Advances in Intelligent Systems and Computing 286

Wojciech Zamojski · Jacek Mazurkiewicz
Jarosław Sugier · Tomasz Walkowiak
Janusz Kacprzyk *Editors*

Proceedings of the Ninth International Conference on Dependability and Complex Systems DepCoS-RELCOMEX. June 30 – July 4, 2014, Brunów, Poland

Springer

Advances in Intelligent Systems and Computing

Volume 286

Series editor

Janusz Kacprzyk, Polish Academy of Sciences, Warsaw, Poland
e-mail: kacprzyk@ibspan.waw.pl

For further volumes:
http://www.springer.com/series/11156

About this Series

The series "Advances in Intelligent Systems and Computing" contains publications on theory, applications, and design methods of Intelligent Systems and Intelligent Computing. Virtually all disciplines such as engineering, natural sciences, computer and information science, ICT, economics, business, e-commerce, environment, healthcare, life science are covered. The list of topics spans all the areas of modern intelligent systems and computing.

The publications within "Advances in Intelligent Systems and Computing" are primarily textbooks and proceedings of important conferences, symposia and congresses. They cover significant recent developments in the field, both of a foundational and applicable character. An important characteristic feature of the series is the short publication time and world-wide distribution. This permits a rapid and broad dissemination of research results.

Advisory Board

Wojciech Zamojski · Jacek Mazurkiewicz
Jarosław Sugier · Tomasz Walkowiak
Janusz Kacprzyk
Editors

Proceedings of the Ninth International Conference on Dependability and Complex Systems DepCoS-RELCOMEX. June 30 – July 4, 2014, Brunów, Poland

Springer

Editors
Wojciech Zamojski
Institute of Computer Engineering, Control and Robotics
Wrocław University of Technology
Wrocław
Poland

Jacek Mazurkiewicz
Institute of Computer Engineering, Control and Robotics
Wrocław University of Technology
Wrocław
Poland

Jarosław Sugier
Institute of Computer Engineering, Control and Robotics
Wrocław University of Technology
Wrocław
Poland

Tomasz Walkowiak
Institute of Computer Engineering, Control and Robotics
Wrocław University of Technology
Wrocław
Poland

Janusz Kacprzyk
Polish Academy of Sciences
Systems Research Institute
Warsaw
Poland

ISSN 2194-5357 ISSN 2194-5365 (electronic)
ISBN 978-3-319-07012-4 ISBN 978-3-319-07013-1 (eBook)
DOI 10.1007/978-3-319-07013-1
Springer Cham Heidelberg New York Dordrecht London

Library of Congress Control Number: 2014939038

Preface

We are pleased to present the proceedings of the Ninth International Conference on Dependability and Complex Systems DepCoS-RELCOMEX, which took place in a beautiful Brunów Palace, Poland, from 30^{th} June to 4^{th} July, 2014.

Started in 2006, DepCoS – RELCOMEX is a conference organized annually by the Institute of Computer Engineering, Control and Robotics (CECR) from Wrocław University of Technology. Its roots go nearly 40 years back to the heritage of the other two cycles of events: RELCOMEX (1977 – 89) and Microcomputer Schools (1985 – 95) which were organized by the Institute of Engineering Cybernetics (the previous name of CECR) under the leadership of prof. Wojciech Zamojski, now also the DepCoS chairman. In this volume of "Advances in Intelligent and Soft Computing" we would like to present results of research on selected problems of complex systems and their dependability. Effects of the previous DepCoS events were published in volumes 97, 170 and 224 of this series.

Today's complex systems are integrated unities of technical, information, organization, software and human (users, administrators and management) resources. Complexity of such systems comes not only from their involved technical and organizational structures built on hardware and software resources but mainly from complexity of information processes (processing, monitoring, management, etc.) realized in their specific environment. In operation of such wide-ranging and diverse systems their resources are dynamically allocated to ongoing tasks and the rhythm of system events (incoming and/or ongoing tasks, decisions of a management subsystem, system faults, "defense" system reactions, etc.) may be considered as deterministic or/and probabilistic event stream. Security and confidentiality of information processing introduce further complications into the modelling and evaluation methods. Diversity of the processes being realized, their concurrency and their reliance on in-system intelligence often significantly impedes construction of strict mathematical models and calls for application of intelligent and soft computing methods.

Dependability is the modern approach to reliability problems of contemporary complex systems. It is worth to underline the difference between the two terms: system dependability and system reliability. Dependability of systems, especially

computer systems and networks, is based on multi-disciplinary approach to theory, technology, and maintenance of the systems working in a real (and very often unfriendly) environment. Dependability concentrates on efficient realization of tasks, services and jobs by a system considered as a unity of technical, information and human assets, while "classical" reliability is more restrained to analysis of technical system resources (components and structures built from them).

Presenting our conference proceedings to the broader audience we would like to express the sincerest thanks to all the authors who have chosen to describe their research here. It is our hope that the communicated results will help in further developments in complex systems design and analysis aimed at improving their dependability. We believe that the selected contributions will be interesting to all scientists, researchers, practitioners and students who work in these fields of science.

Concluding this brief introduction we must emphasize the role of all reviewers who took part in the evaluation process and whose contribution helped to refine the contents of this volume. Our thanks go to, in alphabetic order, Salem Abdel-Badeeh, Andrzej Białas, Frank Coolen, Manuel Gil Perez, Zbigniew Huzar, Jacek Jarnicki, Vyacheslav Kharchenko, Mieczysław M. Kokar, Alexey Lastovetsky, Marek Litwin, Jan Magott, István Majzik, Jacek Mazurkiewicz, Katarzyna M. Nowak, Yiannis Papadopoulos, Oksana Pomorova, Krzysztof Sacha, Ruslan Smeliansky, Janusz Sosnowski, Jarosław Sugier, Victor Toporkov, Carsten Trinitis, Tomasz Walkowiak, Max Walter, Bernd E. Wolfinger, Marina Yashina, Irina Yatskiv, Wojciech Zamojski, and Włodzimierz Zuberek.

The Editors

Ninth International Conference on Dependability and Complex Systems DepCoS-RELCOMEX

organized by

Institute of Computer Engineering, Control and Robotics,
Wrocław University of Technology
under the auspices of prof. Tadeusz Więckowski, Rector

Brunów Palace, Poland, June 30 – July 4, 2014

Programme Committee

Wojciech Zamojski (Chairman)	Wrocław University of Technology, Poland
Salem Abdel-Badeeh	Ain Shams University Abbasia, Cairo, Egypt
Ali Al-Dahoud	Al-Zaytoonah University, Amman, Jordan
George Anders	University of Toronto, Canada
Artem Adzhemov	Technical University of Communications and Informatics, Moscow, Russia
Włodzimierz M. Barański	Wrocław University of Technology, Poland
Andrzej Białas	Institute of Innovative Technologies EMAG, Katowice, Poland
Dariusz Caban	Wrocław University of Technology, Poland
Krzysztof Cios	Virginia Commonwealth University, Richmond, USA
Frank Coolen	Durham University, UK
Antonio Ferrari	University of Aveiro, Portugal
Francesco Flammini	University of Naples "Federico II", Napoli, Italy
Manuel Gill Perez	University of Murcia, Spain
Janusz Górski	Gdansk University of Technology, Poland
Zbigniew Huzar	Wrocław University of Technology, Poland
Igor Kabashkin	Transport and Telecommunication Institute, Riga, Latvia
Janusz Kacprzyk	Polish Academy of Sciences, Warsaw, Poland
Andrzej Kasprzak	Wrocław University of Technology, Poland
Vyacheslav S. Kharchenko	National Aerospace University "KhAI", Kharkov, Ukraine
Mieczysław M. Kokar	Northeastern University, Boston, USA
Krzysztof Kołowrocki	Gdynia Maritime University, Poland
Leszek Kotulski	AGH University of Science and Technology, Krakow, Poland
Henryk Krawczyk	Gdansk University of Technology, Poland

Organizing Committee

Contents

Erratum

Web Systems Availability Assessment Considering Attacks on Service Configuration Vulnerabilities

Vyacheslav Kharchenko[1,2], Alaa Mohammed Abdul-Hadi[1], Artem Boyarchuk[1], and Yurij Ponochovny[3]

[1] National Aerospace University KhAI, Kharkiv, Ukraine
[2] Centre of Safety Infrastructure-Oriented Research and Analysis, Kharkiv, Ukraine
V.Kharchenko@khai.edu
[3] Poltava National Technical University named after Yurij Kondratyuk, Poltava, Ukraine
pnch1@rambler.ru

Abstract. The paper examines the issues of web systems assessment availability. It is defined that unavailability of web services may be caused by internal and external factors in particular server side vulnerability attacks. Three Markov's models of web system availability are developed; these models consider influence of software defects and vulnerability attacks for DNS, DHCP and Route services. Elimination of configuration vulnerabilities during system operation is considered. Conclusions about the impact of the probability of detection and elimination of vulnerabilities and the recovery rate on the web systems availability function are proposed.

Keywords: web system availability, Markov's models, attacks on vulnerability services.

1 Introduction

The successful beginning and operation of web systems is only possible in case of payback on their functioning and positive profit earning. The break-even point is reached after the start of system exploitation, and it might not be achieved at all if risk assessment was wrong. This leads to the importance of modeling the functioning of web systems based on actual cyber security risks [1-3].

Nowadays, most web services experienced the attacks of various kinds. With regard to commercial Web services, they certainly are the most attractive target for attacks [1, 4]. In such circumstances, modeling of web attacks as events that lead to their inaccessibility is in high demand. However, today the majority of the models of attacks, threats and incidents have probabilistic nature of risk assessment. Only some sources refer to the possibility of web system modeling using semi-Markov processes and Petri nets [5].

The modern web system is a complex multileveled and distributed system. It can be presented by the charts with various hierarchy levels. This paper discusses the three-component reliability block diagram of the web system (RBD). It describes the interaction of basic services: IP-address assignment (DHCP), IP routing (Route) and support the direct and inverse transformation of text URLs to IP-addresses (DNS).

W. Zamojski et al. (eds.), *Proceedings of the Ninth International Conference DepCoS-RELCOMEX*, Advances in Intelligent Systems and Computing 286,
DOI: 10.1007/978-3-319-07013-1_26,

This decision is due to the fact that vulnerability subsets of mentioned services might be distinguished in line with CVE classifiers [6,7]. This allows getting estimates of the intensity of attacks and their criticality [8].

Unavailability of any of these services entails the refusal in customer service. On this basis, the RBD will include three consecutive elements, each of which corresponds the up-states of three services (fig.1).

Fig. 1. Reliability block diagram of web system

While assessing web systems availability the focus is given on Markov's models based on hardware and software failures (caused by physical and design faults correspondingly) and recoveries [9, 10]. Researches [11, 12] analyze the concept of an integrated approach of dependability as a property which combine in particular reliability, availability and information security. In [13] the possibility of the development of mathematical models that consider the unavailability of web systems in context security is proposed. Unavailability is caused by not only by software faults, but by attacks on their components as well.

The objective of this paper is to develop Markov models of web systems availability considering attacks, and to investigate the impact of input parameters of the model to the availability function. First of all, we research behavior of web systems in non-stationary modes taking into account various kinds of attacks and recovery procedures. The paper is structured as follows: the second section describes the simple Markov models of web-services without attacks (MA1) and with mechanism for restart after attack (MA2). The third section describes the MA3 model used for assessment of web-service availability considering consequent fixing of vulnerabilities after attacks. Verification results and case study of developed models are presented in the fourth and fifth sections. The last section includes the conclusions and directions of future work.

2 Availability Models of Web Systems without Attacks and with System Restart after Attack

2.1 Model MA1

We consider an ideal web system model without attacks as a basic model in which there are processes of software failures and recoveries of related network services (MA1). Resulting characteristics of such model often are used by hosting providers as the availability and uptime rate of hosting platforms.

Marked graph of states and transitions of such model is shown at the fig.2,a. It includes initial up-state S0 and down-states S1, S2 and S3. The transitions into down-states are marked with the corresponding failure rates (ladns, ladhcp and laroute). System returns into up-state after service recovery with corresponding rates mudns, mudhcp and muroute.

Author Index