

Accepted Manuscript

Empirical analysis of attack graphs for mitigating critical paths and vulnerabilities

Urvashi Garg , Geeta Sikka , Lalit K. Awasthi

PII: S0167-4048(18)30349-3
DOI: [10.1016/j.cose.2018.04.006](https://doi.org/10.1016/j.cose.2018.04.006)
Reference: COSE 1328



To appear in: *Computers & Security*

Received date: 18 October 2017
Revised date: 30 January 2018
Accepted date: 7 April 2018

Please cite this article as: Urvashi Garg , Geeta Sikka , Lalit K. Awasthi , Empirical analysis of attack graphs for mitigating critical paths and vulnerabilities, *Computers & Security* (2018), doi: [10.1016/j.cose.2018.04.006](https://doi.org/10.1016/j.cose.2018.04.006)

This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.

Empirical analysis of attack graphs for mitigating critical paths and vulnerabilities

Corresponding author:

Ms. Urvashi Garg

Department of Computer Science & Engineering,

Dr. B. R. Ambedkar National Institute of Technology, Jalandhar, Punjab, India - 144011

Phone: +91-8968522600

Fax: not available

E-mail: urvashi.garg.24@gmail.com

Co-authors:

Dr. Geeta Sikka

Department of Computer Science & Engineering,

Dr. B. R. Ambedkar National Institute of Technology, Jalandhar, Punjab, India - 144011

Phone: +91-9888582299

Fax: not available

E-mail: sikkag@gmail.com

Prof. Lalit K. Awasthi

Dr. B. R. Ambedkar National Institute of Technology, Jalandhar, Punjab, India - 144011

Phone: +91-181-2690802 (O)

Fax: +91-181-2690932

E-mail: lalitdec@gmail.com

Abstract

The proliferated complexity of network size together with the expeditious development of software applications and their numerous vulnerabilities, security hardening is becoming a considerable challenge for security experts. Although various techniques were already present till date for security analysis, the majority of works focused on individual vulnerability analysis. Attackers do not necessarily compromise a single vulnerability on only one machine, but they can continue exploiting other vulnerabilities by using the resources of the compromised machine. Individual vulnerability analysis may not work well in such situations. This paper bridges the gap between chained vulnerabilities and their analysis. In this work, we have developed a methodology to prioritize individual vulnerability as well as attack paths. The existing CVSS score based scheme has been modified to calculate risk score of individual vulnerability considering all three metrics i.e. base metrics, temporal metrics and environmental metrics of CVSS in conjunction. Finally, Page rank model was used to prioritize attack paths. The results were verified by applying Markov

Download English Version:

<https://daneshyari.com/en/article/6883871>

Download Persian Version:

<https://daneshyari.com/article/6883871>

[Daneshyari.com](https://daneshyari.com)