University of Southern Queensland

Faculty of Business and Law
School of Information Systems

Key factors impacting on response time of software vendors in releasing patches for software vulnerabilities

A Dissertation submitted by

Arjun K.C.

For the award of
Master of Business Research

2012

Abstract

Software vulnerabilities are a major problem for organizations and society given how pervasive the use of computers and the Internet and networks has become. Computers, the Internet and networks in general are underpinned by operating system software and, increasingly, software applications are integrated with the Internet. In this increasingly complex environment hackers and attackers are more likely to take advantage of software vulnerabilities and exploit operating system software and application software. These software exploitations can result in huge losses to businesses which are highly reliant on computerized systems. Software vendors are responsible for securing these vulnerabilities through software patching. This study examines the effect of the level of criticality of software vulnerabilities, type of software vendor and type of software on the software vendors' response time in releasing software patches once software vendors have been informed of vulnerabilities in their software.

The main theoretical support for this study is software security disclosure theory and an economic model of software security investment. These theories provide a framework for understanding how open source versus proprietary software vendors respond with patches to software vulnerabilities depending on the level of criticality of the software vulnerability and the type of software.

Empirical data was collected from four related software vulnerability databases: SecurityFocus, Open Source Vulnerability Database, National Vulnerability Database and Secunia. These four software vulnerability databases contain archival data about software vulnerabilities which has been rigorously collected and screened. This research focuses on software vulnerabilities that have been recently reported in these software vulnerability databases from 2008 to 2010. To test the hypothesised relationships in the proposed research model, multiple regression analysis is used as the main statistical tool.

Analysis of the archival data confirms that software vendors release patches for software vulnerabilities with a medium level of criticality in a shorter response time

than software vulnerabilities with low and high levels of criticality once the vendor has been informed of the software vulnerability. Open source vendors release patches for open source software vulnerabilities 39% quicker than proprietary source vendors release patches for proprietary software. Patches for operating system software vulnerabilities are released 8% slower than patches for application software vulnerabilities.

This study contributes to the existing knowledge and theory by investigating how the different levels of criticality of software vulnerabilities, the differences between open and proprietary source software vendors and the difference between operating system software and application software impact on the response time of software vendors in releasing patches once the software vendor is informed of software vulnerabilities. The findings of this study also establish that responsible disclosure is a more effective mechanism than full disclosure for determining the response time of software vendors. This study contributes to practice by providing an enhanced understanding of the software vulnerability landscape and the complex process of software vendors' patching behaviour.

Certificate of Dissertation

I certify that the ideas, designs, experimental work, results, analyses, software and conclusions set out in this dissertation are entirely my own effort, except where otherwise indicated and acknowledged.

I further certify that the work is original and has not been previously submitted for assessment in any other course or institution, except where specifically stated.

_____ _____

Signature of Candidate Date

ENDORSMENT

_____ _____

Signature of Principal Supervisor Date

_____ _____

Signature of Associate Supervisor Date

Acknowledgements

I would like to take this opportunity to thank everyone who has provided me with assistance and support for the duration of this study. In particular, I would like to thank the following people who helped me to make this thesis a realisation.

Firstly, I would like to express my gratitude to my Principal Supervisor Dr. Michael Lane for his guidance and useful suggestions throughout the structure and contents of this thesis.

Secondly, I would also like to thank Dr. Jianming Yong, my associate-supervisor, who provided initial support during my research proposal.

Last but not least, I wish to express my deepest sense of gratitude to my beloved wife Dilu KC and my daughter Jasmine KC for their love, encouragement and support and my parents for providing me the academic foundations without which this thesis would not be possible. Similarly, sincere thanks to my loving friends Sanjib Tiwari, Arjun Neupane and Rohini Prasad Devkota for their continuous support, cooperation, encouragement and providing light in dark days.

Table of Contents

List of Tables

List of Figures

List of Appendices

List of Abbreviations

NVD:	National Vulnerability Database
OSVDB:	Open Source Vulnerability Database
CERT:	Computer Emergency Response Team
OWASP:	Open Web Application Security Project
OVAL:	Open Vulnerability and Assessment Language
CWE:	Common Weakness Exposure
CVE:	Common Vulnerability Exposure
CAPEC:	Common Attack Pattern Enumeration and Classification
SDLC:	Software Development Life Cycle
CASE:	Computer Aided Software Design
ERP:	Enterprise Resource Planning
S-SDLC:	Software Security Development Life Cycle
SOAP:	Simple Object Access Protocol
OSGi:	Open Services Gateway Initiative
WASC:	Web Application Security Consortium
XSS:	Cross Site Scripting
CSRF:	Cross-Site Request Forgery