Automated Generation of Attack Trees

Attack trees are widely used to represent threat scenarios in a succinct and intuitive manner, suitable for conveying security information to non-experts. The manual construction of such objects relies on the creativity and experience of specialists, and therefore it is error-prone and impracticable for large systems. Nonetheless, the automated generation of attack trees has only been explored in connection to computer networks and leveraging rich models, whose analysis typically leads to an exponential blow-up of the state space. We propose a static analysis approach where attack trees are automatically inferred from a process algebraic specification in a syntax-directed fashion, encompassing a great many application domains and avoiding incurring systematically an exponential explosion. Moreover, we show how the standard propositional denotation of an attack tree can be used to phrase interesting quantitative problems, that can be solved through an encoding into Satisfiability Modulo Theories. The flexibility and effectiveness of the approach is demonstrated on the study of a national-scale authentication system, whose attack tree is computed thanks to a Java implementation of the framework.