 4.2.

University of Cape Town

The tools that were looked at for the SIP proxy include Asterix [53] and Iptel SIP Express Router (SER) [54]. A discussion on the properties of these two tools are as follows:

- Asterix is an open source software for hybrid time division multiplexing (TDM) packet voice private branch exchange (PBX). Its main design philosophy incorporates several VoIP protocols including SIP since this software was designed primarily for interworking different protocols. Asterix can interoperate with most SIP phones but has problems in its time stamp and wake up procedures for a purely VoIP set up. This problem can be solved by loading a kernel module for the VoIP phones. On the up side, C programming can be used by developers to add new functionality to the Asterix PBXs, adding to the flexibility of Asterix. The architecture of Asterix is simple and different from other telephony servers in that Asterix acts as a middleware connecting telephony technologies on the bottom layers, to telephony applications on the top layers.

- The Iptel SER was primarily designed for the SIP protocol and can act as a SIP registrar, proxy, or redirect server. It is open source and very robust. This software supports accounting, authorisation, radius, server monitoring, and web based user provisioning. This SER is written in C and can be installed on Linux. It incorporates different modules that can be loaded for added functionality. Moreover, the Iptel SER has a small code size of about 300kB for the core installation.

After careful consideration, it was decided that the Iptel SER was more suitable for the purpose of this research. The reasons for this choice will be briefly outlined in this paragraph. The SER provided an easier implementation requiring a smaller code size than Asterix. Furthermore, Asterix has many features that are not necessary for this test bed and so makes the configuration and installation of Asterix more difficult. SER is designed to work with the SIP protocol which is the requirement of this evaluation framework, but Asterix was designed for an interworking solution for several protocols. This interworking philosophy is not pertinent for this thesis. Moreover, Asterix has a large document base as compared to Iptel SER. This means that more research is required in understanding and implementing new functionality in Asterix. Furthermore, the Iptel SER requires the modification of only one configuration file for set up, whereas Asterix has several configuration files that must be adjusted.

For the decision on selecting a tool for automatically generating SIP voice calls, this thesis looked at three open source software. These tools are discussed as follows:

- Sipsak [55] is a small command line tool which can be easily installed on Linux distributions. This tool allows simple tests to be performed for SIP clients and servers. Sipsack is very versatile with authentication mechanisms and allows SIP messages to be sent to any address. It also includes a search string functionality using regular expressions and has flooding tests incorporated in the core install. However, this tool is not fully RFC 3261 [12] compliant and cannot be used for IPv6 traffic.

- EXosip2 [56] (extended osip library) is a high level API allowing the implementation of SIP clients and extensions. This stack has no support for RTP

University of Cape Town

or audio interface. However, this API does include features for call management, messaging, and presence. Another feature of the eXosip2 stack is the inclusion of the authentication module allowing passwords to be assigned to users.

- SIPp [52] is an open source SIP traffic generator. This tool relies on XML scenarios for custom call flows and SIP clients. It has mechanisms for authentication, IPv6 traffic, and custom scenarios. This tool supports the use of regular expressions for string matching in the received SIP messages. Moreover, SIPp incorporates simple RTP and audio support. The main function of this tool is to perform stress tests on SIP devices, hence has methods that can control the calls made per second. Furthermore, SIPp incorporates collection of statistics.

SIPp is not the most flexible of all tools, but allows quicker implementation of SIP clients using XML scenarios. The implementation of clients using the eXosip2 stack can provide more functionality but would be more cumbersome. As to sipsack, it is unsuitable for implementing a complete SIP client. With regard to voice transmissions, only SIPp is suitable for such a task. Furthermore, SIPp has methods for authentication and data collection which is important for this evaluation framework. Therefore, SIPp was chosen for implementing the automated SIP clients sending voice calls in the evaluation framework.

University of Cape Town

4.4 Overview of the Test Bed

The previous sections of this chapter discussed the requirements and the limitations of the evaluation framework. And, section 4.3 looked at the choices of the tools to be used in building the test bed. This section briefly gives an overview of all the components in the test bed. The overall layout, components, and their interconnections is presented in figure 4.1. This section plays an introductory role for the next section which will delve deeper into the implementation details of every single component that make up the evaluation framework.

One host of the test bed is used as a S-CSCF and a HSS. The S-CSCF is implemented by the Iptel SER acting as a SIP proxy. The HSS is implemented using

MySQL databases. The SER is modified for authentication of users using the MySQL database. This database contains user names and user passwords. Further, the database is modified to contain media authorisation for audio messages. In addition, a program is installed on this HSS that is capable of removing this audio media authorisation. This program is written in C++ and is responsible for processing decoy blacklist commands.

As illustrated in figure 4.1, background traffic generators are distributed on two host machines. These background traffic generators are implemented using SIPp. A limitation of this tool is that clients can be set up as either receivers or senders of voice messages but not both. The purpose of the background traffic generators is to create different loads on the S-CSCF. For this purpose, the call rates of the senders can be set to different values. These senders send a 8 second voice message to all the receivers. The receiver is chosen at random. It is important to state that the senders send voice messages to the receivers only and not to the decoys. Furthermore, the senders and receivers register with the S-CSCF using a user name and a password. These implemented receivers allow all voice messages to go on till completion.

The spammers are similar to the senders, but with an added modification. These spammers retrieve an HTML file from the University of Cape Town Communications Research Group (CRG) web server. This HTML file is parsed to retrieve SIP URIs of all the receivers and the decoys present in the evaluation framework. These URIs are stored in a file, and the spammers schedule voice messages to be sent to all these addresses. Just like the senders, the spammers must register with the S-CSCF using an user name and a password. Furthermore, the call rate of the spammers can be set to different values.

The last component in the evaluation framework are the two decoy UEs. These are similar to the receivers and must also register with the S-CSCF using an user name and password. But, the decoy UEs parse the INVITE message to retrieve the public user identity of the sender. This identity together with the decoy serial number is sent to the HSS.

It is significant to mention that the SIP signalling for these components is not IMS compliant. The next section will present in detail how these components were implemented in the test bed.

University of Cape Town

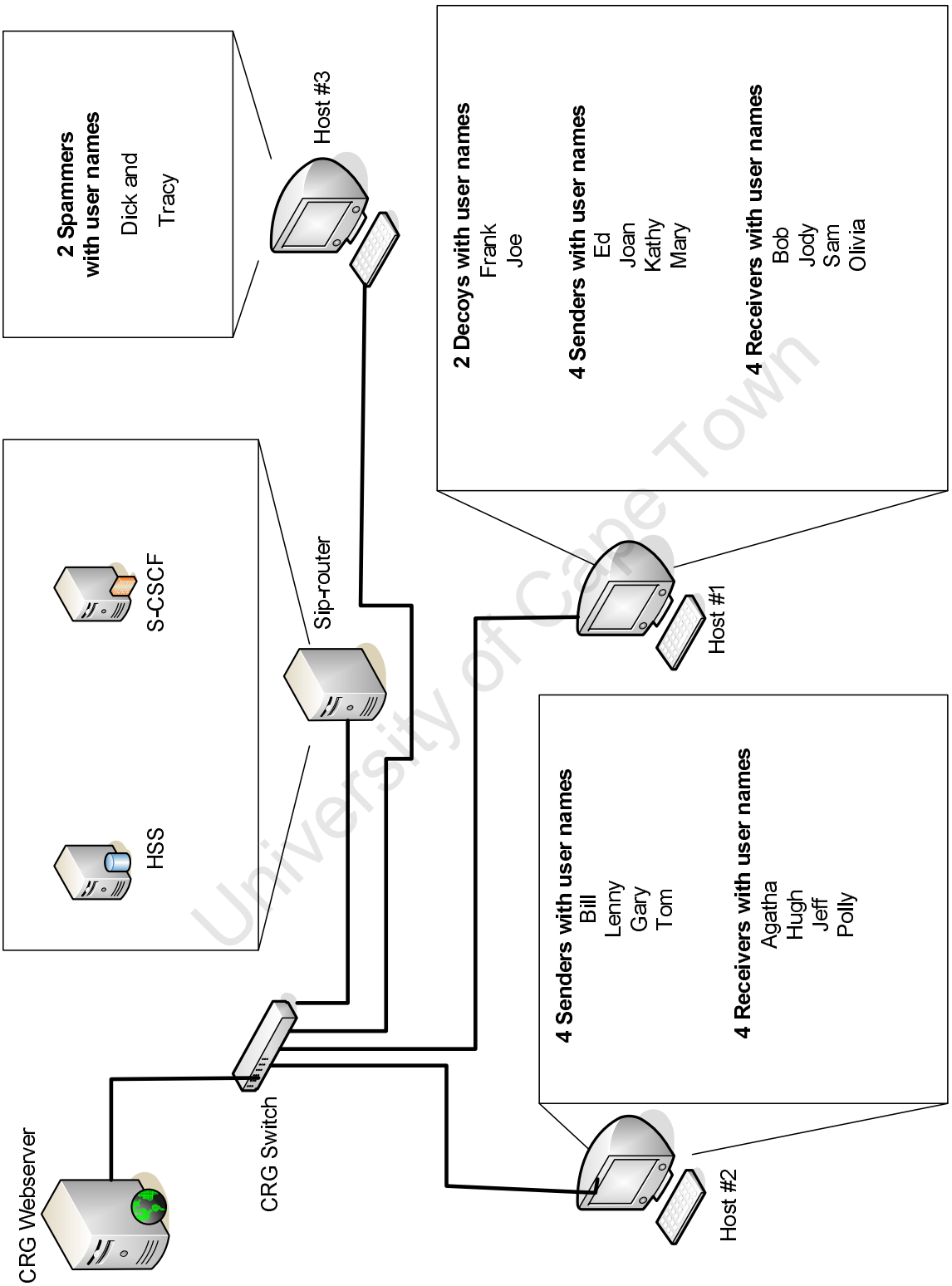


Figure 4.1: Complete layout of the test bed.

University of Cape Town

4.5 Detailed Implementation of Test Bed Components

This section gives the implementation details for the evaluation framework. The section will start off by discussing the registration and authentication mechanisms implemented. Implementation of the various components will be outlined as well.

4.5.1 Registration and Authentication

```
Resolving remote sending address sip-router...
Resolving remote host 'sip-router'... Done.
------------------------------ Scenario Screen -------- [1-4]: Change
Screen --
  Call-rate(length)     Port   Total-time  Total-calls  Remote-host
   1.0(0 ms)/1.000s   5047       2.00 s           2  10.128.0.83:5060
(UDP)

  Call limit reached (-m 2), 0.003 s period  1 ms scheduler resolution
  0 concurrent calls (limit 3)           Peak was 1 calls, after 1 s
  0 out-of-call msg (discarded)
  1 open sockets

                                 Messages  Retrans   Timeout
Unexpected-Msg
    REGISTER ---------->           2         0         0
         401 <----------           2         0                   0
    REGISTER ---------->           2         0
         200 <----------           2         0                   0
------------------------------ Test Terminated --------------------
```

Figure 4.2: Output from SIPp during registration of a receiver.

In the IMS, authentication using passwords and user names are done using HTTP digest mechanisms [57]. Digest authentication involves cryptographic hashes to prevent transferring of passwords in text. This digest authentication scheme relies on a shared secret i.e. the password. Figure 4.2 shows the SIP message exchange for digest authentication during registration in the test bed. This test bed also incorporates INVITE with authentication as shown in figure 4.4. This INVITE authentication although not part of the IMS is incorporated into this evaluation framework to ensure further security enhancements. Moreover, this additional signalling can increase the load on the SIP proxy and HSS. This is helpful in analysing the effectiveness of decoy algorithms on the proxy and the HSS.

University of Cape Town

```
10.128.0.83:5060 -> 10.128.1.252:5047
  SIP/2.0 401 Unauthorized..Via: SIP/2.0/UDP 10.128.1.252:5047;
  branch=z9hG4bK-2-0..
  From: ua1 <sip:sam@sip-router:5047>;tag=2..
  To: ua1 <sip:sam@sip-router:5047>;
  tag=b27e1a1d33761e85846fc98f5f3a7e58.1fd0..
  Call-ID: 2-9485@10.128.1.252..
  CSeq: 1 REGISTER..WWW-Authenticate: Digest realm="sip-router",
  nonce="45a23ac9e8e6ac3a9c2118c5dc526da9f6d9c780"..
  Server: Sip EXpress router (0.9.6 (i386/linux))..
  Content-Length: 0..Warning: 392 10.128.0.83:5060
  "Noisy feedback tells:  pid=5173
  req_src_ip=10.128.1.252 req_src_port=5047
  in_uri=sip:sip-router out_uri=sip:sip-router via_cnt==1"

10.128.1.252:5047 -> 10.128.0.83:5060
  REGISTER sip:sip-router SIP/2.0..
  Via: SIP/2.0/UDP 10.128.1.252:5047;
  branch=z9hG4bK-2-2..
  From: ua1 <sip:sam@sip-router:5047>;tag=2..
  To: ua1 <sip:sam@sip-router:5047>..
  Call-ID: 2-9485@10.128.1.252..
  CSeq: 1 REGISTER..Contact: sip:sam@10.128.1.252:5047..
  Authorization: Digest username="sam@sip-router",
  realm="sip-router",uri="sip:10.128.0.83:5060",
  nonce="45a23ac9e8e6ac3a9c2118c5dc526da9f6d9c780",
  response="1ec6b9ead9f539e2f0d1fc76935ee44f",algorithm=MD5
  ..Content-Length: 0..Expires: 720000....
```

Figure 4.3: Format of REGISTRATION and 401 messages captured from the sip-router using ngrep.

The first REGISTER message in the digest authentication scheme includes no password. The SIP proxy subsequently returns a 401 (Unauthorised) message that includes a digest challenge. The format of this 401 message in the test bed, captured using ngrep [1], is shown in figure 4.3. Furthermore, the cryptographic algorithm used in the test bed is MD5. The UE on receiving the digest challenge, responds with a REGISTER message that includes a digest response. Figure 4.3 shows the structure of this REGISTER message, and the response field includes the encrypted password.

Another functionality of the REGISTER messages is to update the user's location. The contact field in the REGISTER message, shown in figure 4.3, includes the

[1]Ngrep: tool for monitoring network traffic on a specified port.

University of Cape Town

address to which any SIP messages to the corresponding public URI are forwarded by the S-CSCF.

Authentication of users is significant in this study and the test bed. The reason for this is that user authentication is required for any system that blacklists users and so must prevent identity theft. In terms of the test bed, authentication increases queries to the databases in the HSS and causes overheads on core elements present in the IMS. This factor cannot be ignored in analysing the performance of the decoying system.

4.5.2 Background Traffic Generation

The evaluation framework implemented 8 senders and 8 receivers. The number of senders and receivers is chosen as 8 since it is assumed that this will be large enough to create a significant load on the SIP proxy. This study will assume that a high load is experienced when the S-CSCF has to process more than 40 SIP sessions per minute. To achieve this, the 8 senders have to send one voice call every 10 seconds, 8 senders * (60/10 calls per minute per sender) = 48 sessions per minute.

University of Cape Town

```
                                Messages  Retrans   Timeout
REGISTER ---------->            1         0         0
     401 <----------            1         0                   0
REGISTER ---------->            1         0
     200 <----------            1         0                   0
  INVITE ---------->            4         0         0
     407 <----------            4         0                   0
  INVITE ---------->            4         0
     100 <----------            4         0                   0
     180 <----------            0         0                   0
     200 <---------- E-RTD      4         0                   0

     ACK ---------->            4         0
         [ NOP ]
   Pause [   8000ms]            4                             0
     BYE ---------->            4         0         0
     407 <----------            4         0                   0
     BYE ---------->            4         0         0
     200 <----------            4         0                   0
```

Figure 4.4: SIP signalling done by the sender in the test bed.

```
                                  Messages  Retrans   Timeout
  ----------> INVITE             4         0                   1

  <---------- 200                4         0
  ----------> BYE                3         0                   0
  <---------- 200                3         0
  [   2000ms] Pause              3                             0
------------------------------ Sipp Server Mode ------------------
```

Figure 4.5: SIP signalling done by the receiver in the test bed.

The signalling for the senders is illustrated in figure 4.4, and that for the receivers is shown in figure 4.5. The total number of messages in a SIP session, not including packets required for the voice messages, as deduced from the two diagrams is 14. Therefore, if 48 sessions are established during one minute then the S-CSCF has to process about 672 messages per minute (48 sessions per minute * 14 messages per session). This constitutes a significant load for the proxy.

With regard to the SIP signalling, both the receivers and the senders require INVITE authentication. This involves the first INVITE message containing no passwords. On receiving a 407 (Proxy Authentication Required) message, an INVITE with credentials is sent back. It is worth mentioning that the senders perform registration every 50 seconds so as to be able to test if the blacklisting, done by the decoy UEs, can be overcome by a new registration.

It is significant to state that the senders use a text file containing SIP URIs of receivers, and so only send messages to the receivers. The receiver is chosen at random. This puts an extra control factor on the evaluation framework since the senders can never hit the decoys. However, implementing senders that mimic human behaviour, and thus in some circumstances do hit the decoys, is left out of this study.

Previous research on analysing email spam filtering techniques utilised a group of senders and receivers, where the senders and receivers were chosen according to probability distributions [37]. This is similar to this implementation with the exception that several senders are not sending traffic simultaneously. Therefore, for the purpose of this study considering loads on the S-CSCF, the implemented method of generating traffic, with several senders sending traffic simultaneously, seems more reasonable. In other research into email spam filter analysis, no sender

University of Cape Town

or receivers were included but different email messages were utilised [36]. These type of input are suitable for filtering methods that depend on the analysis of message content and is not suitable for this research. For the case of reputation networks preventing SPIT, the first method of generating background traffic was utilised [21]. A better method involves evaluating a prototype on a real network. This method was performed by Talavan for evaluating his proposed greylist email filter [35]. However, this could not be done for this research as SPIT is an expected problem and not present in large enough quantities in todays networks.

4.5.3 Spammers

Spammers are similar to the senders with the exception that the spammers retrieve their destination SIP URIs from a website. This website contains addresses of all the receivers and the two decoys present in the test bed. Hence, the spammers do eventually send voice messages to the two decoys. As a result, they are blacklisted and prevented from making further voice calls.

The web parser implemented, for the automated spammers, downloads an HTML document from a web server. The address of this HTML document is http://crg.ee.uct.ac.za/~aka/test-bed. Next, it parses the HTML document and stores all strings containing the "@" character in a text file. This text file acts as a database of addresses that a spammer will send voice messages to.

In literature, analysis of Bayesian email spam filters modelled spam messages according to their content [36, 37]. Furthermore, for evaluations of voice spam filter using reputation methods, the spammers were modelled according to user input. It is safe to conclude that spammer behaviour was modelled according to the spam filter being investigated. For this research, two properties of automated spammers are required. Firstly, a spammer retrieves addresses from websites that may contain addresses of decoys. Secondly, the spammer sends voice spam messages to all harvested addresses. Both these mentioned criteria is implemented in the evaluation framework.

University of Cape Town

4.5.4 Decoy UEs

The operation of the decoy UEs is presented in figure 4.6. This figure shows that on receiving a voice message the decoy UE retrieves the sender's address form the INVITE message using regular expressions. Regular expressions are expressions that are used to specify string search patterns. An INVITE message in the evaluation framework is shown in figure 4.7 and the sender's URI is highlighted. This URI is retrieved by the decoys.

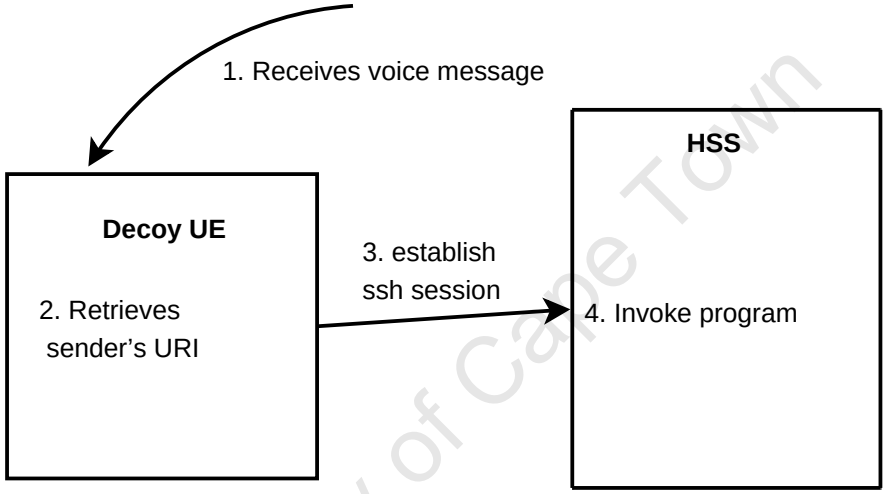
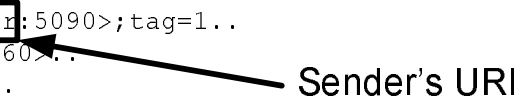


Figure 4.6: Operation of a decoy UE.

There are decoys present in the evaluation framework. The user names of these decoys are frank and joe. Joe has a serial number of 1098, and frank has a decoy serial of 2040. After retrieving the URI of the sender, the decoy UE establishes a ssh (secure shell) connection with the HSS. In the evaluation framework, there are many clients being executed from the same host; therefore the decoys are executed with root privileges so that only these decoy clients have access to this ssh session. Using this ssh session, the decoy UE invokes a program on the HSS with the decoy serial number and sender's URI as arguments. This program is responsible for modifying databases on the HSS and will be discussed in section 4.5.6.

University of Cape Town

```
10.128.0.83:5060 -> 10.128.1.252:5047
  INVITE sip:sam@10.128.1.252:5047
   SIP/2.0..Record-Route: <sip:10.128.0.83;
   ftag=1;lr=on>..
   Via: SIP/2.0/UDP 10.128.0.83;branch=z9hG4bKdaa8.13743c36.0..
   Via: SIP/2.0/UDP 10.128.1.252:5090;branch=z9hG4bK-1-6..
   From: ua1 <sip:kathy@sip-router:5090>;tag=1..
   To: ua2 <sip:sam@sip-router:5060>..
   Call-ID: 1-14711@10.128.1.252..
   CSeq: 1
   INVITE..Contact: sip:kathy@10.128.1.252:5090..
   Proxy-Authorization: Digest username="kathy@sip-router",
   realm="sip-router",uri="sip:10.128.0.83:5060",
   nonce="45a3a50fba8e209e26b2d2963dc153664a6aba18",
   response="2c2423155d8bd16adb8c24802b69281a",
   algorithm=MD5..Max-Forwards: 16..
   Subject: Performance Test..
   Content-Type: application/sdp..
   Content-Length:  190..
   P-hint: usrloc applied....
   v=0..
   o=user1 53655765 2353687637 IN
   IP4 10.128.1.252..
   s=-..c=IN IP4 10.128.1.252..
   t=0 0..m=audio 6011 RTP/AVP 8..
   a=rtpmap:8
   PCMA/8000..
   a=rtpmap:101 telephone-event/8000..
   a=fmtp:101 0-11,16..
```



University of Cape Town

Figure 4.7: INVITE message structure in the evaluation framework, highlighting the URI of sender.

4.5.5 Interface Between Decoy UE and HSS

Section 3.4.3 discussed the operation of the interface between decoy UE and the HSS. This interface utilised the diameter protocol and relies on a set of shared keys for authentication. Furthermore, the interface is encrypted for security reasons. The evaluation test bed implements the functionality of this interface by using a secure shell (ssh) session between the decoy UE and the HSS. For the purpose of this study, the ssh session will be used as a secure means of running remote commands. Just like the operation of the proposed diameter interface, an ssh connection is capable of performing the following functions:

1. Host identification: the server authenticates its identity.

2. Encryption: preventing man-in the-middle attacks.

3. Client authentication: this involves the client proving that it has certain privileges on the server.

For the evaluation framework, the ssh session was set using RSA keys. This was set up by first generating a key on the client by using the command `ssh-keygen`. The generated key is shown in figure 4.8.

```
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEA1CeDk2KF/Ejk ..
.....AAdJxWD44YQxUpOgk+5PfmSQ== root@akazor
```

Figure 4.8: RSA keys stored on the decoy host.

This public key is stored in `~/.ssh/identity.pub` and the private key is stored in `~/.ssh/identity`. The public key stored on the decoy host is shown in figure 4.8. However, only a part of the public key is displayed in this figure and the size of the public key is much larger than this. Furthermore, the public key is appended to the file `.ssh/authorised_keys` in the server. For this ssh interface, the client requests to log onto the server using the public key. The server responds with an RSA challenge encrypted with the public key. Next, the client decrypts this message with the private key and sends it back to the server, thus completing the authentication process.

The process of using this ssh interface is similar in nature to the proposed interface from the decoy to the HSS. Both interfaces employ encryption and authentication via means of shared keys. Therefore, this study assumes that the performance of the two interfaces will be of the same magnitude in terms of time and resource utilisation. It should be noted that in this discussion the client refers to the decoy UEs and the server refers to the HSS.

University of Cape Town

4.5.6 HSS

In the IMS, the HSS is a database containing user service profile information and user locations. Further, in these service profiles user passwords and media authorisation information is stored. The test bed implementation of the HSS

varies from some of these properties. These variations and the structure of the implemented HSS is discussed in this part of the dissertation.

The Iptel SER supports a database on one host by two methods. Either the database can be implemented by flat text files or a MySQL database. The modules required and their relationships to the Iptel SER core is illustrated in figure 4.9. For this test bed, it was decided to implement the database using MySQL because in the IMS, it is unlikely that the large databases will be implemented using flat text files. The reason being flat text files are hard to manage for a large number of data.

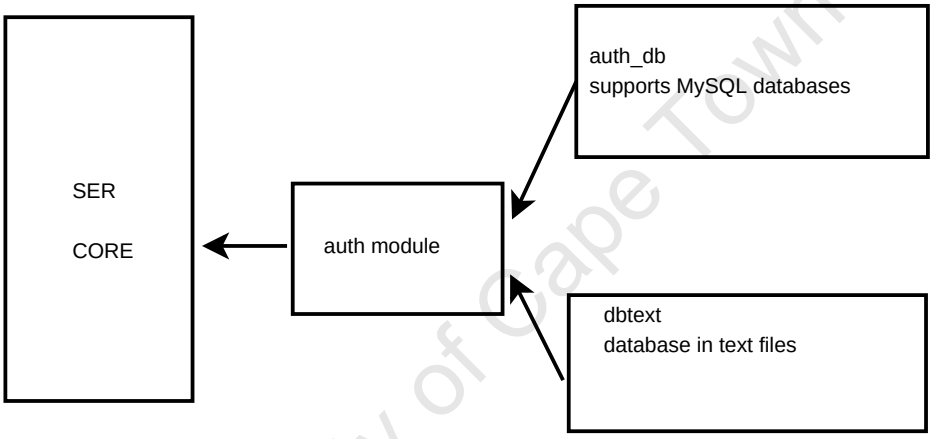


Figure 4.9: Iptel SER architecture supporting databases on one host.

University of Cape Town

The evaluation framework uses MySQL databases to store user names and their corresponding passwords together with location information. However, in order to implement media authorisation, an extra table is added to the database. For this study, it is significant to consider only audio media authorisation, and so a full service profile is not included. To add this functionality, a "grp" table was included containing all users. This table is shown in figure 4.10. The users that are allowed to make voice calls belong to the group GREEN.

The design of the proposed decoying system, discussed in the previous chapter, included two databases for processing decoy messages. However, in the evaluation framework, the "grp" table was used for this purpose as well. This was seen as appropriate since in a real network, the database containing the user service profiles or the databases for the decoy messages will be significantly larger than in the evaluation framework. Therefore, to emulate the effects of queries on these

databases in a real network, a large database combining these three databases is used in the test bed.

username	domain	grp	last_modified
joe	sip-router	green	0000-00-00 00:00:00
cro	sip-router	green	0000-00-00 00:00:00
dick	sip-router	green	0000-00-00 00:00:00
hugh	sip-router	green	0000-00-00 00:00:00
agatha	sip-router	green	0000-00-00 00:00:00
polly	sip-router	green	0000-00-00 00:00:00
jeff	sip-router	green	0000-00-00 00:00:00
jody	sip-router	green	0000-00-00 00:00:00
olivia	sip-router	green	0000-00-00 00:00:00
bob	sip-router	green	0000-00-00 00:00:00
sam	sip-router	green	0000-00-00 00:00:00
gary	sip-router	green	0000-00-00 00:00:00

Figure 4.10: Table "grp" in the database displaying users allowed to initiate audio transmissions.

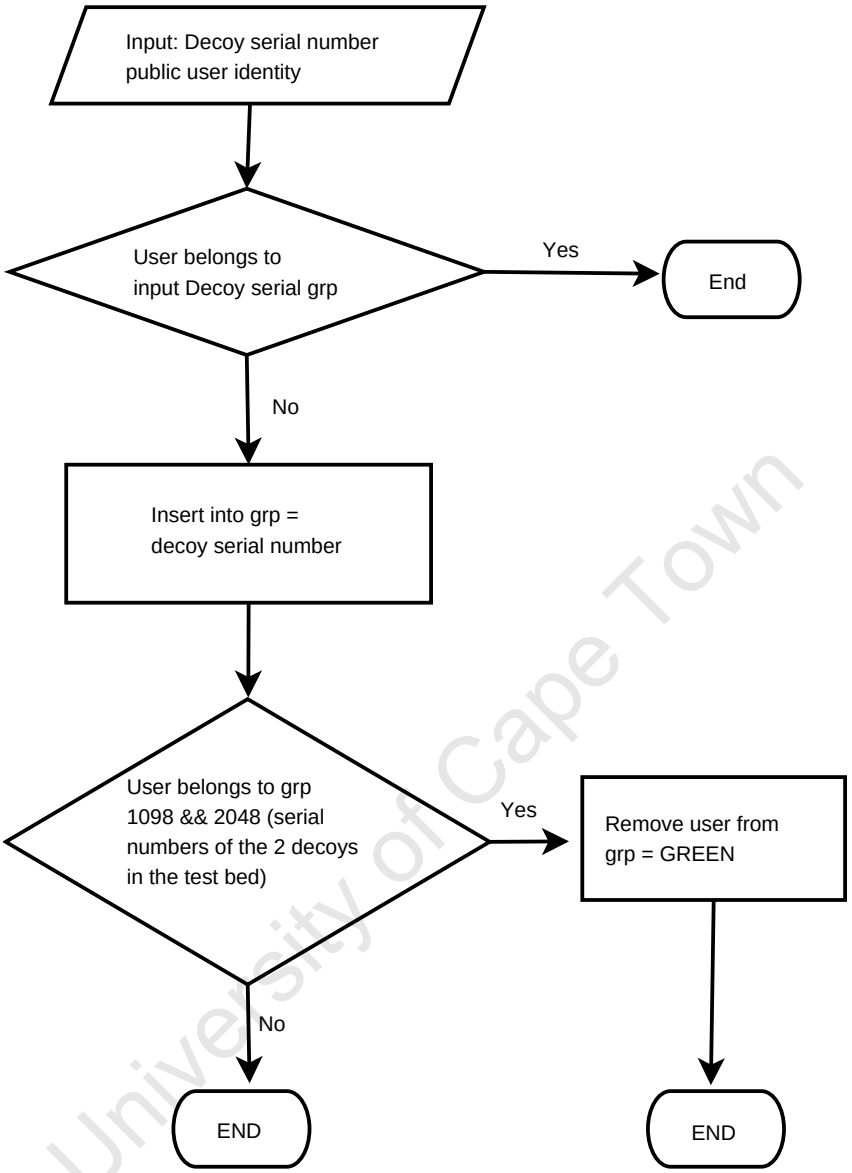
In order to process decoy messages, the HSS contains an added program. The algorithm implemented by this program is presented in figure 4.11. The decoys establish a secure ssh connection with the HSS, and then invoke this program with the decoy serial number and the public user identity of the sender as arguments. This program is responsible for removing the users from the group GREEN.

4.5.7 S-CSCF

The S-CSCF is implemented using the Iptel SER program. The SER is set up to include user authentication and provide support for MySQL databases. However, the modification required for media authorisation involves the S-CSCF checking that the sender of every INVITE message belongs to the group GREEN. The scenario that results when the user does not belong to the group GREEN is shown in figure 4.12, and this user's messages are dropped.

During the implementation of the test bed, it was considered that the S-CSCF deregister the banned user. However, using group check for every INVITE message did not require this modification.

University of Cape Town



University of Cape Town

Figure 4.11: Flow chart showing program algorithm for processing decoy messages.

4.6 Chapter Discussion

The previous chapter presented the design of the decoying system and this chapter presented how the different parts of the design were implemented in an evaluation framework. It was highlighted how the evaluation framework differs from the design, but ultimately performs a similar function of blocking SPIT. This evaluation framework contains other components to emulate a real network traffic and

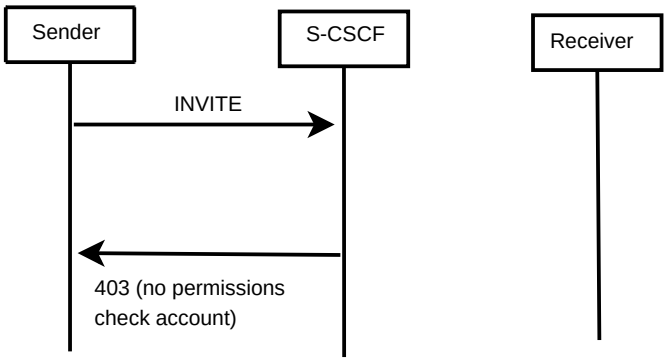


Figure 4.12: Messages exchange when a banned user initiates a voice call.

users. Moreover, limitations of the test bed was discussed. The next chapter will present the tests performed on this evaluation framework for proof of concept and the analysis of the performance factors in adopting a decoying system.

University of Cape Town

Chapter 5

Evaluation of Results and Analysis

University of Cape Town

5.1 Introduction

Chapter 3 introduced the proposed decoying solution and highlighted the changes required in the evaluation framework, and chapter 4 presented the implementation of the evaluation framework. This evaluation framework was built for proof of concept tests. Furthermore, chapter 3 mentioned the requirements of the proposed SPIT blocking solution. These requirements include effective operation during peak traffic periods, robustness, and minimum overhead for the IMS core entities. Therefore, the evaluation framework is used to prove that the proposed solution meets these requirements.

This chapter presents theoretical analysis comparing the proposed decoying solution to several SPIT filtering methods. This was briefly introduced in section 2.3.5, but the analysis presented in this chapter goes into greater detail. Moreover, the primary purpose of the implemented test bed was for proof of concept of the design. Therefore, proof of concept tests are conducted and the results are presented in this chapter. The proof of concept evaluation includes tests on the changes required to deploy a decoying solution. These tests ensure that the components of the proposed solution function as they are required to, and also prove that the system as a whole is capable of blocking SPIT senders.

Section 5.4 of this chapter presents the results of the performance tests. This section also includes relevant points and observations drawn from the results obtained. A summary of the most significant results together with the conclusions drawn from these results are discussed in section 5.5. This section ties the importance of these results to the aims of the thesis.

5.2 Analysis of Methods to Filter SPIT

This dissertation presented four different methods to filter SPIT in section 2.3.5. This section will analyse the suitability of these methods in the IMS framework together with the analysis of the proposed solution. The factors that are considered in this analysis include:

- Overheads.
- Delays in call set up.
- Performance during peak periods.
- Scalability.
- Effectiveness in mobile environments.
- Introduction of points of failure.

This analysis will begin with historical call pattern analysis to filter SPIT, as proposed by Shin and Shim [18].

5.2.1 Historical Call Pattern Analysis

This involves the proxy keeping a record of the call rate for each user. There are two variables that are used, a short term grey level - call rate for short periods - and a long term grey level - call rate based on a larger period. When the sum of these two variables exceeds a threshold, the user is prevented from making further voice calls. The overheads involve keeping record of the calls for a user on the proxy and calculating the two parameters. However, this method introduces

University of Cape Town

little overhead since the threshold check is simple. But concerning call set up delays, this method does introduce an extra step of ensuring that the sum of the two parameters is less than the threshold. The resources required for this computation is not too cumbersome and significant call delays should not occur.

Since, the overheads are little it is assumed this method will perform well during periods of high traffic. It should be considered that this method requires keeping track of every single user being served by a proxy. In cases when the number of users is high during peak periods, the load on the proxy due to parameter queries can lead to failure of this system. In terms of mobility, implementing the record keeping on the P-CSCF means that once a banned user moves to a different access network, he/she will again be able to send voice calls. This can be prevented by implementing the record keeping on the S-CSCF. This method will also ensure that historical call pattern analysis is scalable as long as voice signalling passes through the home network (thus through the S-CSCF).

However, the other downside of this sytem is that it is susceptible to false positives. Take for example, a legitimate business user who can exceed the threshold due to sending a large number of calls within a small period. Also, this system can be fooled by spammers utilising automated senders with on and off periods. This was discussed in section 2.3.5. The main inefficiency of this method is that it must monitor all users not just those sending spam. Furthermore, historical call pattern analysis allows initial spam messages to be sent before a user is blocked.

University of Cape Town

5.2.2 Reputation Networks and Trust

In this method, every user keeps a contact list and assigns a reputation value to each member in the contact list. Combining all the contact lists, a large reputation network can be generated. Social networks are modelled as graphs containing a set of nodes (n) with connections between them called edges (e). The social network formed by two users A and B is shown in figure 5.1. The reputation is denoted by the edge values.

The proposal by Rebahi and Sisalem includes a reputation network manager (RNM) that is responsible for combining all the contact lists [20]. The RNM finds all paths from the sender to the receiver in the social network and calculates

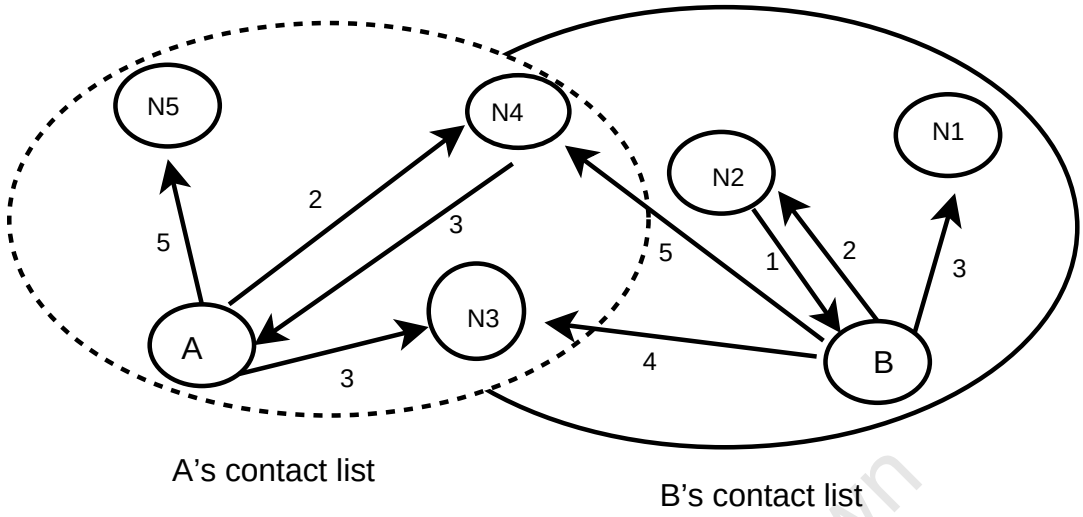


Figure 5.1: Generation of a social network.

the average reputation of all these paths. If the average reputation is higher than the set threshold then the user is blocked.

Reputation systems and social networks are not scalable at all because combining all contact lists to one reputation manager will be extremely difficult. Further, this method restricts the openness of the IMS to little closed communities. Note that the calculation complexity for a reputation network is high, of the order of O(n+e) for a social network consisting of n nodes and e edges [58]. However, a linear algorithm is more desirable. The complexity of the reputation calculation will increase the overhead on a central RNM and may lead to failure during periods of high traffic.

Since, the reputation has to be calculated for each call, this will significantly increase call set up delays in the IMS as the calculation is complex. Therefore, a reputation network for spam filtering will not be efficient for real time voice calls due to this delay [58]. One advantage of this method is that, the contact lists will most likely use public user identities and so will be able to work in mobile scenarios. On the other hand, a disadvantage of this method is that once a user of good reputation changes his/her behaviour to become a spammer, the users may be slow in updating their contact lists. To solve this problem, multi-stage filters [21] were introduced.

University of Cape Town

5.2.3 Multi-Stage Filters

Multi-stage filters proposed by Dantu and Kolan combines Bayesian learning, reputation and trust, and user feedback [21]. To be able to react to spam behaviour quickly, trust is calculated from user feedback provided through a spam button on the phone rather than contact lists. However, to deploy this method either the S-CSCF or the HSS must keep record of all users providing feedback and not just the spammers.

Another downside to this method is that it is resource intensive, since calculation complexity of reputation and trust systems is combined with the complexity of Bayesian learning algorithms. This complexity creates a larger overhead than reputation networks and introduces call set up delays. Furthermore, modifications to the signalling and the UEs are required. This system also suffers from the scalability issues of reputation networks. However, mobility does not affect its performance unless logging of user input is done by the P-CSCF. To support mobility, all records of spam feedback should be kept in the HSS or the S-CSCF.

Any computationally intensive algorithm is bound to perform poorly during peak periods when the proxies have to process a large number of calls. Hence, multi-stage filters can cause a bottleneck in the system and cause failures to the S-CSCF. However, this method is very effective in blocking SPIT, and the only other method that seems to be more effective are challenge-response methods.

5.2.4 Challenge-Response Methods

Challenge-response methods to block voice spam messages was proposed by Madhosingh [19] and was adapted for the IMS using a Spittoon AS [22]. This method involves every sender that does not belong either on the whitelist or the blacklist of the recipient to pass a Turing test. Firstly, the sender's call is redirected to the Spittoon AS which replies with a voice message containing numbers. These numbers must be keyed in correctly by the sender, and then the call is transferred to the intended recipient.

The operations done for this method is simple, however this method introduces extra signalling for call set up. Section 2.2.3 discussed the delays in call establishment for the IMS which is already cumbersome. The delays for the challenge

University of Cape Town

response can be considerable in situations involving international calls. Moreover, during high traffic the load on the Spittoon AS can be high and may cause failure. This method introduces a single point of failure, the Spittoon Server.

The scalability of the challenge-response method is good, overlooking delays in call set up for international calls. Furthermore, this system should not have a problem with mobile terminals in the IMS. The biggest advantage of this method is that it is very effective at blocking spam, and is capable of stopping almost all automated spammers.

5.2.5 Proposed Decoying Method

Addresses of decoy UEs are posted on websites by VoIP service providers. When the spammers hit two different decoys, they are blacklisted and prevented from making further voice calls. This solution is not as effective as challenge-response methods at blocking SPIT. However, this solution does not cause any change to the call set up procedure or introduce any overheads in voice call processing. The decoying system includes some processing at the network edges (decoy UEs) and some processing in the HSS. The distributive nature of the solution means that there is no single point of failure.

Unlike all the other mentioned SPIT blocking solutions, the decoying method includes no extra processing during call set up. All modifications to blacklist the user have been done beforehand. This solution is the most scalable since only accounts of spammers are recorded and modified. Also, the overheads in its operation are very low. Moreover, the decoying system performs well during periods of high traffic. For the case of IMS mobility, this decoying system bans users based on their public user identities and so is unaffected by mobile terminals.

5.2.6 Discussion

Reputation systems and multi-stage filters with their lack of scalability would be unsuitable for the IMS unless these methods are improved. Historical call pattern analysis would require large resources for logging every user. However, the decoying system although not as effective as challenge-response methods is

University of Cape Town

ideal for the newly deployed IMS. The major advantage of the decoying system is that it creates little overheads and does not cause delays in call set up. Further, deploying such a system would be easy since it utilises existing IMS procedures to blacklist users. Evaluations performed to prove the feasibility of the decoying system for the IMS is presented in the next section.

5.3 Proof of Concept Tests

Proof of concept tests are done to prove the operation of the proposed idea. It is a means to test the functionality of the system. With regard to the decoying system, this scheme proposes several modifications to the IMS architecture. The functions of these modifications are implemented on an evaluation framework, details of this evaluation framework was discussed in chapter 4. This part of the thesis will break each of the modifications implemented and test these for correctness of function.

This section will start by outlining the changes in the IMS that are required to implement a decoying solution. The modifications are presented as follows:

- The decoying system requires the installation of decoy UEs in IMS access networks. Several decoy UEs can be implemented virtually on one host, saving capital and resources.
- The decoying solution also requires the posting of SIP URIs of the decoy UEs to public websites and newsgroups.
- The blacklist messages require a means to reach the spammer's HSS from the decoys. Therefore, an interface is added to perform this mentioned function.
- A modification to the P-CSCF to deal with Privacy headers is required. Also, the P-CSCF and S-CSCF must include an additional database with the identity of the decoy UEs they serve and a shared key for each decoy UE. This shared key is used for security associations.
- There are three modifications required on the HSS. The HSS needs to include a database of users that have hit one decoy, and another database to store the banned users. Furthermore, the HSS requires a program that can process the blacklist messages and so result in banning the users.

University of Cape Town

The testing of the modifications proposed for WLANs is beyond the scope of this study. Therefore, the evaluation framework does not incorporate any modifications for active decoy UEs, which are deployed in WLANs. The functions of the mentioned modifications were implemented on the evaluation framework. However, the small scale evaluation framework included only one IMS domain, hence no P-CSCF is implemented. As a result, no modifications for Privacy headers are implemented.

IMS service profile and media authorisation functions were not present on the Iptel SER and was added by further modifications. One of the modifications required the S-CSCF to check if the user has audio transmission rights. For this, a database table called "grp" was added to the HSS, where all users capable of initiating voice calls belong to the group GREEN. The S-CSCF checks to see if the sender belongs to this group before voice transmissions can begin.

A summary of the modifications included in the evaluation framework was presented. Now, test of their performance will be conducted in the later sub sections. The tests involving the functioning of the decoy UE is presented next.

University of Cape Town

5.3.1 Functions of the Decoy UE

The two decoy UEs in the evaluation test bed are set up on one host. Therefore, these decoy UEs emulate the behaviour of virtual decoy UEs. The configuration of the two decoy UEs are presented in table 5.1. It is important that these two decoy UEs utilise different ports for SIP signalling and different ports for media i.e. port for audio transmission.

Table 5.1: Configuration of the two decoy UEs on one host.

Decoy Name	Port	Media Port
joe@sip-router	5051	6045
frank@sip-router	5079	6019

The aim of the tests on the decoy UEs is to prove that the spammer can hit both decoys in this virtual set up, and that the decoys can correctly parse the INVITE message to retrieve the spammer's public user identity. The scenario involves one spammer (dick@sip-router) sending voice spam to all the receivers and the two

decoys. The screen output from the decoy UEs is shown in figure 5.2. The output shows that the decoys can successfully function as virtual decoys on one host, and that the sender's public user identity can indeed be retrieved.

```
decoy joe - serial 1098
parsed ---- dick
dick    sip-router      green   0000-00-00 00:00:00
1 rows returned

          .
          .
          .
decoy frank - serial 2040
parsed ---- dick
dick    sip-router      green   0000-00-00 00:00:00
1 rows returned
dick    sip-router      1098    0000-00-00 00:00:00
1 rows returned
```

Figure 5.2: Output from the decoys when they are hit by a spammer.

5.3.2 Modifications to the HSS

The HSS is modified with a database table called "grp" and a program that blacklists users. The tests aim to prove the correct functionality of the HSS modifications. Firstly, the HSS should be able to enter into the "grp" table public user identities and the decoy serial number. This is done by sending over the secure interface from the decoy to the HSS the public user identity, dick@sip-router and decoy serial, 1098. The resultant entry into the "grp" table is shown in figure 5.3. Furthermore, sending again this same identity and serial number does not cause any additions to the "grp" table.

```
| joan     | sip-router | green | 0000-00-00 00:00:00 |
| ed       | sip-router | green | 0000-00-00 00:00:00 |
| frank    | sip-router | green | 0000-00-00 00:00:00 |
| dick     | sip-router | green | 0000-00-00 00:00:00 |
| tracy    | sip-router | green | 0000-00-00 00:00:00 |
| dick     | sip-router | 1098  | 0000-00-00 00:00:00 |
+----------+------------+-------+---------------------+
```

Figure 5.3: Table "grp" modification when a sender hits only one decoy UE.

Secondly, when the same sender hits a different decoy UE, this decoy sends a

University of Cape Town

different serial number but the same user identity to the HSS. To test this, a different serial number (2040) but the same user identity, dick@sip-router, was sent to the HSS. The correct entries done by the HSS in the "grp" table is shown in figure 5.4. The public user identity, dick@sip-router, no longer belongs to the group GREEN, but to groups 1098 and 2040 corresponding to the decoy serial numbers.

```
| ed       | sip-router | green | 0000-00-00 00:00:00 |
| frank    | sip-router | green | 0000-00-00 00:00:00 |
| tracy    | sip-router | green | 0000-00-00 00:00:00 |
| dick     | sip-router | 1098  | 0000-00-00 00:00:00 |
| dick     | sip-router | 2040  | 0000-00-00 00:00:00 |
+----------+------------+-------+---------------------+
```

Figure 5.4: Table "grp" entries when sender hits two different decoy UEs.

University of Cape Town

5.3.3 Modifications to the S-CSCF

The functionalities to be tested include:

- allowing initiation of calls when the user belongs to group GREEN.
- blocking the user from making calls when the user does not belong to group GREEN.
- re-registration does not allow the user to bypass the ban on making calls.
- message of 403 (no permissions check account) is sent to let the users know that the account is blacklisted.

For the first functionality, the output screen showing the calls made by dick@sip-router who belongs to group GREEN is illustrated in figure 5.5. This proves that a user belonging to group GREEN is allowed to make voice calls.

To test the last three functionalities of the S-CSCF, the user dick is removed from the group GREEN. The SIPp output screen for this user is shown in figure 5.6, and figure 5.7 shows the message exchange as logged from sip-router using ngrep.

```
                                 Messages  Retrans   Timeout   Unexpected-
Msg
    REGISTER ---------->            2         0         0
         401 <----------            2         0                   0
    REGISTER ---------->            2         0
         200 <----------            2         0                   0
      INVITE ---------->            3         0         0
         407 <----------            3         0                   0
      INVITE ---------->            3         0
         100 <----------            3         0                   0
         180 <----------            0         0                   0
         200 <---------- E-RTD      3         0                   0

         ACK ---------->            3         0
               [ NOP ]
       Pause [   8000ms]            3                             0
         BYE ---------->            3         0         0
         407 <----------            3         0                   0
         BYE ---------->            3         0         0
         200 <----------            3         0                   0
```

Figure 5.5: SIPp output showing user making voice calls.

```
                                 Messages  Retrans   Timeout   Unexpected-
Msg
    REGISTER ---------->            8         0         0
         401 <----------            8         0                   0
    REGISTER ---------->            8         0
         200 <----------            8         0                   0
      INVITE ---------->            30        0         0
         407 <----------            30        0                   0
      INVITE ---------->            30        0
         100 <----------            0         0                   30
         180 <----------            0         0                   0
         200 <---------- E-RTD      0         0                   0

         ACK ---------->            0         0
               [ NOP ]
       Pause [   8000ms]            0                             0
         BYE ---------->            0         0         0
         407 <----------            0         0                   0
         BYE ---------->            0         0         0
         200 <----------            0         0                   0
```

Figure 5.6: SIPp output for a banned user trying to make voice calls.

The results shown in the figures 5.6 and 5.7 prove that the S-CSCF can block calls from users not belonging to the group GREEN and sends a 403 message. Further,

University of Cape Town

```
U 10.128.1.39:5080 -> 10.128.0.83:5060
  INVITE sip:joe@sip-router:5060 SIP/2.0..Via: SIP/2.0/UDP
10.128.1.39:5080;b
  ranch=z9hG4bK-49-6..From: ua1 <sip:dick@sip-router:5080>;tag=49..To:
ua2 <s
  ip:joe@sip-router:5060>..Call-ID: 49-5729@10.128.1.39..CSeq: 1
INVITE..Cont
  act: sip:dick@10.128.1.39:5080..Proxy-Authorization: Digest
username="dick@
  sip-router",realm="sip-
router",uri="sip:10.128.0.83:5060",nonce="45b214d8ed

6210f987de3624123e22e699517fa4",response="09c5be73945a6ce9a309f6a744dd75
53"
  ,algorithm=MD5..Max-Forwards: 70..Subject: Performance Test..Content-
Type:
  application/sdp..Content-Length:  188....v=0..o=user1 53655765
2353687637 I
  N IP4 10.128.1.39..s=-..c=IN IP4 10.128.1.39..t=0 0..m=audio 6252
RTP/AVP 8
  ..a=rtpmap:8 PCMA/8000..a=rtpmap:101 telephone-event/8000..a=fmtp:101
0-11,
  16..
#
U 10.128.0.83:5060 -> 10.128.1.39:5080
  SIP/2.0 403 no permissions check account..Via: SIP/2.0/UDP
10.128.1.39:5080
  ;branch=z9hG4bK-49-6..From: ua1 <sip:dick@sip-router:5080>;tag=49..To:
ua2
  <sip:joe@sip-
router:5060>;tag=b27e1a1d33761e85846fc98f5f3a7e58.29a5..Call-I
  D: 49-5729@10.128.1.39..CSeq: 1 INVITE..Server: Sip EXpress router
(0.9.6 (
  i386/linux))..Content-Length: 0..Warning: 392 10.128.0.83:5060 "Noisy
feedb
  ack tells:  pid=5145 req_src_ip=10.128.1.39 req_src_port=5080
in_uri=sip:jo
  e@sip-router:5060 out_uri=sip:joe@10.128.1.252:5051 via_cnt==1"....
```

Figure 5.7: Ngrep output from sip-router letting user know that he/she is banned.

figure 5.6 shows that re-registrations do not allow the banned user to make voice calls.

The tests performed in this part of the thesis prove the correct functioning of the modifications and the feasibility of the decoying system. This test bed is also a small scale prototype of the proposed decoying solution for SPIT. The next parts of the thesis will present tests to verify the performance of the decoying solution

University of Cape Town

under different loads.

5.4 Performance Tests

The thesis aims include proving that the decoying system can operate under different network conditions, adds little overhead to the network, and is robust. To do this performance tests are conducted on the evaluation framework. The different conditions that are tested include a low load scenario, a high load scenario, and a stress test. In these cases, evaluations are done on the detrimental effects of the spammers, and if the presence of a decoying system can improve the network performance. The results obtained are compared to an ideal network where there are no spammers or decoys. The parameters measured are discussed as follows:

- Number of legitimate calls are observed, and these are expected to reduce as the spamming frequency increases. Further, the number of legitimate calls are expected to improve when the decoy UEs are introduced.
- Number of failed calls are expected to increase with spamming frequency, and the decoy UEs should reduce the number of failed calls.
- Response time is the time from sending a SIP message and receiving a corresponding reply. This value is especially sensitive to the load on the S-CSCF.
- Call duration is also affected by the spammers, and the performance tests need to prove that the decoying system can bring an improvement to the network by reducing the call duration in the presence of spammers.
- Cumulative number of packets sent by the spammers gives an indication to the spam messages that are causing overheads on the system. The value should be reduced when decoys are introduced.
- Time that the spammers are blocked and time when two decoys have been hit are recorded. The significance of these values is that if the decoying system causes little overheads, these two times should be equal.

University of Cape Town

- Total number of spam messages and total number of blocked spam messages are observed. These values are noted to calculate the false negatives that the decoying system suffers from. Also, the spamming frequency may affect these values, and thus will be investigated in the tests.

One consideration that has not been mentioned is the duration of the tests to be performed. This is important since the network should be allowed sufficient time to readjust when the decoy UEs have banned the spammers. Therefore, one hour is a reasonable time that should have passed after the spammers have been banned. So considering figure 5.8 that shows the banning of a spammer sending voice spam at 1 call per 30 seconds, a two hour period for the tests is sufficient since the spammer is banned in 29 minutes. This evaluation included a spammer with frequency of 1 call in 30 seconds since in the tests to be performed, this is the lowest frequency of the spammer to be examined, and so is expected to take the longest time to be banned.

University of Cape Town

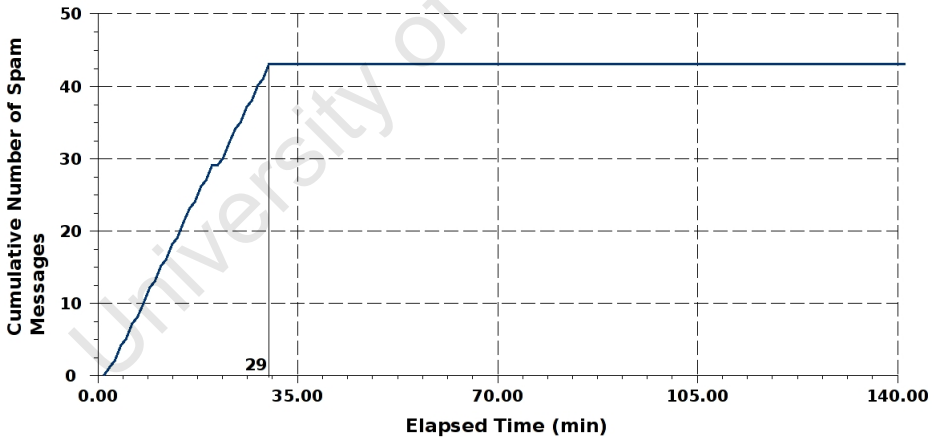


Figure 5.8: Time required to ban a spammer sending voice spam with frequency of 1 call per 30 seconds.

5.4.1 Tests under Low Load

The tests performed in this section used background traffic sent at a frequency of 1 call per 50 seconds. The 8 senders and the two spammers send 8 second voice

messages to the recipients. The configuration of the seven scenarios are presented as follows:

- Scenario 1: Background traffic present with call rate of 1 call per 50 seconds.
- Scenario 2: This includes the same background traffic as scenario 1 but includes two spammers with call rate of 1 call per 30 seconds.
- Scenario 3: This scenario is the same as scenario 2 except that the spammers' call rate is increased to 1 call per 20 seconds.
- Scenario 4: This scenario is the same as scenario 2 except that the spammers' call rate is increased to 1 call per 10 seconds.
- Scenario 5: This scenario is the same as scenario 2 but includes the two decoy UEs.
- Scenario 6: This scenario is the same as scenario 3 but includes the two decoy UEs.
- Scenario 7: This scenario is the same as scenario 4 but includes the two decoy UEs.

The goal of these tests is to evaluate the performace of the decoying system under low load conditions. The detrimental effects caused by the spammers in the network are to be observed, and the improvements experienced by introducing the decoying system are noted. The overheads that may be caused by the introduction of the decoying system are also investigated. Furthermore, the robustness of the proposed solution is tested where spammers with different call rates are included. This is to prove that the decoying solution will not fail when the frequency of spam calls is high.

Number of Legitimate Calls

The results obtained on the total number of legitimate voice calls made by the 8 senders is illustrated in table 5.2. This table shows that during low load, addition of malicious users does not significantly affect the number of legitimate calls being

University of Cape Town

made. This is because the S-CSCF does not have too many packets to process, and any additions can easily be handled. Therefore, with or without the presence of spammers, the total number of legitimate calls remains unchanged. Further, little adverse effects are only observed when the spammer is sending spam at 1 call per 10 seconds. Here, the total number of legitimate calls drops by two, but is not significant enough to be conclusive. Since the spammers have little effect on the network, the presence of decoys hardly brings any improvements. The results show that for scenario 5 and 6 the total number of legitimate calls exceeds that for the ideal case by 1. This can be attributed to when the simulations were stopped, and is not significant.

Table 5.2: Total number of legitimate calls sent by the 8 senders under low load.

Scenario No.	Total Number of Calls
1	986
2	986
3	986
4	984
5	987
6	987
7	985

University of Cape Town

Failed Calls

Table 5.3 shows the number of failed calls for the different scenarios. Since the system is in a low load state, the introduction of the spammers has no detrimental effects to the number of failed calls. Therefore, the introduction of the decoys brings no improvement as well. It should be mentioned that the decoying system does not itself cause any adverse effects to the network performance in terms of failed calls. This would be expected for challenge-response methods, reputation networks, and multi-stage filters whose extra processing requirements are bound to increase the number of failed calls.

Response Times

These response times are averaged for every send and corresponding receive SIP message in the clients, and so are more sensitive to the processing load on the S-

Table 5.3: Total number of failed calls under low load.

Scenario No.	Number of Failed Calls
1	16
2	16
3	16
4	18
5	15
6	16
7	16

CSCF. As shown in table 5.4, the average response times increase as the spamming frequency increases. With the introduction of the decoys, the response times observed are equal to the average response times in the ideal scenario. The results illustrate that the spammers only manage to increase the response times slightly and banning them can revert the response times to the ideal case. The distribution of the response times is shown in table 5.5, this shows the number of calls with average response times within a specific range. The first column shows the number of calls with average response times between 0 and 10ms. Introducing spam voice calls results in less number of calls with average response times from 0 to 10ms and more calls with average response times from 30 to 40ms. The introduction of the decoys does improve the distribution but does not match the ideal scenario.

It is significant to state that the presence of decoys does not cause any increase in response times or cause adverse effects to the distribution of response times, but significantly improves the conditions when compared to the corresponding scenario with no decoys. This shows that the decoying system causes little overheads to the system. Introducing computationally complex methods such as reputation systems or multi-stage filters are bound to have adverse effects on the response times.

Call Duration

Again under low load conditions, introducing the spammers has little effect on the network. The average call duration for the scenarios are illustrated in table 5.6. It shows that an increase in the spamming frequency augments the call duration slightly. It is worth mentioning that the 8 second duration is for the

University of Cape Town

Table 5.4: Average response times under low load.

Scenario No.	Average Response Time (ms)
1	1
2	1.25
3	1.37
4	1.5
5	1
6	1
7	1

Table 5.5: Distribution of response times in milliseconds (ms) under low load.

Scenario No.	0-10	10-20	20-30	30-40
1	959	23	6	
2	948	26	8	1
3	944	35	3	4
4	940	27	8	9
5	956	26	4	
6	958	25	5	1
7	958	24	6	

voice message, and the remaining time is attributed to SIP signalling. The call durations are improved with the presence of decoys. With the exception of the case when the spam voice frequency is 1 call per 10 seconds, the call duration reverted back to the ideal scenario. The decoying system causes no extra delays in call set up, since its presence does not increase the call duration as compared to the corresponding scenario including only the spammers.

Table 5.6: Average call duration under low load.

Scenario No.	Average Call Duration (secs)
1	8.097
2	8.097
3	8.101
4	8.103
5	8.097
6	8.097
7	8.099

University of Cape Town

Blocking Spammers

Statistics on the spam messages obtained from the different scenarios are shown in table 5.7. This table shows that when the spam messages are blocked and not allowed to continue till completion, the spammers are able to generate more spam calls in the allocated time frame as compared to cases where the spam messages are not blocked. This would cause adverse effects to challenge-response methods.

The percentage of spam messages blocked increases with the spam call frequency, and the decoying system seems to be more effective for higher spam call frequencies. However, the number of false negatives or the spam calls allowed through are similar for different spam message frequencies. This is due to the fact that both decoys are hit after a certain number of messages and not after a specified time. As illustrated in table 5.7 and figure 5.9, the decoying system initially allows a certain number of spam calls before they are blocked. It should be noted that all other SPIT blocking methods, with the exception of challenge-response methods, require a learning time before spam calls are eventually blocked. Figure 5.9 illustrates that the decoying system is robust and can effectively block voice spam at high spam voice call frequencies.

University of Cape Town

Table 5.7: Statistics on spam messages under low load.

Scenario No.	Total No. of Spam Messages	No. of Spam Messages Blocked	False Negatives	% of Spam Blocked
2	394	0	-	0
3	448	0	-	0
4	1226	0	-	0
5	452	365	87	81
6	678	594	84	88
7	1434	1348	86	94

Table 5.8: Delays in blocking spammers under low load conditions.

Scenario No.	Time Both Decoys have been Hit	Time Spammers are Blocked
5	29 mins	29 mins
6	22 mins	22 mins
7	8 mins	8 mins

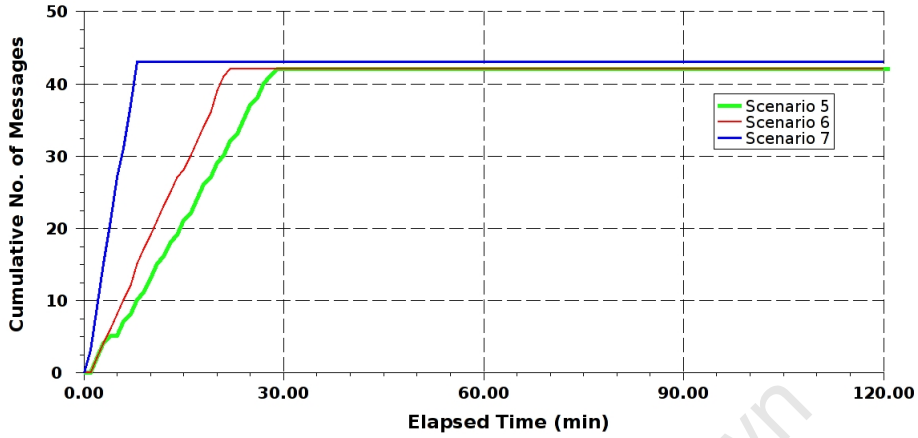


Figure 5.9: Performance of decoys in blocking spammers under low load conditions.

University of Cape Town

Figure 5.10: Messages received by the two decoys in scenario 7.

Figure 5.9 shows that the decoys are capable of blocking spam voice calls independent of their frequency. Furthermore, figure 5.10 and table 5.8 show that there are no delays in blocking a spammer when both decoys have been hit. This result can be used to conclude that the decoying algorithm is simple, with little overheads on the HSS and S-CSCF. However, since the system is under low load, it can be argued that even a complex algorithm may not cause any delays in blocking the spammer. So the next consideration will include the system under high load.

5.4.2 Tests under High Load

The last subsection dealt with the performance of the decoying system under low load. This subsection will present the performance of the decoying system during high load conditions. A SPIT blocking solution should be effective even under conditions when the load on the core entities is high. The tests involve the background senders sending an 8 second voice call with frequency of 1 call per 10 seconds. Any higher frequency is not possible since the 8 second message makes it impractical to have a frequency greater than this. The various scenarios tested are outlined as follows:

- Scenario 1: The ideal case where there are only the background traffic clients with no spammers or decoys.
- Scenario 2: This is the same as scenario 1 but with two spammers sending voice spam at 1 call per 20 seconds.
- Scenario 3: This is the same as scenario 2 except that now the spammers are sending at 1 call per 10 seconds.
- Scenario 4: This is the same as scenario 2 but includes the two decoy UEs.
- Scenario 5: This is the same as scenario 3 but includes the two decoy UEs.

The aims of the test is to note if the decoying system will fail under high load conditions, whether there will be any delays in blocking the spammers, and what improvements does the presence of decoys bring to the network if at all.

University of Cape Town

Number of Legitimate Calls

During high load, addition of spammers significantly reduces the number of legitimate calls, which reduces as the frequency of spam voice calls increase. This is shown in table 5.9. Introducing decoys seems to improve the situation, yet the number of legitimate calls is still less than the ideal case. It can be observed that in high load conditions, the presence of decoys can increase the number of legitimate calls as compared to the corresponding scenario with the two spammers. As compared to low load scenarios, the decoys are more effective in high load scenarios for improving the number of legitimate calls.

Table 5.9: Total number of legitimate calls sent by the 8 senders under high load.

Scenario No.	Total No. of Calls
1	5728
2	5709
3	5665
4	5718
5	5698

Failed Calls

Under high load conditions introducing the spammers results in a greater number of failed calls. Also, as the frequency of spam calls increases so does the number of failed calls. These results can be observed from table 5.10. Introduction of the decoys improves the network performance but still does not result in performance similar to the ideal case. This is due to the fact that the decoying system initially allows a number of voice spam to pass through. The performance during this initial period affects the number of failed calls for scenarios 4 and 5, which will not equal the number of failed calls in the ideal case.

As can be observed from table 5.10, presence of the decoys can improve the performance when compared to the corresponding scenarios with spammers. Moreover, the banning of spammers has a greater effect under high load conditions. Hence, it can be concluded that the decoying system is more suitable for high load conditions than for low load conditions.

Table 5.10: Total number of failed calls under high load.

Scenario No.	Number of Failed Calls
1	32
2	49
3	66
4	38
5	43

Response Times

As already mentioned, the response times are an indication of the processing load on the S-CSCF. The average response times recorded for the scenarios under high

University of Cape Town

load are shown in table 5.11. This shows that including the spammers increases the average response times, and so the S-CSCF incurs overheads in processing these spam messages. The response times increase with an increase in the call frequency of the spammers. It is important to state that the real time nature of voice calls means that even a 10 ms increase in the response time is noticeable to the end users. However, introducing the decoys does reduce the response times because after a while the spammers are blocked. The decoying system does not introduce any extra processing on the S-CSCF that increase the response times when compared to the corresponding scenario with spammers.

Table 5.11: Average response times under high load.

Scenario No.	Average Response Times (ms)
1	36
2	46
3	66
4	38
5	43

University of Cape Town

It can be observed from table 5.12 that the spammers increase the network response times under high load conditions. There are response times that are greater than 200ms with the introduction of the spammers. The spammers reduce the number of calls with average response times less than 10ms. Including decoys in the network ensures that no call has average response times greater than 200ms. Also, comparing scenarios 2 and 3 where spammers are present to scenarios 4 and 5 with both spammers and decoys, there is a significant improvement in the distribution of response times. Furthermore, scenarios 4 and 5 have a larger number of calls with average response times less than 10 ms as compared to scenarios 2 and 3.

Table 5.12: Distribution of response times in milliseconds (ms) under high load.

Scenario No.	0-10	10-20	20-30	30-40	40-50	200+
1	5575	118	34	3		
2	5546	114	45	8		15
3	5475	174	50	14	7	13
4	5561	120	30	8		
5	5520	164	40	15		

Call Duration

As shown in table 5.13, the average call duration is the lowest in the ideal network. Including the spammers increases the average call duration. An increase in the frequency of spam calls increases the average call duration. On the other hand, including the decoy UEs improves the call duration even in the presence of spammers. It is interesting to note that the average call duration for scenario 5 is less than for scenario 4, although the spam call frequency is greater for scenario 5. This can be justified by noting that for scenario 5, the spammers are blocked quicker than in scenario 4. As was the case for the low load scenarios, the decoying system does not affect call set up procedures. This is shown in table 5.13 where average call duration of scenarios 4 and 5 is less than those for scenarios 2 and 3.

Table 5.13: Average call duration under high load.

Scenario No.	Average Call Duration (secs)
1	8.165
2	8.172
3	8.175
4	8.169
5	8.166

University of Cape Town

Blocking Spammers

The statistics collected on the spam messages is shown in table 5.14. This is similar to the results obtained under low load conditions. Figure 5.11 shows that even under high load conditions, the decoying system can block spammers irrespective of their call frequency. This proves the robustness of the system. Further, table 5.15 shows that there are no delays in blocking spammers. So it is now more conclusive to say that the decoying system causes little overheads. Although the S-CSCF is processing a large number of messages, it is still able to block spammers without any noticeable delay. However, this study will take the performance test even further, and the evaluations of the decoying system under extreme load is presented in the next part of the dissertation.

Table 5.14: Statistics on spam messages under high load.

Scenario No.	Total No. of Spam Messages	No. of Spam Messages Blocked	False Negatives	% of Spam Blocked
2	448	0	-	0
3	1226	0	-	0
4	680	594	86	87
5	1438	1352	86	94

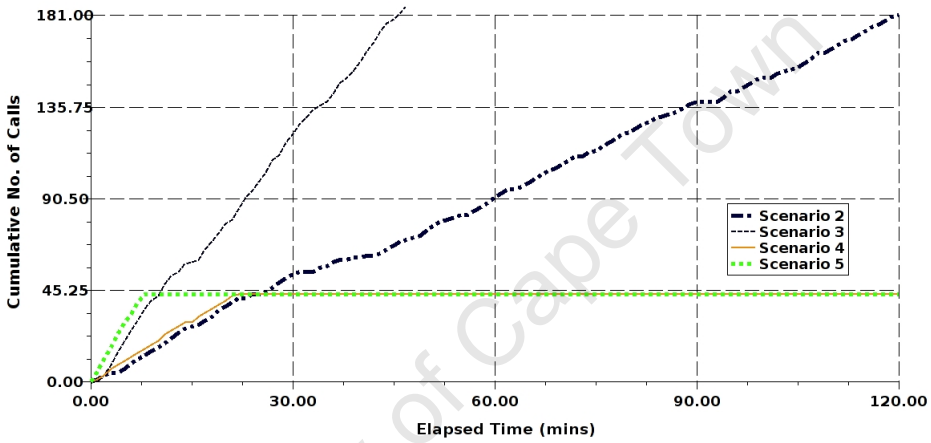


Figure 5.11: Performance of decoys under high load conditions.

Table 5.15: Delays in blocking spammers under high load conditions.

Scenario No.	Time Both Decoys have been Hit	Time Spammers are Blocked
4	22 mins	22 mins
5	8 mins	8 mins

5.4.3 Stress Test

This test includes the 8 senders sending SIP messages at 1 call per second. Due to the high call rate the 8 second voice message is left out. The stress test is performed to further prove the robustness of the decoying system. Additionally, the stress test can prove that the decoying system causes little overheads. The configuration of the scenarios are as follows:

University of Cape Town

- Scenario 1: The ideal with only background traffic generators.
- Scenario 2: This scenario includes the background traffic generators and the spammers. These two spammers are sending SIP messages at a rate of 2 calls per second.
- Scenario 3: This scenario is the same as scenario 2 but includes the two decoy UEs.

In the IMS, once a session has been established the media may not flow through the proxy. For the test bed, therefore the 8 second voice message does not cause any processing on the S-CSCF. This voice message has been left out for the stress test and all the SIP messages in the scenarios have to be handled by the S-CSCF. Hence, the load on the S-CSCF is tremendous, considering the extremely high call rates as well.

Number of Legitimate Calls

Introducing the two spammers reduced the number of legitimate calls. The decoys however banned the spammers very quickly and so the number of failed calls for scenario 3 is much lower than that for scenario 2. The results of the number of legitimate calls is illustrated in table 5.16.

Table 5.16: Total number of legitimate calls sent by the 8 senders during the stress test.

Scenario No.	No. of Legitimate Calls
1	57296
2	57180
3	57280

Failed Calls

The failed calls increases when the spammers are present in scenario 2. But, the decoys managed to improve the situation and the number of failed calls in scenario 3 is less than that for scenario 2. The results obtained are shown in table 5.17.

University of Cape Town

Table 5.17: Total number of failed calls during the stress test.

Scenario No.	Number of Failed Calls
1	380
2	507
3	409

Response Times

Considering the high rates of the spammers, the processing load on the S-CSCF is increased considerably from scenario 1, and so the response times for scenario 2 is larger than scenario 1. As shown in table 5.23, the spammers are blocked in less than a minute in scenario 3. Hence, the presence of decoys can revert the response times to the values obtained in scenario 1. This is shown in table 5.18. Scenario 2 includes several calls with response times greater than 200ms as shown in table 5.20, and less number of calls with response times less than 10ms when compared to scenario 1, as shown in table 5.19. The decoys in scenario 3 result in more calls with response times less than 10ms as compared to scenario 2, and for scenario 3 no calls have response times greater than 200ms (similar to the ideal case).

University of Cape Town

Table 5.18: Average response times during the stress test.

Scenario No.	Average Response Times (ms)
1	5
2	8
3	5

Table 5.19: Distribution of response times from 0 to 50 ms during the stress test.

Scenario No.	0-10	10-20	20-30	30-40	40-50
1	54888	1744	400		
2	54448	2064	448	24	16
3	55064	1592	256	152	24

Table 5.20: Distribution of response times, 50 ms and above, during the stress test.

Scenario No.	50-100	100-150	150-200	200+
1	76			
2				56
3	16	60		

Call Duration

Table 5.21 illustrate that the call duration remains the same even in scenario 2. The reason for this is that since the calls take such a short time, the probability of clashes of calls being sent to the same receiver is reduced even in the case with spammers. Consider, the high load case with 1 call per 10 second and the call duration approximately 8 seconds, in the 10 second period only 1 call can be placed to a single receiver. And considering the low load case with 1 call per 50 seconds and call duration approximately 8 seconds, in the 50 second period only 6 ($\frac{50}{8}$) calls can be placed to a single receiver. But considering the stress test, a single receiver can receive 38 calls ($\frac{1000ms}{26ms}$) in the 1 second period.

Table 5.21: Average call duration during the stress test.

Scenario No.	Average Call Duration (ms)
1	26
2	26
3	26

University of Cape Town

Blocking Spammers

Even under extreme load the decoying system is able to block the spammers as shown in figure 5.12. This proves the robustness of the system. Further, table 5.22 shows that the magnitude of the false negatives is similar for the low load and high load cases. The decoying system blocks a larger amount of calls when the frequency of spam calls is higher. Table 5.23 shows that there are little delays in blocking the spammer. As deduced from figure 5.12, the decoys allow 45 spam messages through. For the low and the high load cases, a spammer is blocked after sending approximately 43 messages. Therefore, an estimate of the delay in

blocking the spammer is about 1 second, given that in the stress test, 2 more spam messages pass through as compared to the other situations and that the frequency of spam calls is 2 calls per second. This is based on the assumption that both decoys are hit on the 43rd spam message in the stress test.

Table 5.22: Statistics on spam messages for the stress test.

Scenario No.	Total No. of Spam Messages	No. of Spam Messages Blocked	False Negatives	% of Spam Blocked
2	13478	0	-	0
3	28742	28652	90	99.7

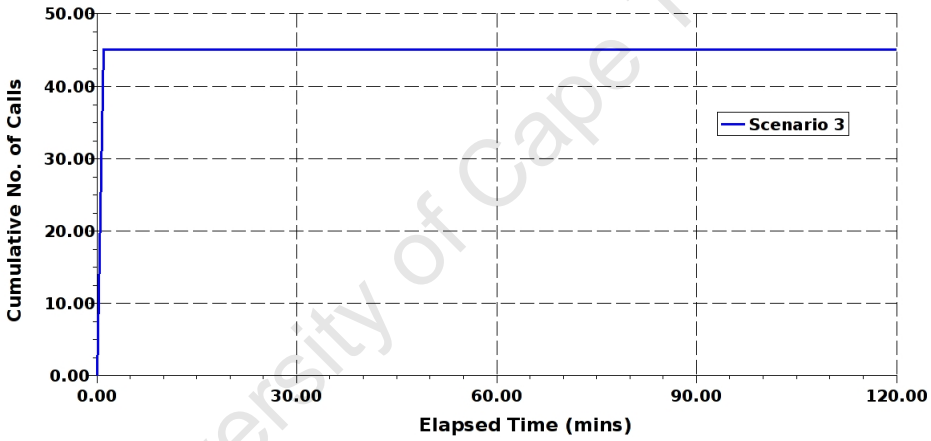


Figure 5.12: Operation of decoys during the stress test.

University of Cape Town

Table 5.23: Delays in blocking spammers for the stress test.

Scenario No.	Time Both Decoys have been Hit	Time Spammers are Blocked
3	<1 min	< 1min

5.5 Chapter Discussion

In this chapter, several experiments were performed on the evaluation framework that demonstrate the adverse effects of spam on voice services in the IMS. How-

ever, it was also shown that the decoying system can successfully block these spammers and improve network conditions. These spammers collect addresses from websites that include the addresses of decoy UEs. So when the spammer hits two different decoy UEs, this spammer is blacklisted and prevented from making any further voice calls.

In the first set of experiments performed under low load conditions, the adverse effects caused by the spammers are minimal. However, the decoying system still reduced these adverse effects. Moreover, there are no delays in blacklisting the spammers so the decoying system causes little overheads to the system. The decoying system was also capable of blocking spammers, even those sending voice calls at a high frequency.

In the second set of experiments under high load conditions, the spammers caused considerable detrimental effects to the network. But, the presence of decoys improved network conditions significantly without causing any additional call set up delays. Furthermore, even under high load conditions, there were no delays in blacklisting spammers, and the decoying system successfully blacklisted spammers with high spam call rates.

The third set of experiments involved a stress test. Even under such conditions, the decoying system blocked the spammer proving that the decoying system causes little overheads. Further, it was deduced that the blacklisting operation only took 1 second. The next chapter will present the conclusions and the future work for this research.

University of Cape Town

Chapter 6

Conclusions and Recommendations

University of Cape Town

6.1 Conclusions

This research has investigated the profitability of SPIT and the various methods with which SPIT can be blocked in the IMS. Several of these methods have been analysed in terms of performance and overheads they can cause in a VoIP network. Moreover, this thesis proposes a novel decoying solution to block SPIT that overcomes some of the shortcomings of other SPIT blocking solutions.

The decoying solution proposes that addresses of decoy UEs deployed on several IMS access networks be posted on websites and news groups. These addresses are harvested by SPIT senders using automated programs. When the spammers hit two different decoy UEs, their IMS accounts are blacklisted, and they are prevented form making further voice calls. For proof of concept of this SPIT blocking solution, an evaluation framework was implemented. Analysis of previously proposed SPIT filtering techniques was presented to show that these techniques introduced large overheads to the network, and some are not suitable for a network during periods of high traffic.

The evaluation framework was implemented using the Iptel SER to emulate an IMS S-CSCF and SIPp to emulate the IMS clients. This evaluation framework included two spammers and several clients to emulate background traffic. The

performance of the decoying system was investigated using this evaluation under different network conditions. The following conclusions are made from the findings and analysis presented in the previous chapters:

- The problem of email spam persists in todays networks with a large proportion of email messages being spam. SPIT is a new problem that has just surfaced for VoIP networks. The profitability of email spam can be attributed to two factors of time and cost. With the introduction of the IMS, VoIP will be more popular since it will be cheaper and support more features than traditional PSTN services. Both the factor of time and cost are present for sending unsolicited calls in the IMS. Therefore, SPIT will be profitable in the IMS and will become as large a problem as email spam in the future.

- Solutions to blocking SPIT have been proposed in literature, however they cause overheads affecting network performance. Further, IMS call set up is already cumbersome, and call set up delays can be large especially for international calls. Solutions to block SPIT such as challenge-response mechanisms, reputation systems, and multi-stage filters introduce extra processing for call set up causing even greater delays. These three solutions are also not suitable for a network under high load conditions. Progressive Multi Grey-Levelling (PMG) does not, however, stop the spam calls completely and fails if the spammer implements on and off periods for sending spam.

- The IMS authentication involves an ISIM module containing a shared key which can only be accessed using a PIN. Therefore, to steal another user's identity, one requires both the PIN and the hardware containing the ISIM module. This makes identity theft in the IMS very difficult.

- To prevent a user from making further voice calls, the audio media authorisation can be removed from the core network service authorisation. The evaluation framework successfully emulated this behaviour where users not belonging to the group GREEN were not allowed to make voice calls.

- The proposed decoying solution can be deployed on an IMS framework with additions to the IMS interface. An interface from decoy UE to the spammer's

University of Cape Town

HSS is required. The other additions include adding databases and programs to the HSS, S-CSCFs, and the P-CSCFs. The feasibility of the decoying solution was demonstrated using the evaluation framework.

- The evaluation framework demonstrated the adverse effects of spam under different network conditions. A greater effect on call duration, distribution of response times, and failed calls were observed during periods of high than low load conditions.

- The decoying solution is capable of blocking spammers in both low load and high load conditions. This was demonstrated using the test bed. Furthermore, improvements to network performance was brought about by the introduction of the proposed decoying system. These improvements included reducing the call duration, response times, and number of failed calls in the presence of spammers. Further, the decoying system does not cause any extra delays in call set up.

- The decoying system managed to block spammers with an estimated 1 second delay under extreme network loads. This was demonstrated by the stress test conducted on the evaluation framework. Therefore, the decoying solution being a simple algorithm causes very little overheads to the IMS core entities.

- As demonstrated by experiments conducted on the evaluation framework, the rate of spam calls does not affect the operation of the decoying system. The higher the spam call rate, the quicker the spammers are banned. Therefore, the decoying system is very robust.

- There is an initial period of time that the decoying system allows spam messages to pass through before the spammers are blacklisted. This is demonstrated by the operation of the test bed and is a downside of the proposed solution.

6.2 Contributions Made

This research has made the following contributions to SPIT research for the IMS:

University of Cape Town

- This dissertation has proposed a novel solution to block SPIT in the IMS. Although, spam trap email addresses have been used by email service providers, they have not been very effective in battling email spam. This is because there is no strong authentication mechanisms present for email. However, the IMS has a strong authentication system making identity spoofing very difficult. Therefore, the decoying system implemented in an IMS network is effective in blocking SPIT. The implementation of the decoying system on the IMS was presented in the thesis, and the modifications required were highlighted.

- Secondly, this dissertation proved that previous SPIT blocking solutions caused higher overheads on the network than the proposed decoying system. Furthermore, the latter is robust and capable of blocking SPIT even under high loads. Also, the decoying solution manages to block spammers irrespective of their rate of spam calls.

- Thirdly, this dissertation presented an evaluation framework that was used for proof of concept of the decoying solution. The behaviour of the SPIT sender in this evaluation framework can be used for future research on filtering SPIT. And, this evaluation framework can be used for gauging the performance of SPIT filtering solutions in the presence of background traffic.

University of Cape Town

6.3 Future Work and Recommendations

A number of issues were raised in this research regarding the decoying system and the evaluation framework. These issues are presented for consideration for future research in the field of blocking SPIT for the IMS.

- The evaluation framework in this research included only one IMS domain. Future research involving the investigation of the performance of the decoying solution for several domains can demonstrate the behaviour of the decoying solution for large networks.

- This research did not deal with determining the optimum number of decoy UEs that are hit before a spammer is banned. Future research to determine this value can improve the decoying solution significantly.

- For WLANs, active decoy UEs were introduced. This research proposes two types of decoy UEs: active and passive decoys UEs. Passive decoy UEs do not send any voice messages. On the other hand, active decoy UEs, present in WLANs, send voice messages to other decoy UEs in their access network. Spammers eavesdrop on these messages and retrieve the addresses of the decoy UEs. Therefore, these spammers will hit the decoy UEs and as a result will be prevented from making further voice calls. This research did not propose a call scheduling algorithm for these active decoy UEs. Further research needs to be conducted to block spammers exploiting WLANs.

- The refresh time for the database containing users who have hit only one decoy was assumed to be 24 hours. Further work to determine an optimum refresh time for this database is required to improve the decoying solution.

- One way that the identity of decoy UEs can be discovered by the spammers include examining the last recipient before the spammer is blacklisted. To stop this, a random back off period before a user is banned can be added to the decoying system. Further research to investigate this shortcoming and the solution proposed can be conducted in the future.

- Reputation networks propose calculating the reputation of the sender when a call is received. However, for real time voice calls this can introduce severe delays. A proposal to calculate trust of users beforehand would improve this situation. In the IMS, users can upload their contact lists with reputation ratings on an AS. Crawlers from these ASs can search reputation ratings of their users on other similar ASs in different domains. An average value is calculated which is referred to during call set up. The crawlers update these reputation values continuously. This scheme ensures that the reputation of the sender is calculated before a call is initiated, thus removing the delay caused by reputation calculation during call set up. Further research on this scheme is needed to prove its feasibility.

University of Cape Town

Bibliography

[1] A. M. Odlyzko, "Internet traffic growth: sources and implications," *Proceedings- SPIE The International Society for Optical Engineering*, vol. 5247, pp. 1–15, 2003.

[2] L. F. Cranor, "Internet privacy," *Communications of the ACM*, vol. 42, pp. 28–38, 1999.

[3] S. Goodman, L. Press, S. Ruth, and A. Rutkowski, "The Global Diffusion of the Internet: Patterns and Problems," *Communications of the ACM*, vol. 37, pp. 27–31, 1994.

[4] WAP-Forum, "WAP Architecture Version 30-Apr-1998," April 1998.

[5] T. A. Longstaff, J. T. Ellis, S. V. Hernan, H. F. Lipson, , R. D. McMillan, L. H. Pesante, and D. Simmel, "Security of the Internet," *The Froehlich/Kent Encyclopedia of Telecommunications*, vol. 15, pp. 231–255, 1997.

[6] The Radicati Group, "Taming the growth of email: An ROI analysis," The Radicati Group, Inc., Tech. Rep., 2003.

[7] M. Sunner, "Email security best practice," *Network Security*, vol. 2005, pp. 4–7, 2005.

[8] H. M. Butler, "Spam-the meat of the problem," *Computer Law & Security Report*, vol. 19, pp. 388–391, 2003.

[9] G. A. Grimes, M. G. Hough, and M. L. Signorella, "Email end users and spam: relations of gender and age group to attitudes and actions," *Computers in Human Behavior*, vol. 23, pp. 318–332, 2007.

University of Cape Town

[10] skype, "Skype Hits One Million SkypeOut Users," March 2005. [Online]. Available: http://about.skype.com/2005/03/skype_hits_one_million_skypeou.html

[11] M. Vagliasindi, I. Guney, and C. Taubman, "Fixed and mobile competition in transition economies," in *Telecommunications Policy*, ser. 7, vol. 30, 2006, pp. 349–367.

[12] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler, "SIP: Session Initiation Protocol," *IETF RFC 3261*, June 2002.

[13] N. Frost, "VoIP threats - getting louder," *Network Security*, pp. 16–18, March 2006.

[14] 3GPP, "IP Multimedia Susbsystem: Stage 2," *TS 23.228 v7.5.0*, September 2006.

[15] *CAN-SPAM Act of 2003 (S.877)*, U.S. Senate and House of Representatives, 2004.

[16] S. Quo, "Spam: Private and Legislative Responses to Unsolicited Electronic Mail in Australia and the United States," *Murdoch University Electronic Journal of Law*, vol. 11, no. 1, March 2004.

[17] B. Teitelbaum, "Sip Spam: the Coming Storm," *First SIP.edu Implementors Workshop*, 2004.

[18] D. Shin and C. Shim, "Voice Spam Control with Gray Levelling," *1st Workshop on Securing Voice over IP*, December 2004.

[19] A. Madhosingh, "The Design of a Differentiated Session Initiation Protocol to Control VoIP Spam," Master's thesis, Florida State University, 2006.

[20] Y. Rebahi and D. Sisalem, "SIP Service Providers and the spam problem," *1st VoIP Security Workshop*, December 2005.

[21] R. Dantu and P. Kolan, "Detecting Spam in VoIP Networks," *Globecom*, December 2004.

University of Cape Town

[22] D. Waiting and N. Ventura, "Detection of Unsolicited Voice Calls in the IP Multimedia Subsystem," *SATNAC*, September 2006.

[23] X. Jiang, D. Xu, and Y. Wang, "Collapsar: A VM-based honeyfarm and reverse honeyfarm architecture for network attack capture and detention," *Journal of Parallel and Distributed Computing*, vol. 66, pp. 1165–1180, September 2006.

[24] S. Khattab, R. Melhem, D. Mosse, and T. Znati, "Honeypot back-propagation for mitigating spoofing distributed Denial-of-Service attacks," *Journal of Parallel and Distributed Computing*, vol. 66, pp. 1152–1164, September 2006.

[25] P. Calhoun, J. Loughney, E. Guttman, G. Zorn, and J. Arkko, "Diameter Base Protocol," *IETF RFC 3588*, September 2003.

[26] .3GPP, "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); 3G security; Access security for IP-based services," *TS 33.203 version 6.10.0 Release 6*, September 2006.

[27] 3GPP, "Universal Mobile Telecommunications System (UMTS); 3G security; Security architecture," *TS 33.102 version 7.0.0 Release 7*, December 2005.

[28] M. Poikselka, G. Mayer, H. Khartabil, and A. Niemi, *The IMS IP Multimedia Concepts and Services in the Mobile Domain.* John Wiley & Sons, Ltd, 2004.

[29] V. Niemi, "Trends in mobile security standards," *Information Security Technical Report*, December 2004.

[30] C. Guo, H. Wang, and W. Zhu, "Smart-Phone Attacks and Defenses," *Hotenets-III*, November 2004.

[31] P. Mockapetris, "Domain Names - Implementation and Specification," *RFC 1035*, November 1987.

[32] A. Kist and R. Harris, " SIP Signalling Delay in 3GPP," *Sixth International Symposium on Communications Interworking of IFIP-Interworking*, pp. 13–16, 2002.

[33] Barracuda Networks, "An Overview of Spam Blocking Techniques."

University of Cape Town

[34] AOL Postmaster, "Whitelist Information," 2006. [Online]. Available: http://postmaster.aol.com/whitelist/

[35] G. Talavan, "A simple, configurable SMTP anti-spam filter: Greylists," *Computers & Security*, vol. 25, pp. 229–236, May 2006.

[36] I. Androutsopoulos, J. Koutsias, K. V. Chandrinos, G. Paliouras, and C. D. Spyropoulos, "An Evaluation of Naive Bayesian Anti-Spam Filtering," *11th European Conference on Machine Learning*, pp. 9–17, 2000.

[37] F. D. Garcia, J.-H. Hoepman, and J. van Nieuwenhuizen, "Spam Filter Analysis," *19th IFIP International Information Security Conference, WCC2004-SEC*, August 2004.

[38] I. Clarke, T. B. Flaherty, and M. T. Zugelder, "The CAN-SPAM Act: New rules for sending commercial e-mail messages and implications for the sales force," *Industrial Marketing Management*, vol. 34, pp. 399–405, May 2005.

[39] Y. Lee, "The CAN-SPAM Act: a silver bullet solution?" *Communications of the ACM*, vol. 48, pp. 131–132, June 2005.

[40] A. Cournane and R. Hunt, "An analysis of the tools used for the generation and prevention of spam," *Computers & Securit*, vol. 23, pp. 154–166, 2004.

[41] H. Reading, "The Future of VOIP: A Heavy Reading Service Provider Survey," September 2005.

[42] Center for Democracy & Technology, "Why Am I Getting All This Spam?" March 2003.

[43] D. Forte, "Part I: Deploying Honeypots: Project background and implications," *Network Security*, vol. 2003, pp. 13–14, July 2003.

[44] .D. Forte, "Part II: Honeypots in Detail: the Variations," *Network Security*, vol. 2003, pp. 14–15, July 2003.

[45] H. Artail, H. Safab, M. Sraja, I. Kuwatlya, and Z. Al-Masri, "A hybrid honeypot framework for improving intrusion detection systems in protecting organizational networks," *Computers & Security*, vol. 25, pp. 274–288, June 2006.

University of Cape Town

[46] N. Provos, "A Virtual Honeypot Framework," *13th USENIX Security Symposium*, pp. 1–14, 2004.

[47] 3GPP, "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); 3G security; Network Domain Security (NDS); IP network layer security," *TS 33.210 version 7.2.0 Release 7*, December 2006.

[48] .3GPP, "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Cx and Dx interfaces based on the Diameter protocol; Protocol details," *TS 29.229 version 7.3.0 Release 7*, September 2006.

[49] 3GPP, "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); IP Multimedia (IM) Subsystem Cx and Dx Interfaces; Signalling flows and message," *TS 29.228 version 7.3.0 Release 7*, September 2006.

[50] 3GPP, "Group Services and System Aspects; Service aspects; Service principles," *TS 22.101*, December 2006.

[51] R. Housley and W. Arbaugh, "Security problems in 802.11-based networks," *Communications of the ACM*, vol. 46, pp. 31–34, May 2003.

[52] HP Invent, "SIPp." [Online]. Available: http://sipp.sourceforge.net/

[53] Digium, "Asterix." [Online]. Available: http://www.asterix.org

[54] Iptel.org, "SIP Express Router." [Online]. Available: http://www.iptel.org/ser

[55] sipsak, "sipsak." [Online]. Available: http://www.sipsak.org

[56] Antisip, "eXosip2." [Online]. Available: http://www.antisip.com/documentation/eXosip2/

[57] J. Franks, P. Hallam-Baker, J. Hostetler, S. Lawrence, P. Leach, A. Luotonen, and L. Stewart, "HTTP Authentication: Basic and Digest Access Authentication," *RFC 2671*, June 1999.

University of Cape Town

[58] J. Golbeck and J. Hendler, "Reputation Network Analysis for Email Filtering," *First Conference on Email and Anti-Spam*, 2004.

[59] 3GPP, "Internet Protocol (IP) multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3," *TS 24.229*, January 2005.

University of Cape Town

Appendix A

Details on the IMS

University of Cape Town

This appendix presents information on the IMS components and interfaces. Moreover, properties of the different IMS user identities is discussed. The next section will present the design philosophy of the IMS.

A.1 IMS Design Requirements

The IMS is designed on a philosophy of open and standardised interfaces allowing fast service creation and deployment. The several requirements that the standardising bodies adhered to in designing IMS are as follows [28]:

- **IP Connectivity:** All IMS related services can be delivered to IP based packetised networks, and IMS includes gateways for interworking with circuit-switched networks. A user equipment requires an IP address obtained either from the visited or the home network to access any subscribed IMS service. A further requirement states that the UE can have access to all IMS services even when connected to an IP network not supporting IMS. This is possible by allocating an IP address to this UE from the home network. However, an issue of routing efficiency arises due to this system when considering international roaming. In such a case, no real time IMS service can be supported [28].
- **Access Independence:** IMS services should be able to be delivered to any IP based access network be it WLAN, GPRS, Ethernet LANs, satellite

networks etc. Also, the access network should be independent from the IMS services available.

- **Provide Quality of Service (QoS) for Multimedia:** Unlike the best effort Internet, the IMS in collaboration with the access network provides end to end QoS. The UE negotiates QoS parameters using SIP. These parameters normally consist of media type, bit rate, packet size, bandwidth adaptation, and usage of RTP payload. This research is not concerned with the details of QoS for multimedia transmissions and so details on IMS QoS methods will not be provided.

- **Policy Control for Media Resources:** Policy control is not a fundamental element in this research, hence only a summary of this function is provided. Policy control is required to authorise network resources for IMS media. This is done by interaction between the IMS and access network components.

- **Security:** A fundamental requirement of the IMS is that users have to be authenticated before they have access to any IMS related services. And, privacy levels can be selected by the users in using these services.

- **Charging:** IMS is flexible in terms of charging, allowing different charging methods to be used. Different charging methods can be applied for the different services or by the different network operators.

- **Mobility:** The geographic location of the user should be independent from access to IMS services, allowing UEs to access IMS services from any location.

- **Interworking with other Networks:** Any new networking architecture will not be adopted instantaneously by all network providers, therefore IMS must be able to interwork with non-IMS networks and legacy networks.

- **Service Control Model:** The IMS uses home service control. This means that the user subscriber profiles together with the service platforms are always located at the user's home network.

University of Cape Town

- **Service Development:** The IMS was designed to allow fast creation and integration of services. Standardising of services has been dropped by the 3GPP who are now standardising only the service capabilities. As a result IMS has capabilities supporting basic voice, data, multimedia, file sharing, and gaming.

- **Layered Design:** Session signalling and management are separated from the access network and bearer services in the IMS. Also, the services layer is above the signalling layer. The aim was to incorporate minimum dependency between the layers. This layered approach is advantageous, allowing addition of access networks, and the same services to be available on different access networks.

University of Cape Town

A.2 IMS Components

IMS entities are divided into six categories: session management and routing family, databases, interworking elements, application servers, support entities, and charging entities. Figure A.1 illustrates the session management components, database components and the application servers. This study is concerned with session management entities so as to able to understand voice calls in the IMS. Moreover, subscription details are involved with database families and hence is significant to the research. It should be highlighted that the research although not concerned with interworking elements, needs the SPIT blocking solution to be access network independent. Additionally, any support entities that deal with Authentication, Authorisation, and Accounting (AAA) are discussed in detail since the SPIT blocking solution aims to utilise these functions.

Description of the IMS entities are outlined as follows:

Proxy - Call Session Control Function (P-CSCF): The P-CSCF is the first point of contact for the User Equipment (UE) into the IMS framework. REGISTER requests from the UE is forwarded to the I-CSCF (Interrogating - Call Session Control Function) by the P-CSCF. In addition, all other SIP requests from the UE are forwarded to the S-CSCF (Serving - Call Session Control Function). Moreover, security associations of the SIP signalling from the UE is maintained

by this component. All SIP messages from and to the UE pass through the P-CSCF which must either compress or decompress these messages. The P-CSCF also takes account of charging related parameters and ensures authorisation of resources. For detailed information on the functions of the P-CSCF refer to 3GPP specifications TS 24.229 [59].

Interrogating- Call Session Control Function (I-CSCF): This is the entry point to all connections to a subscriber of a specific operator's network. This entity retrieves information from the HSS (Home Subscriber Server) to locate the correct S-CSCF. The I-CSCF forwards all SIP signalling to the S-CSCF. Another function of this entity is to perform topology hiding.

Serving - Call Session Control Function (S-CSCF): This entity is located in the home network and registers UEs. Multiple S-CSCFs may be present in an operator's network. Further, the S-CSCF maintains the state of all sessions of the UE, exchanges charging information with other IMS entities, and decides if a request needs to be routed to a Application Server (AS). The S-CSCF is the entity that authenticates users and downloads user profiles from the HSS. The S-CSCF enforces these service profiles and performs media authorisation for users i.e. checks the SIP messages to ensure that the codecs and media types are of the type allowed for a specific user. The S-CSCF also routes messages to the P-CSCF or the I-CSCF and can perform a network initiated de-registration.

Home Subscriber Server (HSS): The HSS is a database storing user service profiles. The data stored include user identities, registration information, access parameters, and service triggering data.

Application Server (AS): These entities provide value added services in the IMS domain. Although the ASs are not pure IMS entities, they are discussed in this study since voice call services or additional services involving voice may be deployed in the future by third parties with the use of ASs. Messaging, conferencing, and presence are provided using SIP ASs. Requests on these services provided by the AS are routed from the S-CSCF to the AS. The AS can act as redirect server, SIP proxy or generate a SIP message that it sends back to the S-CSCF in order to fulfil its function.

Subscription Locator Function (SLF): When there are multiple HSSs in the same domain, the SLF is queried by the I-CSCF, S-CSCF or the AS to locate the

University of Cape Town

correct HSS for the user.

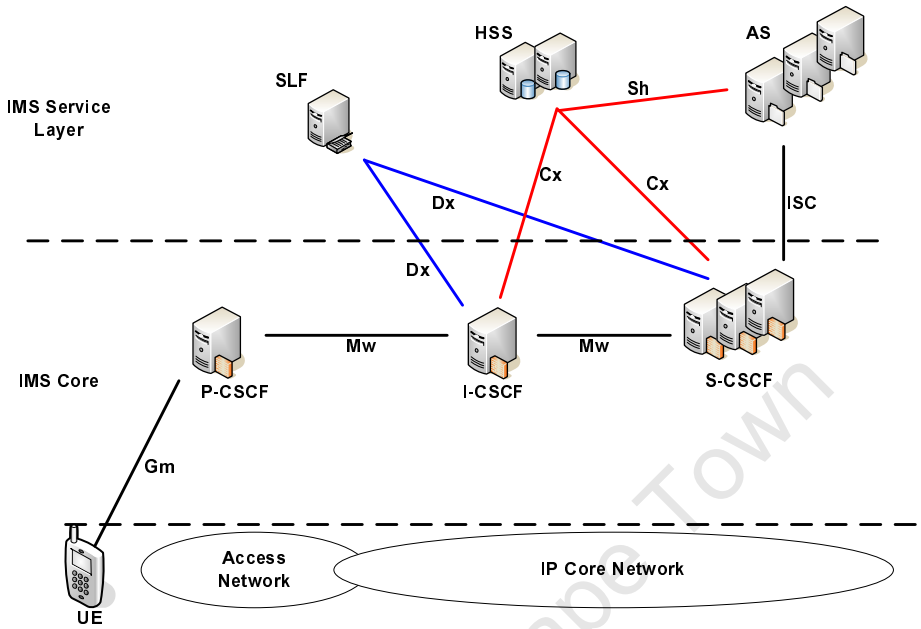


Figure A.1: IMS components and interfaces.

For further information on the other entities present in the IMS refer to the 3GPP specification TS 23.228 [14]. This section has looked at the relevant IMS entities and their functions. It is now necessary to discuss the main interfaces that these entities use to communicate with each other.

A.3 IMS Interfaces

This subsection will highlight on the main interfaces of the IMS. The reader needs to have knowledge of these interfaces to understand the decision to choose certain interfaces in the decoying system. The interfaces between the various IMS entities are illustrated in figure A.1, and table A.1 shows the purpose of the interfaces. However, there are other interfaces present in the IMS, for information on these interfaces refer to the IMS 3GPP specification [14] or the IMS book by Miika Poikselka et al [28].

University of Cape Town

Table A.1: Functions of the IMS interfaces.

Interface	IMS entities involved	Protocol	Function
G_m	UE, P-CSCF	SIP	Exchange of SIP messages of registration, session control, and transaction type between UE and P-CSCF.
M_w	P-CSCF, I-CSCF and S-CSCF	SIP	Exchange of SIP message between the P-CSCF, I-CSCF, and S-CSCF.
ISC (IMS Service Control)	S-CSCF and AS	SIP	Communication between AS and S-CSCF.
D_x	SLF, I-CSCF, S-CSCF	Diameter	When there are multiple HSS in an operator's network, the I-CSCF or S-CSCF query the SLF using this interface.
C_x	Between I-CSCF and HSS; Between S-CSCF and HSS	Diameter	Receiving a request, the I-CSCF queries the HSS on the S-CSCF allocated to the user. When the S-CSCF receives a REGISTER message, it informs the HSS it is serving the user. If the registration times out the S-CSCF can inform the HSS that it is no longer serving the user. The S-CSCF can download the user service profile from the HSS and can also update this profile via this interface. Shared secrets and shared sequence used for user authentication are obtained by the S-CSCF from the HSS using this interface.

University of Cape Town

A.4 IMS User Identities

The different IMS identities are presented as follows:

Private user identity: This identity is allocated by the network operator and is used to identify a user's subscription [14]. The private user identity is used for

authentication, hence it is present in all registration requests. This identity plays no part in routing messages. The S-CSCF stores this identity on registration and discards it after deregistration. The private user identity is stored in the IMS Identity Module (ISIM) so the user cannot modify this identity. The private user identity is of the form user_name@realm.

Public user identities: These identities are used for routing and are published on websites, phone books etc. These identities are not used for authentication and are either a SIP Uniform Resource Identifier (URI) e.g. sip:aka@sip-router.com or a telephone uniform resource locator (tel URL) [14]. These identities cannot be modified by the user and are stored in the ISIM.

Derived identities: With the introduction to the IMS, there will be a lot of UEs without the ISIM, however these UEs can use the Universal Subscriber Identity Module (USIM) to get a derived public and private user identity. The derived identities are set to barred and cannot initiate any IMS communication.

The private and public user identities are stored on the ISIM which is an application on the Universal Integrated Circuit Card (UICC). The UICC is a physical device that can be inserted or removed from an UE.

University of Cape Town

Appendix B

Installation Notes for Tools Used for the Evaluation Framework

University of Cape Town

B.1 SIPp

SIPp on Linux requires the following packages:

1. C++ Compiler
2. Curses or ncurses library
3. For authentication: OpenSSL >=0.9.8
4. For pcap play: libpcap and libnet

To install with PCAP play (for audio files) and authentication support, execute the following commands :-

```
cd sipp
make pcapplay_ossl
```

B.1.1 Adding patches

On the evaluation framework, one host had several SIPp clients running. To prevent each one from generating an output on the screen, a silentMode patch was installed. This patch added a new command line switch `"-si"`.

Another patch installed on the system, included functionality to register the clients after a specified time interval. This patch was called the Pace patch. For additional information on patches, refer to the website http://sourceforge.net/tracker/?atid=637566&group_id=104305&func=browse.

B.2 Iptel SER Installation

The source code for the Iptel SIP Express Router (SER) can be downloaded from `ftp://www.berlios.org/pub/ser`. Then unzip and untar all files and switch to the `sip_router` directory. To make the source code, root priviledges are required and the following command needs to be executed :-

```
make all
```

All the modules will be compiled. To install the binaries to location `/usr/local/etc/ser`, invoke the command :-

```
make install
```

To start the SER, the following command is executed :-

```
ser
```

Check that the SER is working properly by invoking `ps` which should show several ser processes.

University of Cape Town

B.2.1 Adding MySQL Support

A database is required to support authentication functions. SER uses MySQL databases to store authentication as well as media authorisation data. In order to support MySQL databases, the SER must be reinstalled.

The `Makefile` in `src/sip_router/` needs to modified. To ensure that MySQL module is loaded, remove reference to MySQL in `exclude_modules`. Next, recompile the SER as discussed previously. However, to support SER databases MySQL needs to be modified as well. This can be done by executing the command :-

```
dbinstall
```

To use the database, a modification to `ser.cfg` is required, and this was discussed in chapter 4.

University of Cape Town

Appendix C

Accompanying CD-ROM

The content of the accompanying CD-ROM are listed as follows:

- A soft copy of this thesis document in pdf format.
- Relevant publications used in this research.
- Lyx files and drawings required to generate the thesis document.
- Programs written to implement the evaluation framework.
- Publications of the author of this thesis.

University of Cape Town