A Formal Framework for Patch Management

Guillermo A. Francia, Jacksonville State University, Jacksonville, AL, USA
Kihyun Kim, Jacksonville State University, Jacksonville, AL, USA
Byungoh Ahn, Korea Institute for Defense Analyses, Seoul, Korea
Sen Xin Zhou, Anhui University of Finance and Economics, Anhui, China

ABSTRACT

A patch management model provides a framework with which a system’s parameters and behavior can be tested and validated. The authors propose a formal framework that is based on the Continuous Time Markov Chain Model and validate the model using the SHARPE modeling tool. Furthermore, they perform sensitivity analyses to study the dynamic behavior of the proposed model with varying parameter values. A discussion on the results of our study and future research directions concludes the paper.

Keywords: Availability, Patch Management, Patchability, Sensitivity Analysis, Survivability, Vulnerability

INTRODUCTION

Motivation and Research Objective

The primary objective of this research study is to create a patch management model that has generic applicability to computer systems that are connected over the Internet. The secondary objectives are to establish meaningful metrics to measure the system patch and its performance, and to study system behavior with varying parameters.

We present the stochastic model that was developed and based on the Continuous Time Markov Chain (CTMC) Model. The proposed model is validated using the Symbolic Hierarchical Automated Reliability and Performance Evaluator (SHARPE) tool. This proven and stable tool is primarily used to specify and analyze the performance, reliability and performability models (Sahner, Trivedi, & Puliafito, 1996). We also illustrate the sensitivity analyses that we performed to study the dynamic behavior of the proposed model with varying parameter values.

Background

Most security vulnerabilities are caused by software flaws, and software vendors are in a race to develop patches against vulnerability. According to McAfee’s report (2012), 438 information technology (IT) professionals

DOI: 10.4018/jitn.2013040102
worldwide have indicated that the largest risk management challenges are discovering threats and vulnerabilities in their information systems, and one-third of their organizations keep increasing their risk and compliance expenditures. Though the number of reported vulnerabilities has been under a descending trend after a peak in 2008, secure and mission-critical companies and organizations still faced approximately ten newly discovered vulnerabilities per day in 2011 (McAfee report, 2012; NIST-NVD, 2013).

A security patch is a program for fixing bugs in information systems. Currently, patching is a major remediation process for controlling security risks. Understanding patch management as a continuous vulnerability management process to maintain system reliability is critical. A vulnerability caused by insecure software has a life cycle, which includes the introduction, discovery, private exploitation, disclosure, public exploitation, patch release, patch testing, and patch deployment phases (Okhravi & Nicol, 2008). Among the given eight phases, some studies focus on the time gap between a software vendor’s patch release and a firm’s patch deployment. Because of the burden of operational risks and managerial costs of patching (Shostack, 2003), asynchronous patch updating is common (Cavusoglu, Cavusoglu, & Zhang, 2004). Many systems have been left unpatched for months and even years (Shostack, 2003). More recently, periodic patching became a common trend (Cavusoglu, Cavusoglu, & Zhang, 2008). Nearly half of the midsized companies applied patches monthly, and one-third did it on a weekly basis (McAfee report, 2012).

Patch management became a strategic decision to balance security risks and operational costs. However, there is a lack of quantitative security models to find the optimal equilibrium or managerial implications. Studies have shown that a more quantitative approach to the security attributes that satisfy quality-of-service (QoS) requirements, such as reliability, availability, and performance, is needed (Madan, Goševa-Popstojanova, Vaidyanathan, & Trivedi, 2004).

In the following discussion, we develop and present a formal framework for modeling the states of the patch management process and develop metrics that, to our knowledge, are novelties in this area. Similar works along the same vein are on vulnerability discovery modeling (Alhazmi & Malaiya, 2005), on patch management evaluation (Okhravi & Nicol, 2008), on the impact of vulnerability disclosure and patch availability (Arora, et al., 2004), on stochastic activity networks (Sanders & Meyer, 2002), and on patch management practices (Gerace & Cavusoglu, 2005; Gerace & Cavusoglu, 2009; Chan, 2004).

**Markov Chain Model**

There are two key mathematical concepts in this paper: the Markov Chain and the global balance equation. A Markov process is a stochastic process that has a dynamic behavior and whose probability distributions for its future developments depend only on the present state (Trivedi, 2002). A Discrete Time Markov Chain (DTMC) is a Markov process that has discrete state spaces and discrete parameters. A Continuous Time Markov Chain (CTMC) is a Markov process that has discrete state spaces; however, unlike DTMC, the transition from state to state can occur at any instant in time.

The global balance equations, also known as full balance equations (Kelly, 1979), are a set of equations that, in principle, can always be solved to give the equilibrium distribution of a Markov chain (when such a distribution exists). For a Markov chain with state space S, the transition rate from state i to j is given by \( q_{ij} \), and the equilibrium distribution is given by \( \pi \). The global balance equations are given for every state i in S, as shown by Chandy (1972), as follows:

\[
\sum_{j \in S \setminus \{i\}} \pi_j q_{ji} = \sum_{j \in S \setminus \{i\}} \pi_i q_{ij}
\]  

(1)
Related Content

Reservation MAC protocols for Ad-Hoc Networks: Analysis of the Approaches
[www.irma-international.org/article/reservation-mac-protocols-hoc-networks/3885/](www.irma-international.org/article/reservation-mac-protocols-hoc-networks/3885/)

Resource Management of Multicast Services Over LTE
Giuseppe Araniti, Massimo Condoluci and Antonella Molinaro (2014). *Convergence of Broadband, Broadcast, and Cellular Network Technologies* (pp. 77-93).
[www.irma-international.org/chapter/resource-management-of-multicast-services-over-lte/108089/](www.irma-international.org/chapter/resource-management-of-multicast-services-over-lte/108089/)

Diffusion Forecasting and Price Evolution of Broadband Services in Europe
[www.irma-international.org/chapter/diffusion-forecasting-price-evolution-broadband/20472/](www.irma-international.org/chapter/diffusion-forecasting-price-evolution-broadband/20472/)

Sensing Orders in Multi-User Cognitive Radio Networks
[www.irma-international.org/chapter/sensing-orders-in-multi-user-cognitive-radio-networks/123567/](www.irma-international.org/chapter/sensing-orders-in-multi-user-cognitive-radio-networks/123567/)

Mobile Agent Based Enhanced Security for Wireless Sensor Networks