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.