Reliability Engineering and System Safety 133 (2015) 275–299

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress

Analysis of information security reliability: A tutorial

Suleyman Kondakci *

Faculty of Engineering & Computer Sciences, Izmir University of Economics, Sakarya Cad. No. 156, 35330 Balcova-Izmir, Turkey

ARTICLE INFO

Article history:
Received 24 January 2014
Received in revised form
15 August 2014
Accepted 21 September 2014
Available online 30 September 2014

Keywords:
Availability modeling
Reliability
Security
Risk assessment

ABSTRACT

This article presents a concise reliability analysis of network security abstracted from stochastic modeling, reliability, and queuing theories. Network security analysis is composed of threats, their impacts, and recovery of the failed systems. A unique framework with a collection of the key reliability models is presented here to guide the determination of the system reliability based on the strength of malicious acts and performance of the recovery processes. A unique model, called Attack-obstacle model, is also proposed here for analyzing systems with immunity growth features. Most computer science curricula do not contain courses in reliability modeling applicable to different areas of computer engineering. Hence, the topic of reliability analysis is often too diffuse to most computer engineers and researchers dealing with network security. This work is thus aimed at shedding some light on this issue, which can be useful in identifying models, their assumptions and practical parameters for estimating the reliability of threatened systems and for assessing the performance of recovery facilities. It can also be useful for the classification of processes and states regarding the reliability of information systems. Systems with stochastic behaviors undergoing queue operations and random state transitions can also benefit from the approaches presented here.

1. Introduction

One of the major reasons for developing concrete theories is to enhance their practical applicability to some desired technology and engineering fields. Our objective here is to find an efficient way of bringing parts from reliability theory into a practical technique for the analysis of information security. As known, the main objective of information security relies on the provision of the general triad called CIA, *Confidentiality*, *Integrity*, and *Availability*. Within this context, availability (as a measure of service degradation) is the most critical factor that can cause immense cost on the communication infrastructure and on general business outcomes. We usually have effective protection mechanisms for providing confidentiality and integrity. However, protecting from threats causing unavailability is more complex and often requires additional mechanisms (e.g., redundant or standby systems), which may also be under the same type of threats leading to additional losses.

Building reliable models for analyzing failures and impacts caused by different threat types on information systems can be extremely complicated, or models to describe these processes may not even exist. Therefore, in order to achieve at least an analytical tractability, we need to separate the problem domain into three major parts: (i) attack and failure modeling, (ii) impact modeling, and (iii) recovery modeling. Theoretical approaches alone are often difficult to satisfy these with rapidly evolving IT systems and emerging networking concepts. Simulations and empirical studies are only devoted to observe and assess system behaviors in order to substantiate the reliability in practical situations. Theoretical models used for simulations and experiments need also be justified and matched to the well-established modes of operations. Probabilistic approaches can be used to build impact models and estimate the loss due to system failures caused by the threats with predefined probability and hazard distributions. Additionally, queuing theory and stochastic processes (e.g., Markov chains) can be used to guide stationary analysis of system failures and hazard functions together with the associated repair models.

The major problem for many information security engineers is as follows. Though theoretical frameworks are critical in guiding research, however, in some contexts, they can be confusing and much cumbersome to apply. Especially, for complex network structures facing complicated threat types, matching a theoretical security model to an overall analysis need to be inductive, tractable, explanatory, and well-thought to guide access to concretely measurable results obtained from many interrelated concepts and their influencing parameters. Reliability models dealing with complex systems are numerous, and naturally, some of them are too diffuse to some computer engineers to apply. As the complexity increases alongside with the drastically growing information systems' diversity, adapting a concrete model becomes

* Tel.: +90 232 488 8256.
E-mail address: suleyman.kondakci@ieu.edu.tr

http://dx.doi.org/10.1016/j.ress.2014.09.021
0951-8320/

more and more complicated. Therefore, obtaining practically sound reliability functions that can address different paths of a complex and redundant security structures are necessary.

The objective of this article is thus to present and discuss several useful reliability models dealing with the availability analysis of information systems. Two major reasons have triggered the development of this work: (1) lack of a holistic approach to network reliability analyses in the current literature and (2) to enhance the knowledge of formal reliability analysis in the computer engineering discipline. In fact, we find various work in the literature that mainly consider the analysis of singular systems, such as the analysis of a specific type of worm/virus propagation and analysis of software (SW) and hardware (HW) faults. With this work, we intend to bring front an umbrella framework that can facilitate the analysis of a broad spectrum of network structures, their components, interdependence among the interconnected structures, impacts (cost of service degradation) caused by the associated threats, and performance analysis of the facilities used to repair the threatened systems.

The second reason triggering this idea is such that the most of the universities and institutions around the world do not provide system reliability courses in their computer science departments. Thus, we have a good reason to provide the fundamental modeling approaches that are applicable to the analysis of various aspects of reliability and security of computer networks. This paper will therefore emphasize this issue by presenting a set of practical models derived from the reliability theory and queuing systems.

Obviously, complexity of the reliability models increases in parallel with the system complexity, which is then multiplied with the level of system redundancy, if implemented so. Communication networks, Internet search engines, cloud computing environments, smart grid networks, and resources of the grid networks are good examples of such a complexity that contain a high degree of redundancy and discrepancy in the overall system structure and the services provided by these globally distributed systems. Defining a separate reliability function for each subset of such conglomerate structures, and integrating them under a framework will always introduce additional complexities. Estimating the overall reliability of such a complex structure can be facilitated if we were able to get down to some concrete models from the theoretical reliability concepts. Accordingly, this paper is intended to provide a framework of models applicable to the reliability analysis of computer networks.

Primarily, we customize a set of functions and models from the reliability concept and lay down some model assumptions that are specific to the analysis of information security. An appropriate model can then be selected to determine system states as a metric reflecting the degree of the system availability. The results obtained can then be used for risk assessment of systems under different situations. Related to this, as a special case, we present a numerical analysis that determines the reliability measure of a network of susceptible computers, which are vulnerable to some virus attacks and software failures. A reliability measure is composed of a set of parameters, such as mean failure and recovery rates, total down times, service efficiency, and repairman utilization. Some systems may experience alternating states, while others experience increasing or decreasing failure states, depending on the cause of the failure or the efficiency of the recovery operations. That is, we will analyze time-dependent states of some suspected systems and determine expressions representing the failure and recovery rates of them as well as the stationary characteristic describing the long-run reliability figures of these systems. Accordingly, throughout the paper, we define an unreliable node as a repairable/renewable system since the node can be restored to operate after eventual failures.

1.1. Outline of the paper

Following the introduction and the objective of this work in Section 1, a brief review about the related work is given in Section 2. Section 3 describes the terminology used in this paper, presents a concise overview of the key reliability models, describes the failure sources (threats) and associated failures, presents the method for constructing reliability structures from network structures, and outlines the main steps of the reliability analysis used here. Section 4 summarizes the threat categories and tabulates the candidate reliability models for modeling attacks and failures. Assumptions and limitations regarding the discussed reliability models are presented in Section 5. Section 6 defines a new class of the reliability patterns associated to the reliability of networks security. Section 7 presents a detailed discussion of the reliability models and their applications to the analysis of network security threats and failures. Impact analysis of the threats is presented in Section 8. Section 9 presents models for describing and analyzing repair processes, service efficiency for recovery facilities, whereas Section 10 goes through a case study dealing with the recovery operations and service degradation caused by a virus infection scenario. A brief discussion on the presented material and the feature extension of the work is given in Section 11. Finally, a detailed background of the model theories is presented in Appendix A.

2. Related work

There exist numerous work being considered within the general context of the reliability engineering. However, it is hard to find approaches specific to the reliability analysis of network security. An earlier software failure analysis model was developed by [1], which presents a stochastic model for the software failure phenomenon based on a nonhomogeneous Poisson process. A service reliability approach for a distributed software is considered in [2], where a distributed system was modeled as a single service system shared by some distributed clients. This could be interpreted as a single service system shared among multiple customers using a control center that allows access for the client machines. The system availability of the control center is determined by the probability for itself to be available, which is also the overall reliability measure representing its clients. As known, wireless communication networks often have degraded throughput of broadcast packets due to the nature of the transmission characteristics. Related to this, a composite reliability analysis is given by [3], which illustrates three modeling approaches for composite performance and availability analysis. A high-level description language, stochastic reward net, and continuous time Markov chain are used to construct models for evaluating the performability measures of a channel allocation scheme in a wireless network. Service reliability in a grid system with star topology is considered by [4], and a topological view on the reliability of a large-scale distributed system is presented by [5]. One of the main objectives of our work is to facilitate the quantitative reliability analysis of interconnected systems. Wherever applicable, a candidate model defined here will embody the fundamental steps for assessing information security risks of a given network. The selection of the candidate model depends basically on the underlying assumptions for the applicability of the model to the network under consideration.

Reliability engineering covering various types of system safeties encompasses a wide spectrum of theoretical areas, each of which needs a closer look for accurate adaptation to more specific engineering problems. Therefore, the discussion taken here can be considered as a dedicated focus on the information security compared to that of