Zeeshan Afzal, Karlstad University

Title:
Automated Testing of IDS Rules

Abstract:
As technology becomes ubiquitous, new vulnerabilities are being discovered at a rapid rate. The security experts continuously find ways to detect the attempts to exploit those vulnerabilities. The outcome is a huge and complex rule set used by Intrusion Detection Systems (IDSs) to detect and prevent the vulnerabilities. The rule sets have grown so much over the years that it has become infeasible to verify their accuracy or identify overlapping rules. This presentation will discuss a proposed methodology consisting of a set of tools that will make rule management easier.