Title: BUFFER OVERFLOW PROTECTION USING STACKGUARD AND STACK-SMASHING PROTECTION aka PROPC LICE

By

MOHD NOR EFFENDY BIN ZAINON AZNAN
(2001189075)

A project paper submitted to
FACULTY OF INFORMATION TECHNOLOGY AND QUANTITATIVE SCIENCES
MARA UNIVERSITY OF TECHNOLOGY

In partial fulfillment of requirement for the
BACHELOR OF SCIENCE (Hons) IN DATA COMMUNICATION AND NETWORKING

Major Area : Network Security

Approved by the Examining Committee :

.....

En. Abdul Hamid bin Othman — Project Supervisor

.....

En. Kamarul Ariffin Abdul Basit — Examiner

MARA UNIVERSITY OF TECHNOLOGY
SHAH ALAM, SELANGOR
OCTOBER 2003

ACKNOWLEDGEMENT

By the name of Allah, the Most Gracious and Most Merciful.

All praises be to Allah s.w.t, duely to His blessing and kindness that I had gain during the completion of this project. Without His guidance, the completion of this project is impossible.

I would like to express my sincere and highest gratitude to those who had been involved in contributing their help and support, directly or indirectly, in making this project a successful reality. It has been my good fortune to have the advice and guidance of many talented people, whose knowledge and skills have enhance this project so many ways.

First and foremost, I would like to address my deepest appreciation and highest admiration to my dedicated supervisor, En. Abdul Hamid bin Othman, for his guidance, encouragement, ideas, tolerance, motivation and support that led to the completion of this project. I feel most fortunate to have this opportunity to learn and gain experience from such a skilled and experienced supervisor.

Then I would like to give my thanks to all the lecturers of TMSK for their loving, guidance and motivation not only to me, but the whole students of the faculty especially to Prof Dr. Saadiah Yahya, En Mohd. Faisal b Ibrahim, En. Jamal, and En. Kamarul Ariffin Abdul Basit .

Last but not least, to all my friend, classmate and family for the love, encouragement and strength they gave me.

Thank You.

ABSTRACT

Buffer overflow vulnerabilities emerge and are announced frequently. Exploitation details and exploits are publicly available for interested parties. These code-based attacks allow malicious code to be executed on the vulnerable systems. This paper provides a brief introduction to buffer overflow vulnerabilities and methods of exploiting them and how the prevent these attacks using compiler tools. The tools used in this project are StackGuard from Wirex Immunix and Stack Smashing Protection aka ProPolice from IBM. A survey is made of exploits that are easily available to everyone, including the underground community. Articles on buffer overflows are reviewed, and the exploits presented are examined in terms of functionality. A platform is setup where these protections will be tested. An attempt to compile a vulnerable program is made to verify the capabilities of each compiler. Whether these compilers can detect, prevent or stop vulnerable programs from being compiled or executed.

TABLE OF CONTENT **PAGE**

CHAPTER 1

INTRODUCTION

1.1 PROBLEM STATEMENT

The day when the world finally acknowledged the risk entailed in overflow vulnerabilities and started coordinating a response to them was the day when the Internet Worm was introduced, spread and brought the Internet to its knees. In his analysis of the worm, Spafford (1989) presents some details of the buffer overflow exploit against the 'fingered' program for BSD-derived versions of Unix running on VAX computers. Some research and response work was initiated in the security field, but a limited amount of academic work was available to the general public regarding the causes behind buffer overflow vulnerabilities and their ease of exploitation. Since then, several discoveries have been announced as public disclosures on mailing lists, such as Bugtraq, where security-aware people has donated their knowledge on the subject (Myers, 1993-1999; Netspace, 1995-1999; SecurityFocus, 1999).

Buffer overflows are probably one of the most advanced attack techniques ever made or created. Ever since Dr. Mudge's discussions of the subject in his 1995 paper "How to write buffer overflows", the world of UNIX security has never been the same. Aleph One's 1996 articles on "Smashing the stack for fun and profit", originally published in Phack Magazine issue no 49, is also a classic paper detailing how simple the process is for overflowing buffer.

According to Taeho Oh of Postech Linux User Group in his paper titled Advanced Buffer Overflow Exploit, the early buffer overflow exploit codes only spawn a shell (execute /bin/sh).