Distributed intrusion detection trust management through integrity and expertise evaluation

Abstract

Information sharing and collaboration has facilitated decision accuracy and reaction time in many applications. Distributed Intrusion Detection Systems (DIDS) solutions are one of such applications that have dramatically been transformed. This is mainly due to increasing number of attacks as well as sophisticated nature of today's intrusions. Moreover, it has been shown that various critical components of a system can be targeted. This is further exasperated by the fact that most DIDS models do not consider attacks that targets the collaborative network itself. We specifically find this issue to be very critical and hence in this paper we propose a trust aware DIDS simulation model that is capable of categorizing each participating IDS expertise (i.e. speciality and competence), therefore helps collaborating organizations to consult our simulation model for choosing the right candidate for any type of intrusion. We call our proposed DIDS model Consultative Trusted Computing-based Collaborative IDS (CTC IDS). We utilize the Trusted Platform Module (TPM) for integrity evaluation and to fine-tune peer evaluation.