DEVELOPING A SERVER-LEVEL VIRUS-DETECTION AND BLOCKING SOLUTION FOR EMAIL VIRUSES

BY

JENNIFER D. DORADO

CHESTER A. GO

KRISTINE I. LABRADOR

SCHOOL OF ARTS AND SCIENCES
ATENEO DE DAVAO UNIVERSITY

MARCH 2002

DEVELOPING A SERVER-LEVEL VIRUS-DETECTION AND BLOCKING SOLUTION FOR EMAIL VIRUSES

A Mini-Thesis

Presented to

The Faculty of the Computer Science Division

Ateneo de Davao University

In Partial Fulfillment

of the Requirements for the Degree

Bachelor of Science major in Computer Science

by

Jennifer D. Dorado

Chester A. Go

Kristine I. Labrador

March 2002

TABLE OF CONTENTS

ABSTRACT

Electronic mail is the new mode of sending messages to millions of computer users worldwide. Compared to the traditional snail mail, email proves to be much quicker as well as much efficient. The ease of sending email messages to people around the world brought about the ease of spreading computer viruses too. A computer virus is a dangerous computer program, whose purpose is to destroy computer systems as well as spread its destructive code to innocent computer users.

Users and corporations began practicing safe computing by backing up every possible bit of data and run virus-scanning programs. However, these preventive measures are done on desktop workstations. This research aims to protect computer systems from email-borne viruses even before it reaches the workstations by detecting and blocking these viruses at the server level. This technique is beneficial since the virus will be contained even before it reaches the company's network therefore, preventing further damages to the computer system.

Chapter 1

Introduction

1.1 Background of the Study

Nowadays, email has become an important and convenient communication tool among people. Organizations, both large and small consider email as critical tool for delivering vital information and as a medium for communication. However, email becomes the new method of distributing viruses over computers through the Internet. Almost everyday, one reads new threats on the electronic transmission of information. The ease with which a user can click on an attachment is a significant factor in the spread of email-borne viruses. Due to this increasing threat, many attempts had been made to protect emails from viral infection. Several anti-virus software were developed to remove the viruses from the infected mails. These software could not protect emails against all viruses and attacks. Email content filtering software was also developed to check all inbound and outbound emails at the server level. Despite of this, many email viruses bypass the virus detection capability of these software and continue to infect millions of computer systems. Thus, there is a need to find a solution to this problem.

1.2 Statement of the Problem

The main problem of this study is how to develop a virus-detection and blocking solution for email viruses based on the detection mechanism of email anti-virus and content filtering software.

1.3 Objectives

The main objective of this study is to develop a virus-detection and blocking solution for email viruses based on the detection mechanism of three existing email anti-virus and content filtering software.

The specific objectives are:

- To identify three email virus categories.
- To identify two email viruses for each category.
- To identify three existing email anti-virus and content filtering software.
- To make a comparison on the detection mechanism of these three email anti-virus and content filtering software.
- To develop a new framework for a virus-detection and blocking solution.
- To demonstrate the solution by developing a blocking application.

1.4 Scope and Limitation

The study focused on developing a blocking solution for email viruses on Linux-based mail servers that uses Sendmail. It blocked all inbound and outbound email messages infected with two email viruses under three categories. Also, three existing email anti-virus and content filtering software were studied.

1.5 Significance of the Study

Email viruses damaged millions of computers worldwide. Large corporations, organizations, and even common computer users suffered major losses. This research will address the escalating email security problem caused by these viruses through developing a blocking solution for three email virus categories. This blocking solution will scan all inbound and outbound email messages at server level before distributing it to users. This approach will ensure the security of computer systems, which is important to every organization. Moreover, this study can be used as reference for further studies on blocking email viruses of other categories.