Chapter 5.6
Teamworking for Security:
The Collaborative Approach

Rainer Bye
Technische Universität Berlin, Germany

Ahmet Camtepe
Technische Universität Berlin, Germany

Sahin Albayrak
Technische Universität Berlin, Germany

ABSTRACT

Collaborative methods are promising tools for solving complex security tasks. In this context, the authors present the security overlay framework CIMD (Collaborative Intrusion and Malware Detection), enabling participants to state *objectives* and *interests* for joint intrusion detection and find groups for the exchange of security-related data such as monitoring or detection results accordingly; to these groups the authors refer as *detection groups*. First, the authors present and discuss a tree-oriented taxonomy for the representation of nodes within the collaboration model. Second, they introduce and evaluate an algorithm for the formation of detection groups. After conducting a vulnerability analysis of the system, the authors demonstrate the validity of CIMD by examining two different scenarios inspired sociology where the collaboration is advantageous compared to the non-collaborative approach. They evaluate the benefit of CIMD by simulation in a novel packet-level simulation environment called NeSSi (Network Security Simulator) and give a probabilistic analysis for the scenarios.

INTRODUCTION

Teamwork– nowadays professional life as well as private life is hardly imaginable without teamwork. Above all, complex tasks are usually managed in teams. Ideally, each participant of a team can contribute in the area of his strengths. However, teams can also be homogeneous; dependent on the task a team is to fulfill, a heterogeneous set-up might not be necessary or may even be disadvantageous due to arising conflicts.

DOI: 10.4018/978-1-60566-414-9.ch002

Intrusion detection is indisputably a complex task and there is no silver bullet coping with threats arising from malicious software or attackers. According to the 2008 Symantec Internet Security Threat Report, the security landscape was characterized by an "increasing professionalization of malicious code and the existence of organizations that employ programmers dedicated to the production of these threats" (Turner, 2008, p.46). That indicates the situation is even becoming worse.

Computer networks are exposed to a variety of threats: Zero-day attacks leave devices connected to the Internet susceptible to attacks because there are no appropriate signatures available during the vulnerability window. On the other hand, purely anomaly-based detection schemes capable of detecting new attacks are often of limited use due to a high false-positive rate.

Due to the shortcomings of conventional intrusion detection approaches we propose **CIMD** (**Collaborative Intrusion & Malware Detection**), a scheme for joint intrusion detection approaches. We argue that teams respectively groups with a common purpose for intrusion detection and prevention provide improved protection from malware. An intrusion detection overlay is realized by enabling participants to state their ***objectives***, i.e. the aim of a ***detection group***, and ***interests***, i.e. the desired properties of the team members. CIMD is collaborative, since for a common task, groups can be dynamically created in a heterarchical manner without pre-defined roles. After the **group formation** is complete, cooperative detection approaches can be carried out, i.e. tasks are divided between group members and roles are assigned. Nevertheless, in this phase a collaborative approach can be employed as well. In the following, the term joint intrusion detection is used when a differentiation between collaboration and cooperation is not necessary. CIMD is a part of ongoing research in the context of research activities aiming to develop autonomous intrusion detection and response techniques.

This work contributes a taxonomy-based data model reflecting relevant properties of the participants of the overlay. We discuss each category in the taxonomy with regard to their value for collaborative intrusion detection. Additionally, we also provide a group formation algorithm to establish these groups. Each participating node executes this algorithm that receives input objectives and associated interests defined as instances of the **property taxonomy**. Moreover, it takes maximum group sizes into account. We examine different realization strategies for the system and discuss their characteristics.

Finally, we introduce the notion of homogeneous as well as heterogeneous detection groups analogous to the introductory example of teamwork in a sociological context. We consider a distributed anomaly detection approach as a scenario for homogeneous groups and discuss device similarity as a prerequisite. In the second scenario, we apply a signature mediation scheme wherein disparate NIDS (Network Intrusion Detection Systems) collaborate to reduce the vulnerability window. This is an example for a heterogeneous detection group enabling exchange of signatures between the devices. We conduct simulations for the latter scenario in a novel network simulation environment addressing the needs of security experts: NeSSi. Nevertheless, a distributed scheme like CIMD exhibits the danger of being compromised. Hence, we discuss security aspects of the system itself, provide adversary scenarios and discuss appropriate countermeasures.

This paper is organized as follows: subsequently, we introduce related work, present CIMD and show realization strategies of the system. We conduct a **vulnerability analysis** of CIMD and outline in the following the merits of an intrusion detection overlay based on the outlined scenarios. Subsequently, we simulate the "signature mediation" scenario as an example for collaboration in heterogeneous groups. Finally, we conclude and give an outlook on future work.