Title:

Designing and Deploying Network based Intrusion Prevention System on FSBM Holding Berhad Network

By

ABU UBAIDAH BIN MD ZAIN

A project paper submitted to the
Faculty of Information Technology and Quantitative Science
MARA UNIVERSITY OF TECHNOLOGY

In partial fulfillment of requirement for the
BACHELOR OF SCIENCE (Hons) IN DATA COMMUNICATION AND NETWORKING
CS225

Approved by the Examining Committee:

En. Faisal B. Ibrahim — Project Supervisor

Prof. Madya Dr. Saadiah binti Yahya — Examiner

OCTOBER 2003

ACKNOWLEDGEMENT

In the name of Allah, (Al-Mighty) The Most Gracious, The Most Merciful.

I would especially like to thank my supervisor, En. Mohd. Faisal B. Ibrahim whose teachings have given me ideas, advises and guides to complete this research paper. Special thanks also to my project coordinator and examiner, Dr Saadiah binti Yahya.

In addition, I would like to thank to all lecturers of the Faculty of Information Technology and Quantitative Science, for their support and encouragement.

I also would like to thank, Mr Tahrizi Tahreb and Mr. Zahidi Zaini for their support and cooperation.

To my family, my loving mother, to all my brothers and sisters, I thank Allah for having such a supportive family.

Lastly, I would like to state on record here that in the compilation of this research I have taken some co-operation, advises, some portion of writing and references from many sources. If due acknowledgement has not been made, I sincerely regret the omission and apologize for the oversight

Thank You.

Abu Ubaidah bin Md Zain
October 2003

ABSTRACT

The tools available to IT security professionals are becoming more proactive by attempting to prevent, rather than only detect. Intrusion prevention, in particular, has received a lot of attention in the IT press in the last several years. But not many are research are made on intrusion prevention system.

In this report we explored Intrusion Protection Systems (IPS) from the perspective of using IPS as part of a Defense in Depth strategy. We studied about embedded intrusion prevention system network performance. We also focused in writing rules for our embedded intrusion prevention system based on vulnerabilities that we had found.

TABLE OF CONTENT