Accepted Manuscript

Title: Multi-source fusion based security detection method for heterogeneous networks

Author: Hao Wu, Zhonghua Wang

PII: S0167-4048(18)30006-3
DOI: https://doi.org/10.1016/j.cose.2018.01.003
Reference: COSE 1265

To appear in: *Computers & Security*

Received date: 17-5-2017
Revised date: 16-11-2017
Accepted date: 2-1-2018

Please cite this article as: Hao Wu, Zhonghua Wang, Multi-source fusion based security detection method for heterogeneous networks, *Computers & Security* (2018), https://doi.org/10.1016/j.cose.2018.01.003.

Multi-Source Fusion Based Security Detection Method for Heterogeneous Networks

Hao Wu, Zhonghua Wang

Hao Wu is with Research institute, CNCERT/CC, Beijing 100029, China. Fax: 8601082990375. Corresponding author, emails: whman@isc.org.cn, wuhao@cert.org.cn.

Zhonghua Wang is with Research institute, CNCERT/CC, Beijing 100029, China. Emails: wzh@cert.org.cn.

Hao Wu was born in Shandong, China, in 1985. He received the Bachelor and Ph.D. degrees in mathematics and automation from the Shandong University and Tsinghua University, China, in 2008 and 2014, respectively. Since 2014, he has been a senior engineer with the network information security institute of CNCERT/CC. His research interests lie in the areas of intrusion detection, IoT security and state estimation.

Zhonghua Wang was born in Shandong, China, in 1986. He received the Bachelor and Ph.D. degrees in electronics and communication engineering from the Harbin Institute of Technology and Peking University, China, in 2008 and 2013, respectively. Since 2013, he has been an engineer with the network information security institute of CNCERT/CC. His research is mainly on intrusion detection, network attack and defense technology.

Abstract

In this paper, multi-source fusion based detection method for the security of heterogeneous network is investigated. Fusion based detection method exploits multi-source profiles from the whole network to make decisions on whether intrusion incident happens. A game theoretic analysis method for the concerned detection strategy is presented, where the attacker and defender are thought to be rational humans and they always try their best to get their maximum payoffs. A nonzero-sum game model is established to formulate the confrontation between the defender and attacker by considering the detection threshold and attack resource allocation as their strategies. The optimal strategies are then solved by using Nash equilibrium theory. The local optimal attack allocation scheme is firstly presented for heterogeneous network, which shows that with limited resources the attacker should only launch attacks to more valuable nodes and more attack resources should be allocated to more valuable nodes also. Then a general conclusion about the existence of the Nash equilibrium is given, which indicates that the Nash