Author's Accepted Manuscript

www.elsevier.com/locate/ress

Multiple Cyber Attacks Against a Target with Observation Errors and Dependent Outcomes: Characterization and Optimization

Xiaoxiao Hu, Maochao Xu, Shouhuai Xu, Peng Zhao

PII: S0951-8320(16)30723-2
DOI: http://dx.doi.org/10.1016/j.ress.2016.10.025
Reference: RESS5672

To appear in: *Reliability Engineering and System Safety*

Received date: 22 February 2016
Revised date: 3 October 2016
Accepted date: 30 October 2016

Cite this article as: Xiaoxiao Hu, Maochao Xu, Shouhuai Xu and Peng Zhac Multiple Cyber Attacks Against a Target with Observation Errors and Dependen Outcomes: Characterization and Optimization, *Reliability Engineering an System Safety,* http://dx.doi.org/10.1016/j.ress.2016.10.025

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

ACCEPTED MANUSCRIPT

Multiple Cyber Attacks Against a Target with Observation Errors and Dependent Outcomes: Characterization and Optimization

Xiaoxiao Hu[⋆] Maochao Xu[†] Shouhuai Xu[‡] Peng Zhao[⋆⋆]

[⋆] School of Mathematics and Statistics, Lanzhou University, China
[†] Department of Mathematics, Illinois State University, USA
[‡] Department of Computer Science, University of Texas at San Antonio, USA
[⋆⋆] School of Mathematics and Statistics, Jiangsu Normal University, China [*]

Abstract

In this paper we investigate a cybersecurity model: An attacker can launch multiple attacks against a target with a *termination strategy* that says that the attacker will stop after observing a number of successful attacks or when the attacker is out of attack resources. However, the attacker's observation of the attack outcomes (i.e., random variables indicating whether the target is compromised or not) has an observation error that is specified by both a false-negative and a false-positive probability. The novelty of the model we study is the accommodation of the *dependence* between the attack outcomes, because the dependence was assumed away in the literature. In this model, we characterize the monotonicity and bounds of the compromise probability (i.e., the probability that the target is compromised). In addition to extensively showing the impact of dependence on quantities such as compromise probability and attack cost, we give methods for finding the optimal strategy that leads to maximum compromise probability or minimum attack cost. This study highlights that the dependence between random variables cannot be assumed away, because the results will be misleading.

Key words: Copula; Cybersecurity; Defense; Optimal strategy.

Accepted manuscript

[*]Corresponding author. Email: zhaop@jsnu.edu.cn

Download English Version:

https://daneshyari.com/en/article/5019608

Download Persian Version:

https://daneshyari.com/article/5019608

Daneshyari.com