Automating Cyber Defence Responses Using Attack-Defence Trees and Game Theory

Ravi Jhawar[1], Sjouke Mauw[1] and Irfan Zakiuddin[2]
[1]Interdisciplinary Centre for Security, Reliability and Trust, University of Luxembourg, Luxembourg
[2]Noumena Research Ventures Ltd., UK
ravi.jhawar@uni.lu
sjouke.mauw@uni.lu
noumena.research.ventures@gmail.com

Abstract: Cyber systems that serve government and military organizations must cope with unique threats and powerful adversaries. In this context, one must assume that attackers are continuously engaged in offence and an attack can potentially escalate in a compromised system. This paper proposes an approach to generate defensive responses against on-going attacks. We use Attack-Defence Trees (ADTrees) to represent situational information including the state of the system, potential attacks and defences, and the interdependencies between them. Currently, ADTrees do not support automated response generation. To this end, we develop a game-theoretic approach to calculate defensive responses and implement our approach using the Game Theory Explorer (GTE). In our games, Attackers and Defenders are the players, the pay-offs model the benefit to each player for a given course of action, and the game's equilibria is the optimal course of action for each player. Finally, given the dynamic nature of cyber systems, we keep our ADTrees and the corresponding game trees up-to-date following the well-known OODA (observe, orient, decide, act) loop methodology.

Keywords: cyber defences, attack modelling, game theory, security, incident response

1. Introduction

Cyber systems are becoming highly complex with ever-increasing dependencies both internally as well as with strategic partners and commercial service providers. Military organizations and critical businesses are also relying heavily on such cyber systems to meet their operational demands and to support mission execution. At the same time, cyber attacks are becoming stealthy and sophisticated, posing potentially very high damaging impact. In this context, a holistic framework for responding to cyber attacks becomes essential and it must encompass several functions including:

- efficient collection of cyber situational information,
- analysis of possible attacks,
- determining the courses of actions in response, and
- taking the appropriate actions.

This paper focuses mainly on the 'determining the courses of actions in response' component of a deployed cyber system. We assume that situational information including the system state and parameters, and attack and defence related information is available. In this work, we systematically represent the situational information using Attack-Defence Trees (ADTrees) (Kordy, Mauw, & Radomirovic, Attack-defence trees, 2014). ADTrees improve the widely used attack trees formalism, by including not only the actions of an attacker, but also possible counteractions of a defender. The root node in an ADTree represents the attacker's (or defender's) goal and the children of a given node represents its refinement into sub-goals. Each node can have one child of the opposite type, representing the node's counteraction, which can be refined and countered again. The leaves of an ADTree represent the basic actions of an agent, which need not be refined any further.

Formally, ADTrees extend the formalism of defence trees (Bistarelli, Fioravanti, & Peretti, 2006), where defensive measures are not refined and can only be attached to leaf nodes. ADTrees can also be seen as merging attack trees and protection trees (Edge, Dalton, Raines, & Mills, 2006) into one formalism. Protection trees are AND-OR trees depicting how defensive measures can be refined into simple actions. Given the high expressivity and intuitiveness of ADTrees, complemented with strong mathematical foundations, they seem as an appropriate choice to describe and analyze cyber situational information.