UNIVERSITI PUTRA MALAYSIA

EFFECTS OF AUTHENTICATION OF USERS IN MOBILE INTERNET PROTOCOL VERSION 6

SIMON TABI OBENOFUNDE.

EFFECTS OF AUTHENTICATION OF USERS IN MOBILE INTERNET PROTOCOL VERSION 6

By

SIMON TABI OBENOFUNDE

Thesis Submitted to the School of Graduate Studies Universiti Putra Malaysia in partial Fulfilment of the Requirements for the Degree of Master of Science

July 2004

DEDICATION

To Arah, Auyaut and Ekepata.

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in partial fulfilment of the requirements for the degree of Master of Science

EFFECTS OF AUTHENTICATION OF USERS IN MOBILE INTERNET PROTOCOL VERSION 6

By

SIMON TABI OBENOFUNDE

July 2004

Chairman : Professor Borhanuddin Mohd Ali, Ph. D.

Faculty : Engineering

User security in the Internet has generally been well taken care of at the application layer. Judging from the mobility and portability of a mobile terminal and its ability to get connected to the Internet while away from home, it becomes necessary to be sure of who is using that terminal.

Presently, mobility is difficult, if not impossible to detect at the application layer though easily detectable at the network layer. Therefore it becomes necessary to apply the application layer solution to the network layer.

In this thesis, a user authentication program is modeled and simulated using *Network simulator2* (NS2). Various network topologies are simulated in order to investigate the effects of implementing this program on a network for various network performance

parameters. The results are stored in trace files. *Tracegraph201* is used to generate plots, from which data is extracted and then plotted again using *Excel* for comparison purposes.

In this thesis, we measured the throughput against simulation time, and then the delay against throughput and event time.

Comparisons are done between systems implementing authentication and those that do not. The results show that the average delay is not much affected by the implementation of the program. The network performance is greatly affected by the number of packet present in the network at any given time. Nevertheless, throughput is much improved at the detriment of bandwidth, as seen from the number of dropped packets. Thus, it is recommended that user authentication be applied to *mobile Internet Protocol version 6* (IPv6) as a security measure.

The conclusions made above are based purely on simulation results.

The password system is also recommended as a viable solution for this authentication as its implementation is most convenient for mobile users. A password algorithm is proposed from which a program can be written in any language deemed suitable.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia sebagai memenuhi sebahagian keperluan untuk Ijazah Master Sains

KESAN PENGESAHAN PENGGUNA DALAM IPv6 BERGERAK

Oleh

SIMON TABI OBENOFUNDE

Julai 2004

Pengerusi : Profesor Borhanuddinn Mohd Ali, Ph. D.

Fakulti : Kejuruteraan

Keselamatan pengguna Internet memang telah diambil kira dengan baik pada lapisan aplikasi. Dengan bersandarkan kebolehgerakan dan pangkalan bergerak mudah alih serta keupayaannya untuk disambungkan ke Internet ketika berada di luar rumah, adalah penting untuk menentukan siapa yang mengendalikan pangkalan tersebut.

Pada masa kini kebolehgerakan adalah rumit dan hampir tidak mungkin untuk mengesan lapisan aplikasi, walaupun lapisan rangkaian dapat dikesan dengan mudah. Oleh itu, ia menjadi sesuatu yang penting untuk menggunakan penyelesaian lapisan aplikasi terhadap lapisan rangkaian.

Di dalam tesis ini, satu program pengesahan pengguna telah disimulasi menggunakan *Network Simulator2* (NS2). Pelbagai rangkaian topologi telah disimulasikan bagi menyiasat kesan pelaksanaan program ini terhadap rangkaian untuk pelbagai parameter

prestasi rangkaian. Hasil program ini disimpan di dalam fail surihan. *Tracegraph201* digunakan untuk menjana plot dan datanya disaring dan diplot semula dengan menggunakan *Excel* bagi tujuan perbandingan.

Dalam tesis ini, truput diukur lawan masa simulasi dan seterusnya lengah lawan truput dan masa kejadian.

Perbandingan dilakukan di antara sistem dengan dan tanpa pelaksanaan kesahan. Keputusan menunjukkan bahawa purata lengah tidak mengalami kesan yang ketara. Prestasi rangkaian mengalami kesan yang besar akibat bilangan paket yang wujud dalam rangkaian pada sebarang masa. Sungguhpun demikian, truput dapat diperbaiki dengan ketara tetapi menjejaskan lebar jalur. Oleh itu, adalah disarankan agar pengesahan pengguna digunakan dalam Protokol Internet Versi 6 (IPv6) sebagai pengukuran keselamatan.

Kesimpulan tersebut di atas adalah berdasarkan keputusan simulasi sahaja.

Sistem kata-laluan juga disarankan menjadi sebagai satu penyelesaian yang mungkin untuk program pengesahan kerana perlaksanaannya adalah paling sesuai bagi pengguna bergerak. Algoritma kata-laluan dicadangkan dengan menulis satu program dalam sebarang bahasa yang bersesuaian.

ACKNOWLEDGEMENTS

I would like to express my profound gratitude firstly to my Supervisory committee chairman, Prof Borhanuddin Mohd Ali and then its members, Associate Prof Mahamod Ismail and Dr Sabira Khatun for their encouragements, time, suggestions etc. The importance of these to the completion of this work cannot be overemphasized.

I also want to thank my brother Chief Moses Obenofunde for the eye he put in the running of my business "TARAKAN VENTURES" in my absence, which provided the finances that enabled me undertake this degree program. Special thanks also go to my sisters Esther Tabenyang and Frida Enow, and my brothers Mukete and Egbe Obenofunde, and Divine Egbe Besong, their financial contributions cannot be overlooked.

This will not be complete, if I don't express my appreciation to my wife Sophia Arah and children for the sacrifices they made in staying with me, suspending their going to school, as our finances could not let all of us study at the same time. I simply say, "*Merci beaucoup, mes chers*".

I also mention some of my colleagues who helped me in one way or another. I am mainly talking about Naseer Abbas, and a host of others, whom because of space, their names cannot be mentioned here.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AH	-	Authentication header
AP	-	Application processes
ARP	-	Address Resolution Protocol
ARPA	-	American Advanced Research Projects Agency
ARPANET	-	American Advanced Research Projects Agency Network
ATM	-	Asynchronous Transfer Mode
BFWA	-	Broadband Fixed Wireless Access
CBC	-	Cipher block chaining
CBR	-	Constant Bit Rate
CCITT	-	International Telegraph and Telephone Consultative Committee
CFB	-	Cipher Feedback
CN	-	Corresponding Node
CSMA/CD	-	Carrier Sense Multiple Access Collision Detection
DES	-	Data Encryption Standard
DHRP	-	Dynamic Host Reconfiguration Protocol
DTE	-	Data Terminal Equipment
ECB	-	Electronic Codebook
ESP	-	Encapsulating Security Payload
FDDI	-	Fiber Distributed Data Interface
FTP	-	File Transfer Protocol
GPS	-	Global Positioning System
HA	-	Home Agent

HLEN	-	Header Length
IAB	-	Internet Architecture Board
ICCB	-	Internet Control and Configuration Board
ICMP	-	Internet Control Message Protocol
ICV	-	Integrity Check Value
IDEA	-	International Data Encryption Algorithm
IEEE	-	Institute of Electrical and Electronics Engineers
IETF	-	Internet Engineering Task Force
IP	-	Internet Protocol
IPng	-	Internet Protocol Next Generation
IPsec	-	Internet Protocol Security
IPv4	-	Internet Protocol version 4
IPv6	-	Internet Protocol version 6
IRG	-	Internet Research group
IRTF	-	Internet Research Task Force
ISDN	-	Integrated Services Data Network
ISO	-	International Standards Organization
ITF	-	Internet Task Force
KDC	-	Key Distribution Center
LAN	-	Local Area Network
MAN	-	Metropolitan Area network
MILNET	-	Military Network
MN	-	Mobile Node
MTU	-	Maximum Transfer Unit

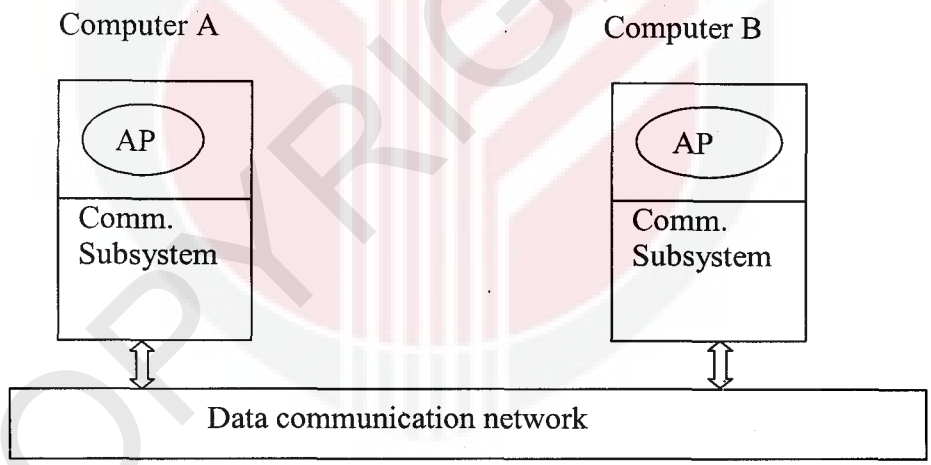
NS2	-	Network Simulator 2
OFB	-	Output Feedback
OSI	-	Open System Interconnection
OSIE	-	Open System Interconnection Environment
PC	-	Personal Computer
PSDN	-	Public Switched Data Network
PSTN	-	Public Switched Telephone Network
RARP	-	Reverse Address Resolution Protocol
RSA	-	Rivest-Shamir-Adelman
SDRP	-	Source Dynamic Routing Protocol
SFQ	-	Stochastic Fare Queuing
SNMP	-	Simple Network Management Protocol
SONET	-	Synchronous Optical Network
TCP	-	Transmission Control Protocol
TDM	-	Time Division Multiplexing
TELNET	-	Telecommunication Network
TFTP	-	Trivial File Transfer Protocol
TIL	-	Time Interval Length
UDP	-	User Datagram Protocol
UMTS	-	Universal Mobile Telecommunication System
WAN	-	Wide Area Network

CHAPTER 1

INTRODUCTION

The importance of connecting computers together cannot be overemphasized, especially since the introduction of personal computers (PC). Presently, a whole world of new applications is now possible because of these [Behrouz, 2000]. These are found in areas ranging from optical communications to mobiles and even satellite communication.

Computer communication entails consideration of both the hardware and software. For this purpose, a computer can be said to be made up of applications and a communication subsystem [Fred, 1997], as shown in Figure 1.1



AP= Application Processes

Figure 1.1: Computer subsystems in terms of communication

The type of data communication network technology applied, is a function of the nature of the application, number of computers in communication and their physical separation.

Hence, there exist local area networks, LANs, metropolitan area networks, MANs and Wide area networks, WANs. Various combinations of these (Internetworking) might result in the use of public transmission facilities. These include the Internet, Packet switched Network, 3G, UMTS, GPS, BFWA and others.

1.1 Problem Statement

Extensive research on IPv6 security issues, especially on security mechanisms usually excludes the authentication of users [Williams, 1995, Kent and Atkinson, 1998]. User authentication is usually considered only at the application layer. With increase in portability of mobile devices, it becomes easy for mobile terminals to be stolen or get into the hands of malicious users. Since a mobile terminal in Mobile IPv6 can get connected to the Internet at any location away from its home network, the user of this terminal at this point must be ascertained in order not to compromise the security of the network.

Authentication of a mobile user therefore, involves making sure that it is the owner (authorized user) of the terminal who is trying to get connected to the Internet at a location away from his home network. Authentication as defined in the IPsec usually concerns ascertaining that packets come from where (nodes) they claim to come from, having nothing to do with user (people).

Therefore, there is need to look into ways and means of securing users in Mobile IPv6.

1.2 Objectives of The Thesis

The aim of this thesis is to simulate the authentication of users in Mobile IPv6 and then examine the effects on network performances, especially the amount of delay, throughput, and bandwidth that will be introduced in the process. These will then be used as parameters to determine if it is worthwhile applying this process for the security of the entire network or for a particular node that is in a dire need to secure its transactions.

1.3 Scope of Work

This thesis proposes the implementation of a user authentication program as a network security measure. It does not cover the subject of authentication as a whole, though a brief introduction of this topic is given in chapter 3,which deals with Internet security. It also does not cover the subject of Mobile IPv6 as a whole. Mobile IPv6 is only introduced here in order to help in the understanding of the problem being addressed in this thesis.

Only three topologies (among a many that can be used to study the system) will be studied in this thesis.

Only bi-directional tunneling in Mobile IPv6 has explicitly been examined in this thesis. The same solution can then be applied to the other option of route optimization.

Also, a password authentication algorithm is proposed, from which an authentication program can be written with any suitable programming language.

Though the password system is being proposed here as a viable solution for authenticating a mobile user, it is by no means implied to be the best in terms of security. Other solutions like retinal pattern, hand scan, and other biological authentication methods, have not been looked into as they are out of the scope of this thesis.

1.4 Network Performance Parameters

For this thesis, the network performance parameters to be studied include:

a. Link bandwidths

b. Delay

c. Throughput, and

d. Packet losses

1.4.1 Bandwidth

An important parameter determining the network performance is the bandwidth [Kleinrock, 1976]. Bandwidth can be defined as the width of the frequency spectrum. In other words, it is a measure of the link capacity, the number of channel it can support. It can be expressed as:

$$bw = f_{max} - f_{min} \quad (1.1)$$