Identifying Passive Message Fingerprint Attacks via Honey Challenge in Collaborative Intrusion Detection Networks

To enhance the detection capability of a single intrusion detection system (IDS), collaborative intrusion detection networks (CIDNs) have been exploited and developed via enabling a set of IDS nodes to exchange information with each other. In CIDNs, challenge-based trust mechanism has been considered as one promising solution to identify malicious nodes by evaluating the satisfaction levels between challenges and responses. However, such mechanism is still vulnerable to some advanced insider attacks like passive message fingerprint attack (PMFA), which is deemed as an advanced attack on challenge-based CIDNs by collecting messages and identifying normal requests in a passive way. In this work, we focus on PMFA and design Honey Challenge, an improved challenge mechanism for challenge-based CIDNs characterized by sending challenges in a similar way of sending normal requests, in such a way malicious nodes cannot accurately identify the normal requests. In the evaluation, we investigate the attack performance under both simulated and real network environments. Experimental results demonstrate that our proposed mechanism can identify malicious nodes under PMFA and decrease their trust values in a quick manner.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cyber Security, City University of Hong Kong, Guangzhou University, University of New Brunswick
Contributors: Li, W., Meng, W., Wang, Y., Kwok, L. F., Lu, R.
Pages: 1208-1213
Publication date: 5 Sep 2018

Host publication information
Title of host publication: Proceedings of 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications and 12th IEEE International Conference on Big Data Science and Engineering, Trustcom/BigDataSE 2018
Publisher: IEEE
Article number: 8456036
ISBN (Print): 9781538643877
Keywords: Challenge-based Mechanism, Collaborative Environment, Insider Threat, Intrusion Detection, Passive Message Fingerprint Attack, Trust Computation
DOIs: 10.1109/TrustCom/BigDataSE.2018.00167
Source: Scopus
Source-ID: 85054099374
Research output: Research - peer-review > Article in proceedings – Annual report year: 2018