Quantitative Verification and Synthesis of Attack-Defence Scenarios

Attack-defence trees are a powerful technique for formally evaluating attack-defence scenarios. They represent in an intuitive, graphical way the interaction between an attacker and a defender who compete in order to achieve conflicting objectives. We propose a novel framework for the formal analysis of quantitative properties of complex attack-defence scenarios, using an extension of attack-defence trees which models temporal ordering of actions and allows explicit dependencies in the strategies adopted by attackers and defenders. We adopt a game-theoretic approach, translating attack-defence trees to two-player stochastic games, and then employ probabilistic model checking techniques to formally analyse these models. This provides a means to both verify formally specified security properties of the attack-defence scenarios and, dually, to synthesise strategies for attackers or defenders which guarantee or optimise some quantitative property, such as the probability of a successful attack, the expected cost incurred, or some multi-objective trade-off between the two. We implement our approach, building upon the PRISM-games model checker, and apply it to a case study of an RFID goods management system.