DESIGN & DEVELOPMENT OF AN EMBEDDED NETWORK SECURITY SYSTEM (ENSS)

By

NASIM AHMED
(0630210132)

A thesis submitted
In fulfillment of the requirements for the degree of
Master of Science (Computer Engineering)

School of Computer and Communication Engineering
UNIVERSITY MALAYSIA PERLIS (UniMAP)
MALSYSIA

2009

UNIVERSITY MALAYSIA PERLIS

DECLARATION OF THESIS

Authors Full Name : NASIM AHMED

Date of birth : 26 September 1979

Title : DESIGN & DEVELOPMENT OF AN EMBEDDED NETWORK SECURITY SYSTEM (ENSS)

Academic Session : 2007/2008

I, hereby declare that this thesis becomes the property of University Malaysia Perlis (UniMAP) and to be place at the University library. This thesis is classified as :

CONFIDENTIAL	□	(Contains confidential information under the Official Secret Act 1972)
RESTRITED	□	(Contains restricted information as specified by the organization where research was done)
OPEN ACCESS	☑	I agree that my thesis is to be made immediately available as hard copy or on-line open access (full text)

I, the author, give permission to the University Malaysia Perlis to reproduce this thesis in whole or in part of the purpose of research or academic exchange only (except during a period of ……. years, if so requested above).

	Certified by
…………………….	………………………………….
SIGNATURE	**SIGNATURE OF SUPERVISOR**
Q-0397113	ASSOCIATE PROFESSOR DR. R. BADLISHAH BIN AHMAD
…………………………………..	………………………………………………………………
(PASSPORT NO. / NEW IC NO.)	NAME OF SUPERVISOR
Date: ………………..	Date: …………………………

NOTES: * If there is CONFIDENTIAL or RESTRICTED, please attach with the letter from the organization with period and reasons for confidentially or restriction.

GRADUTE SCHOOL

UNIVERSITY MALAYSIA PERILS

PERMISSION TO USE

In presenting this thesis in fulfillment of a post graduate degree from the University Malaysia Perils, I agree that permission for copying of this thesis in any manner, in whole or in part, for scholarly purposes may be granted by my supervisor(s) or, in their absence, by the Dean of the Graduate School. It is understood that any copying or publication or use of this thesis or parts thereof for financial gain shall not be allowed without any written permission. It is also understood that due recognition shall be given to me and to University Malaysia Perils for any scholarly use which may be made of any material from my thesis.

Request for permission to copy or to make other use of material in this thesis whole or in part should be addressed to

Dean of Graduate School
University Malaysia Perils (UniMAP)
Jalan Meranti Paya off Jalan Bukit Lagi
01000 kangar
Perlis

ACKONWLEDGEMENT

First and foremost, I would like to convey my deepest graduate to the Almighty Allah (SWT), the Omnipotent, the Merciful and the Compassionate, for giving me strength, patience, courage and determination in compiling this research. Alhamdulilah.

A journey is easier when you travel together. Interdependence is certainly more valuable than independence. This thesis is the result of work whereby I have been accompanied and supported by many people. It is a pleasant aspect that I have now the opportunity to express my gratitude to all of them.

With immense pleasure I express my sincere gratitude, regards and thanks to my supervisors, Associate Professor Dr. R. Badlishah Ahmad, and Zahereel Ishwar Abdul Khalib for the excellent guidance, invaluable suggestions and continuous encouragement at all stages of my research work. Their interest and confidence in me was the reason for all the success I have made. I have been fortunate to have them as my guides as they have been a great influence on me, both as a person and as a professional.

It was a pleasure to be associated with Computer Computing Research Cluster (ECRC, UniMAP) and I would like to thank the entire Lab member. Special thanks to Md. Mostafijur Rahman, Yacine Laalaoui, Mr. Basir, those are at some or the other point involved in my works. I would like to thank all my friends for their smiles and friendship making my life at (ECRC) enjoyable and memorable.

Above all, I am blessed to have such caring parents. I convey my deepest gratitude to my parents and sisters for their invaluable love, affection, encouragement and supports. My heartfelt thanks go out to my dear wife Mst. Noorzahan Begum, who has been so patient and supportive since I started my research. She has been my inspiration and provided the encouragement when my research progress was slow, and when I felt like spiraling out of control, she has brought serenity. It should be no surprise that this thesis would be impossible without her. I dedicate this thesis to my parents and beloved wife.

The chain of my gratitude would be definitely incomplete if I forget to thank the first cause of this chain, using Aristotle's words, The Prime Mover.

Thanks to Almighty ALLAH.

NASIM AHMED
UNIVERSITY MALAYSIA PERLIS
nasim751@yahoo.com

TABEL OF CONTENTS

CHAPTER 1: INTRODUCTION

CHAPTER 2: LITERATURE REVIEW

CHAPTER 3: EMBEDDED SYSTEM BASED ON GNU/LINUX

CHAPTER 4: SYSTEM DEVELOPMENT

CHAPTER 5 : RESULTS AND DISCUSSION

APPENDICES Pages

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AC	*Alternating Current*
ACK	*Acknowledgement*
ACPI	*Advanced Configuration and Power Interface*
API	*Application Programming Interface*
AMD	*Advance Micro Device*
ANSI	*American National Standard Institute*
ARPANET	*Advanced Research Project Agency Internet Work*
ARM	*Advance RISC Machine or Acorn RISC Machine*
BIOS	*Basic Input/Out-Put System*
BSD	*Berkeley Software Distribution*
CF	*Compact Flash*
CPU	*Central Processing Unit*
CERT/CC	*Computer Emergency Response Team Coordination Center*
DDoS	*Distributed Denial-of-Service Attack*
DOD	*Department of Defense*
DoS	*Denial-of-Service*
DOS	*Disk Operating System*
DNS	*Domain Name System*
DRAM	*Dynamic Read Access Memory*
EOS	*Embedded Operating System*
EEPROM	*Electrically Erasable Programmable Read-Only Memory*

ENSS	*Embedded Network Security System*
EXT2	*Second Extended File system*
EXT3	*Third Extended File system*
FAT	*File Allocation Table*
FSB	*Front Side Bus*
FTP	*File Transfer Protocol*
GCC	*Gnu Compiler Collection*
GNU	*Gnu's Not Unix*
GPL	*General Public License*
GUI	*Graphical User Interface*
HTTP	*Hypertext Transfer Protocol*
IBM	*International Business Machine*
ICMP	*Internet Control Message Protocol*
ICs	*Integrated Circuits*
IDE	*Integrated Device Electronics*
IDS	*Intrusion Detection System*
IEEE	*Institute of Electrical and Electronics Engineers*
I/O	*Input Output*
IPV	*Internet Protocol Version*
IP	*Internet Protocol*
IPS	*Intrusion Prevention System*
ISPs	*Internet Service Providers*
JFS	*Journaled File System*

JPL	Jet Propulsion Laboratory
JVM	*Java Virtual Machine*
LAN	*Local Area Network*
LCD	*Liquid Crystal Display*
LSI	*Large – Scale – Integrated*
MB	*Megabyte*
MIPS	*Million Instruction Per Second*
MMU	*Memory Management Unit*
NIDS	*Network Intrusion Detection System*
NFS	*Network File System*
OEM	*Original Equipment Manufacture*
OOP	*Object Oriented Programming*
OS	*Operating System*
PC	*Personal Computer*
PCMCIA	*Personal Computer Memory Card International Association*
PDA	*Personal Digital Assistant*
PSH	*Push*
POSIX	*Portable Operating System Interface*
R & D	*Research and Development*
RISC	*Reduce Instruction Set Computer*
RFC	*Request for Comments*
ROM	*Read Only Memory*
RAM	*Random Access Memory*

RTOS	*Real Time Operating System*
SBC	*Single Board Computer*
SCP	*Secure Copy*
SCSI	*Small Computer System Interface*
SDRAM	*Synchronous Dynamic Random Access Memory*
SSH	*Support Secure Shell*
SNMP	*Simple Network Management Protocol*
SP2	*Service Pack2*
SSD	*Solid State Disk*
SRAM	*Static Random Access Memory*
SVGA	*Super Video Graphics Array*
SYN	*Synchronize*
TCP	*Transmission Control Protocol*
TCBs	*Transmission Control Blocks*
TFTP	*Trivial File Transfer Protocol*
TS	*Technologic System*
UART	*Universal Asynchronous Receiver Transmitter*
UDP	*User Datagram Protocol*
URG	*Urgent*
USB	*Universal Serial Bus*
VHDL	*Very High Hardware Description Language*
VHSIC	*Very High Speed Integrated Circuit*
VGA	*Video Graphics Array*

VoIP	*Voice Over Internet Protocol*
WAN	*Wide Area Network*
WWW	*World Wide Web*

ABSTRAK

Membangun dan mereka bentuk Satu Sistem Keselamatan Rangkaian Terbenam (ENSS)

Sistem terbenam makin menjadi satu penyelesaian yang menarik bagi pelbagai aplikasi kerana kestabilan, penggunaan kuasa elektrik yang rendah dan kemudahalihan. Tesis ini membincangkan rekabentuk dan pembangunan sebuah sistem terbenam bagi aplikasi keselamatan jaringan (ENSS), yang berasaskan komputer di atas satu papan menggunakan sistem operasi(OS) GNU/Linux. Perisian ENSS distrukturkan kedalam tiga modul yang dinamakan, pengimbas terminal (port scan), serangan pengimbas terminal, pengesan serangan 'smurf'. Pendekatan yang diambil ialah membina perisian yang mampu mengimbas terminal menggunakan teknik half-open,UDP dan horizontal selain dari mengesan kemungkinan serangan imbasn terminal dan serangan smurf. Perisian ini dijanakan keatas komuter sistem terbenam berasaskan pemproses x86 keluaran TS-Linux. ENSS direkabentuk untuk menjalankan operasi imbasan port yang bertujuan mengenalpasti kelemahan host dengan menghantar pengesan terminal. Serangan pengimbas terminal pula berfungsi untuk mengesan percubaan imbasan terminal yang dilakukan dan mengumpul maklumat sistem komputer berkenaan. Sementara pengesan serangan smurf pula berfungsi unutk mengesan serangan smurf (siar raya paket yang disalin dan analisa maklumat trafik ICMP). Hasil kajian menunjukan bahawa prestasi sistem yang dijanakan diatas sistem terbenam adalah hampir sama dengan pengimbas terminal yang lain yang dijanakan diatas PC yang mempunyai kuasa pemprosesan yang tinggi. Prestasi ENSS dari segi penggunaan CPU dan ingatan menunjukan bahawa sistem terbenam GNU/Linux adalah sesuai bagi aplikasi keselamatan rangkaian walaupun mempunyai kemampuan perkakasan pemprosesan dan ingatan yang rendah. Harga komputer sistem terbenam yang rendah dan kemudahalihan menjadikan ENSS satu alternatif yang baik bagi sistem pengesan keselematan jaringan.

ABSTRACT

Embedded system is becoming an interesting solution to various applications due to high stability, minimal power consumption, and portability. This thesis describes the design and development of an embedded system for Network Security Applications (ENSS), which is based on Single Board Computer (SBC) utilizing GNU/Linux Operating System (OS). The ENSS software is structured in three modules namely Port Scan, Port Scan Attack and Smurf Attack Detection. The approach is to develop software which performs port scan using half-open, UDP, and horizontal techniques as well as to detect the possible port scan attack and Smurf Attack. The software is executed on an x86 based TS-Linux Single Board Computer (SBC). ENSS is designed to operate Port scan, which is used for discovering hosts weaknesses by sending port probes. Port scan attack detection is to identify port scan attempts and find out information about the machine. The Smurf Attack Detection is used to identify Smurf based attack (Broadcast Duplicate Packet and analyze ICMP traffic information). Results show that the system performance on the embedded platform is almost similar to other port scanners running on a much better performance PC. The ENSS performance in terms of CPU utilization and memory usage indicate that embedded GNU/Linux platform is suitable for network security applications although under hardware limitations of memory and processing speed. Lower cost of the Single Board Computer and the extra benefit of portability make ENSS a good alternative system for network security detection system.

CHAPTER 1

INTRODUCTION

1.1 Overview

Security is an important issue for all computer networks. It is a continuing problem with constant evolution and changes. Hackers and intruders can create many successful attempts to cause the crash of networks and web services of individual companies. Many methods were developed to ensure the protection of the network infrastructure and communication over Internet, such as firewalls, encryption, and virtual private networks.

Intrusion detection is a set of techniques and methods which are used to identify the malicious activity on the network as well as host level (L. Vokorokos, 2006). Network – oriented intrusion detection systems can be roughly divided into distributed IDSs and network-based IDSs. Network-based IDSs take a different perspective and change their focus from the computational infrastructure (the hosts and their operating systems) to the communication infrastructure (the network and its protocol) (Snapp et al., 1991). A survey of network-oriented IDSs is given in Mukherjee and Levit (Mukherjee, Heberlein, & Levitt, 1994).

Given the recent growth of the Internet, network-scanning incidents are becoming common events of life. Although several network information centers have declared that network scanning is an illegal activity. As an example, China Education and Research

Network (CERNET) enacted a law to prohibit network scanning (such as port scans and IP-address scans) in Nov 27, 1999, the events still occurring and becoming more frequent. The reason why network scanning occurs increasingly is pretty obvious because network scanning is a prerequisite of many network attacks. A successful attack usually proceeds by scanning. With a good TCP/IP scanner tool, hackers will quickly find which OS host is running. The current methods of detection and protection against network scanning are limited in their strategy.

The aim of network scanning is used to obtain the information of a host on a particular network. Generally, we can gain it through three ways: the first is through normal use, the second is through misuse, and the last way goes through sniffing. Network scanning implementation includes the first and the second method. The purpose of network scanning can be summarized as:

- Obtaining the application information of the host, for example, which port service name and protocol works.
- Obtaining the basic system information of the host, such as: hardware platform, operating system (OS), including its version.

An embedded system is defined as a combination of computer hardware and software and perhaps additional mechanical and other parts that perform a dedicated function. In some cases, embedded systems can be a part of a larger system or a product (Barr, 2002). However, there are many basic design differences between embedded systems and conventional personal computers (PCs). Some of the distinct attributes of embedded systems are (Koopman & 1999):

- A dedicated processor that may be specifically designed for the application.
- Application specific software that may not even use an operating system.
- Often no standard keyboard.
- Limited or no display capability.
- Designed to react to external periodic and/or a periodic event.
- Designed to operate in a real time environment.

Embedded systems have become ubiquitous due to the wide range of functionality it provides. A recent survey on the sale of microprocessors worldwide has indicated that while the number of personal computers shipped each year exceeds 140 million units; the number of embedded microprocessors shipped each year exceeded 5 billion units (Nick Tredennick & 2000). These numbers suggest the overwhelming presence of embedded systems in today's technology savvy world. While the PC market has stagnated in recent years, the embedded systems market is growing every year. From an applications perspective, embedded systems can be broadly categorized into four types (Koopman & . 1999).

1. General computing
    - Applications similar to desktop computing but in an embedded package.
    - Video games, automatic tellers.
2. Control systems
    - Closed- loop feedback control of a real- time system.
    - Automobiles, chemical processes, power plants, flight control.