UNIVERZITA KOMENSKÉHO FAKULTA MATEMATIKY, FYZIKY A INFORMATIKY

Abstract (EN):

Attack trees are formal model and analysis techniques that are used to study the potential threats in various kinds of systems. In this thesis, we work with attack trees as a modeling formalism to analyse the security challenges of systems, against different attack scenarios. We proposed different extensions and variants of attack trees to analyse complex attackers models. We also proposed ways to translate the attack trees into automata models, and then use a software tool to perform model checking of security properties. Additionally, we combine attack trees with an information security property named opacity in order to study eavesdropping attacks - which is impossible to model using attack trees.

Our contributions in this thesis include the introduction of protection nodes in attack trees. This enables us to model possible defence against attackers actions at the leaves level of the tree. We also proposed dynamic trees that can be used to model and analyse systems with dynamic threat environments. In addition to extending the set of actions that denote the basis of attack with time durations, we also introduced timed constraints that characterize the validity/success of an attack at the set of gates of the trees. We then show how to use the concept of opacity to determine whether an attacker can uncover some hidden states of a system - which are not visible by observing the system's weak points. This is translated to checking current state opacity on the system model. Furthermore, we introduced reversible attack trees, as a variant of attack trees for which an ongoing attack can be fully or partially reset to the original state of the trees (system).