Teams Rather Than Individuals: Collaborative Intrusion Detection

R. Bye *,1, S. A. Camtepe[1], and S. Albayrak[1]

[1] *Technische Universität Berlin - DAI-Labor, Ernst-Reuter-Platz 7, D-10587 Berlin, Germany*

There still exist challenges for intrusion detection approaches such as zero-day attacks, high false-alarm rates or architectural drawbacks, e. g., centralized designs exposing the Single-Point-of-Failure. From the field of sociology, we learn that teams respectively groups cope with complex tasks by their inherent cooperative character.

A Collaborative Intrusion Detection System (CIDS) is a dynamic, distributed system where participants form new organizational structures such as teams and can adapt to different roles to fulfill a common, Intrusion Detection related task not solvable by a participant on its own, i.e. the result must substantially differ from the individual functionality. The advantages of Collaboration include architectural benefits, the teamwork aspect and the realization of a “Bigger Picture”.

The pillars a CIDS is built on, the CIDF refer to key aspects of Collaboration itself: a *Communication Scheme* realises well-established communication channels, whereas *Organizational Structure* and *Group Formation* provide the ability for comprehensive planning and commitment to a common mission. The *Information Sharing and Interoperability* allows resource investment and sharing. In addition, the *System Security* is an important characteristic owed to the application domain.

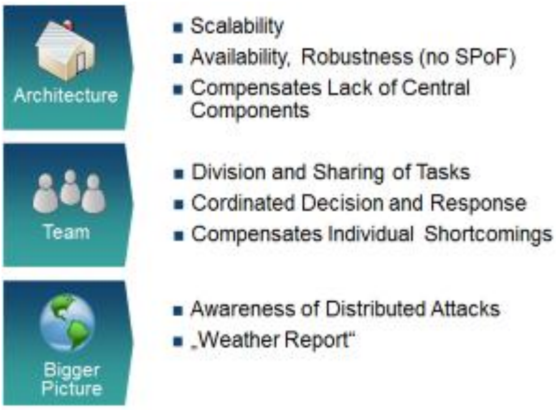
Architecture
▪ Scalability
▪ Availability, Robustness (no SPoF)
▪ Compensates Lack of Central Components
Team
▪ Division and Sharing of Tasks
▪ Cordinated Decision and Response
▪ Compensates Individual Shortcomings
Bigger Picture
▪ Awareness of Distributed Attacks
▪ „Weather Report“

Fig. 1. Advantages of collaborative solutions, in particular of CIDS are threefold: Architectural Benefits, working in teams and the realization of a Bigger Picture.

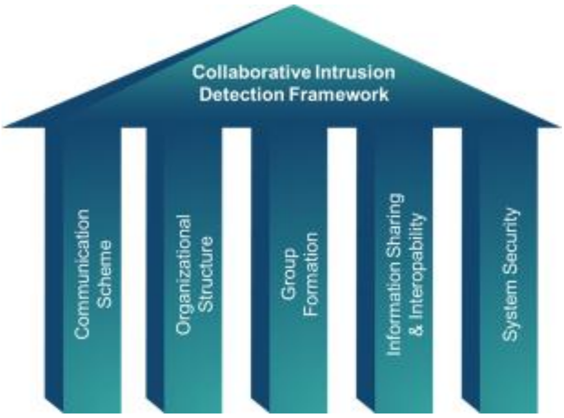
Collaborative Intrusion Detection Framework
Communication Scheme
Organizational Structure
Group Formation
Information Sharing & Interopability
System Security

Fig. 2. CIDF represents a template for creating CIDS solutions. The five pillars to be considered reflect collaboration requirements as well as the security of the system owed to the application domain.

There exist intrusion detection systems that work cooperatively, bypassing the aforementioned shortcomings of the conventional approaches. However, these systems remain limited to very specialized scenarios and do not take configuration and explicit grouping of participants into account. Furthermore, they do neither consider arising adversarial opportunities introduced by work-coupled IDS nor provide countermeasures such as anonymous message exchange.

We propose CIMD (Collaborative Intrusion and Malware Detection), a scheme for the realization of collaborative intrusion detection approaches [1]. We argue that teams, respectively detection groups with a common purpose for intrusion detection and response, improve the measures against malware. CIMD provides a collaboration model, a decentralized group formation and an anonymous communication scheme. Participating agents can convey intrusion detection related

*Corresp. author: rainer.bye@dai-labor.de, Phone: +49-30-314-74045, Fax: +49-30-314-74003

objectives and associated interests for collaboration partners. These interests are based on intrusion detection related ontology, incorporating network and hardware configurations and detection capabilities. Anonymous Communication provided by CIMD allows communication beyond suspicion, i.e. the adversary can not perform better than guessing an IDS to be the source of a message at random [2]. The evaluation takes place with the help of NeSSi² (www.nessi2.de), the Network Security Simulator, a dedicated environment for analysis of attacks and countermeasures in mid-scale and large-scale networks. A CIMD prototype is being built based on the JIAC agent framework (www.jiac.de).

The approach has shown its merits in various case studies: Collaborating anomaly detection agents achieved a lower false-positive compared to a non-collaborative approach, solving an inherent problem of anomaly detection itself. Computational complexity of training and detection was reduced as well. In another case study, we investigated a signature mediation scheme. The result was a shorter vulnerability interval in the context of zero-day exploits.

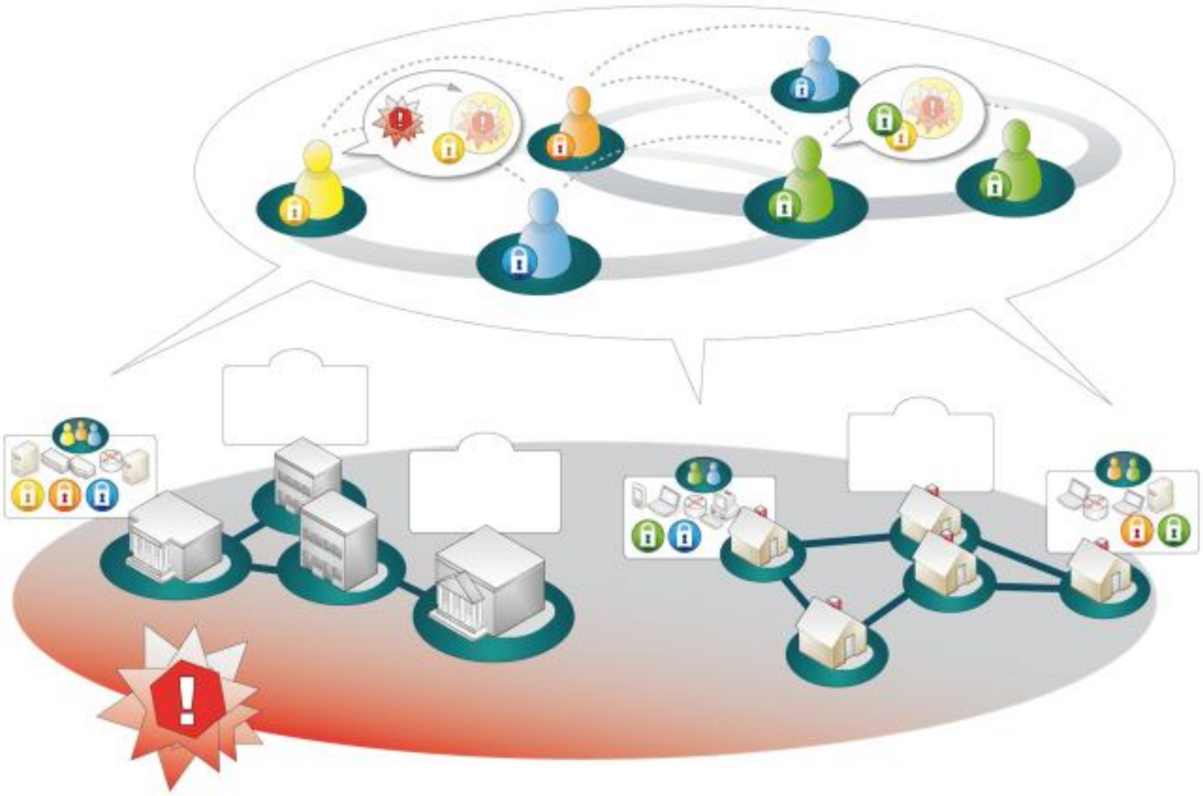

Fig. 3. There exist a heterogenity of IDS deployments as well as heterogeneity of IDS products with their distinct capabilities. CIMD realizes detection groups, enabling the exchange of intrusion related information. In this example, a distributed attack, e.g. worm spread, takes place. The yellow agent is capable of preventing the threat and sends a signature to the collaborating agents within the detection group.

References

[1] R. Bye, A. Camtepe and S. Albayrak, Collaborative Computer Security and Trust Management, Chapter Teamworking for Security: The Collaborative Approach, 1st edition, page 342, (2009)

[2] R. Bye, A. Camtepe and S. Albayrak, Collaborative Intrusion Detection Framework: Characteristics, Adversarial Opportunities and Countermeasures, in Proceedings of *CollSec*: *Usenix Workshop on Collaborative Methods for Security and Privacy*, (2009)