

Teamworking for Security with CIMD: A Collaborative Approach to Intrusion Detection

Rainer Bye, Ahmet Camtepe, Sahin Albayrak
{rainer.bye, ahmet.camtepe, sahin.albayrak}@dai-labor.de
www.dai-labor.de

Why Collaborative IDS?

A 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 task not solvable by a participant on its own, i.e. the result must substantially differ from the individual functionality.

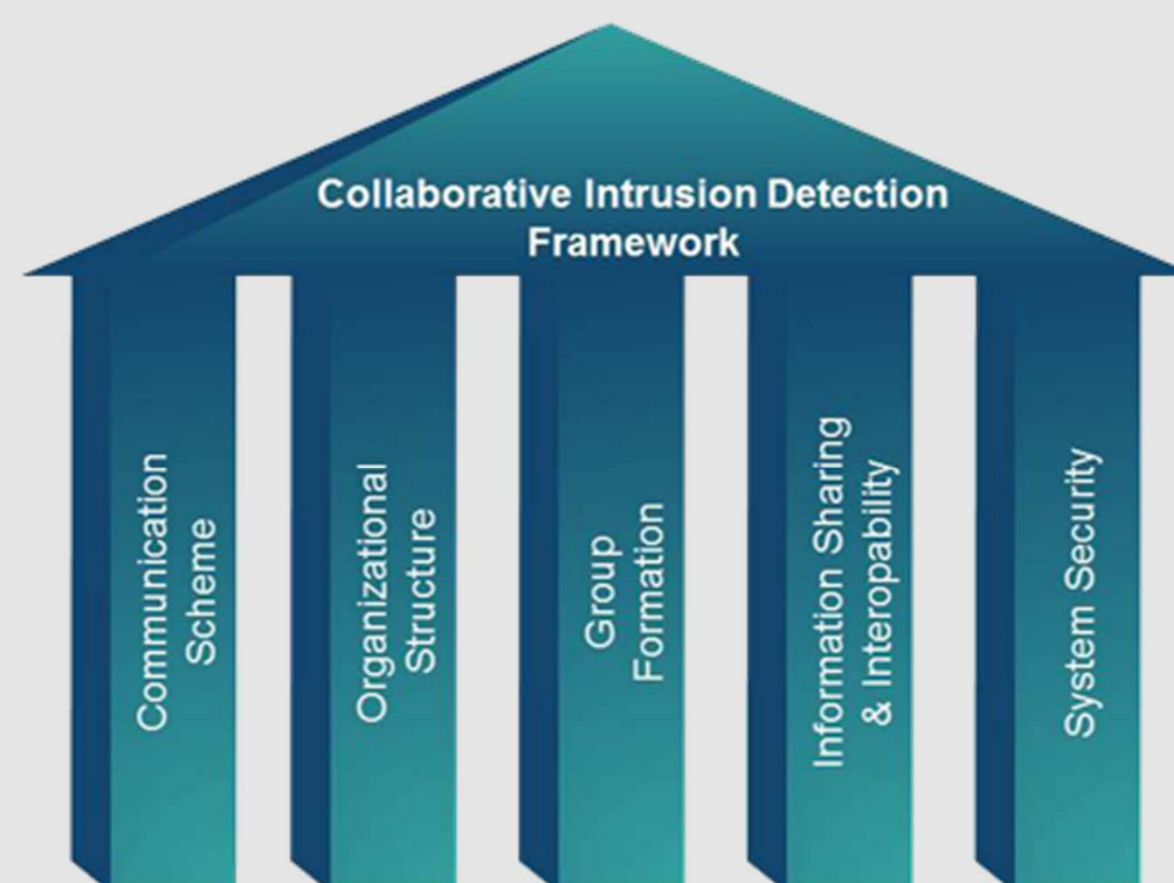
The advantages of Collaboration include architectural benefits, the teamwork aspect and the realization of a "Bigger Picture".



What is necessary?

The pillars a CIDS is built on, the CIDEF, 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.



CIMD - The Approach

Collaborative Intrusion & Malware Detection offers a scheme for the formation of *detection groups*. CIMD provides a collaboration model, a decentralized group formation algorithm and an anonymous communication scheme.

Every participating agent can convey intrusion detection related objectives and associated interests for collaboration partners. These interests are based on an intrusion detection related ontology, incorporating network and hardware configurations and detection capabilities.

The Anonymous Communication scheme 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.

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 large-scale networks. A CIMD prototype is being built based on the JIAC agent framework (www.jiac.de).

Results:

A lower false-positive rate was achieved by collaborating anomaly detection agents, 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.

References:

R. Bye, A. Camtepe and S. Albayrak. *Collaborative Computer Security and Trust Management*, Chapter Teamworking for Security: The Collaborative Approach, Information Science Reference, 2009.

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*, 2010.

