Designing collaborative blockchained signature-based intrusion detection in IoT environments - DTU Orbit (05/05/2019)

Designing collaborative blockchained signature-based intrusion detection in IoT environments
With the rapid development of Internet-of-Things (IoT), there is an increasing demand for securing the IoT environments. For such purpose, intrusion detection systems (IDSs) are one of the most important security mechanisms, which can help defend computer networks including IoT against various threats. In order to achieve better detection performance, collaborative intrusion detection systems or networks (CIDSs or CIDNs) are often adopted in a practical scenario, allowing a set of IDS nodes to exchange required information with each other, e.g., alarms, signatures. However, due to the distributed nature, such kind of collaborative network is vulnerable to insider attacks, i.e., malicious nodes can generate untruthful signatures and share to normal peers. This may cause intruders to be undetected and greatly degrade the effectiveness of IDSs. With the advent of blockchain technology, it provides a way to verify shared signatures (rules). In this work, our motivation is to develop CBSigIDS, a generic framework of collaborative blockchained signature-based IDSs, which can incrementally build and update a trusted signature database in a collaborative IoT environment. CBSigIDS can provide a verifiable manner in distributed architectures without the need of a trusted intermediary. In the evaluation, our results demonstrate that CBSigIDS can enhance the robustness and effectiveness of signature-based IDSs under adversarial scenarios.

General information
Publication status: Published
Organisations: Department of Applied Mathematics and Computer Science, Cyber Security, City University of Hong Kong, Technical University of Denmark, Guangzhou University
Corresponding author: Meng, W.
Contributors: Li, W., Tug, S., Meng, W., Wang, Y.
Pages: 481-489
Publication date: 1 Jul 2019
Peer-reviewed: Yes

Publication information
Journal: Future Generation Computer Systems
Volume: 96
ISSN (Print): 0167-739X
Ratings:
BFI (2019): BFI-level 1
Web of Science (2019): Indexed yes
Original language: English
Keywords: Blockchain technology, Collaborative network, Insider attacks, Internet-of-Things, Intrusion detection system, Signature-based detection
DOIs:
10.1016/j.future.2019.02.064
Source: Scopus
Source-ID: 85062284371
Research output: Contribution to journal › Journal article – Annual report year: 2019 › Research › peer-review