A Collaborative Attack Detection and its Challenges in the Future Internet

Thomas Gamer, Hans Wippel
Institute of Telematics, Karlsruhe Institute of Technology (KIT), Germany
{thomas.gamer, hans.wippel}@kit.edu

I. Introduction

Today, the Internet is an inherent part of our daily life. The Internet's availability is, however, threatened primarily by large-scale attacks like distributed denial-of-service (DDoS) attacks [1]. In the context of the G-Lab project[1] we therefore worked on a suitable solution that allows for an effective Internet-wide detection of such attacks in today's Internet. This solution, in a next step, has to be analyzed with respect to its applicability in a Future Internet that, e. g., relies on virtual networks and application-tailored architectures and protocols. The collaborative attack detection, which we developed with focus on currently common large-scale attacks, can be divided into three major parts:

- Local detection of traffic anomalies,
- Local identification of the respective attack, and
- Collaboration of detection systems that are distributed Internet-wide, act independently of each other, and do not require pre-established trust relationships.

These parts and their interaction are shortly described in the following Section II. The challenges of applying such an anomaly detection in a Future Internet are subsequently detailed in Section III as an outlook on ongoing and future work.

II. Collaborative Attack Detection

Our collaborative attack detection is based on the assumptions that detection systems of different administrative domains mostly act independently of each other and that close trust relationships rarely exist between the various domains. In addition, detection systems may be heterogeneous in regard to anomaly detection methods as well as resources available for the detection. Thus, the local detection has to be flexible, easily extensible and should autonomously adapt to different situations and environments.

The interaction of all parts of the collaborative detection is depicted in Fig. 1. There, an exemplary local anomaly detection process is indicated, which results in the detection of a volume anomaly in TCP packets and a protocol anomaly with respect to incoming TCP SYN packets. These anomalies lead to the local identification of a SYN flooding DDoS attack. Subsequent to the identification, attack type and attack characteristics, e. g., victim address and port, are sent to neighboring detection systems—allowing them to locally validate the received information and, thus, to eliminate a possible false negative detection error.

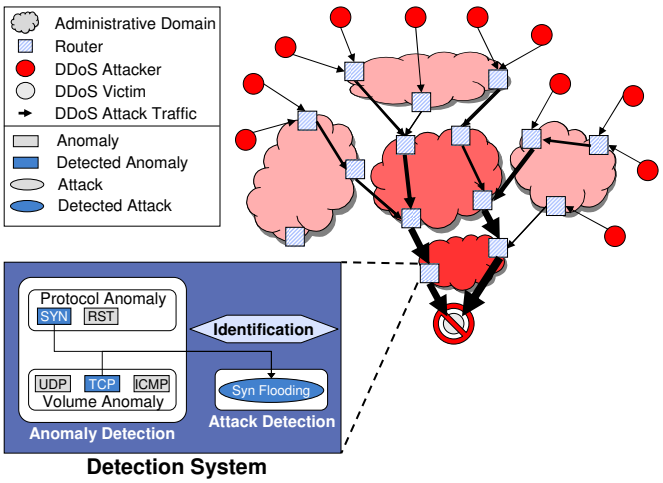

Fig. 1. Interaction of local anomaly detection, attack identification, and collaboration

A. Anomaly Detection and Attack Identification

The local anomaly detection is based on the principle of detection *refinement*, i. e., multiple different anomaly detection methods like [2], [3] are executed in subsequent detection stages—the basic stage being rather coarse-grained while traffic analysis becomes more and more fine-grained with higher stages. Such a hierarchical approach ensures applicability on systems having only limited resources for detection, e. g., high-bandwidth routers within the core of the Internet.

The local detection process relies on a *generalized model* of anomaly detection methods, anomalies, and attacks [4]. From this model, the information necessary for the *autonomous processing control*—e. g., preconditions of and dependencies between detection methods—and for the *iterative identification* of attacks is derived. The iterative identification relies on various rule sets that each characterize a certain attack type by required as well as optional anomalies. Moreover, if required, a geometric classifier is subsequently applied, e. g., in case the rule-based identification fails due to imperfect or inaccurate anomaly detection. This approach ensures a flexible, extensible, and autonomous local anomaly detection and attack identification.

[1]We gratefully acknowledge that this work is funded by the Federal Ministry of Education and Research of the Federal Republic of Germany

B. Collaboration of Distributed Detection Systems

In case detection is based on local observations only, a detection system may experience *false negative errors*, i. e., an ongoing attack is not detected, e. g., due to unfavorable aggregation of attack traffic. Hereby, collaboration of detection systems may help to reduce the number of false negative detection errors through additional information. Our approach [5] for a collaboration of detection systems distributed Internet-wide relies on exchanging solely descriptive information about locally detected attacks—no sensitive traffic data in regard to operational aspects or user privacy has to be exchanged as with [6]. Similar to [7], a detection system receiving such descriptive information first has to locally validate it in order to establish trust into this information locally. This facilitates a collaboration beyond domain-boundaries without the need for close trust relationships. In contrast to [7], our approach additionally considers resource limitations of the detection systems as well as vulnerability of the collaboration itself.

Our collaboration builds on two main design principles: (1) each detection systems autonomously decides how to react on received information and (2) information exchange is limited to neighboring detection systems only. In order to achieve (1) a *metric-based decision algorithm* is applied on incoming attack information. This algorithm considers that only limited resources are available for validation of information, i. e., a validation can be explicitly rejected by the decision algorithm. A decision function, therefore, rates incoming information in regard to its relevance—allowing to prefer the information for validation that seems most important. Thus, this approach ensures robustness against overload situations and attacks on the collaboration itself.

A neighborhood discovery is used to achieve the *limited collaboration*—principle (2). Hereby, the discovery mechanism defines the neighborhood structure, e. g., ring-based or an overlay network. This limited collaboration facilitates a significantly lower communication overhead than existing approaches. In addition, attack information spreads mainly along attack paths instead of Internet-wide and thereby, significantly reduces validation overhead as well as false positive errors.

A simulative evaluation of our collaborative detection, which used a ring-based neighborhood discovery and an analytically derived decision function tailored to this discovery mechanism, showed that this approach is superior to existing ones with respect to the reduction of false negative errors, lower overhead, and consideration of limited resources.

III. Challenges regarding a Future Internet

Having developed, implemented, and evaluated a collaborative, anomaly-based attack detection that focuses on currently common large-scale attacks like DDoS, we in a next step directed our attention to anomaly detection in a Future Internet. In our opinion, anomaly detection will still be necessary in a Future Internet. Even though security is considered in most Future Internet research from scratch, anomaly detection at least is necessary in order to detect node or network failures and to initiate adaptation or tuning, e. g., of protocol parameters, at runtime. Furthermore, we think that malicious attacks cannot be prevented completely in a Future Internet and, thus, attack identification and collaboration should be considered.

For these reasons, we examined the applicability of our collaborative detection in a Future Internet and identified some challenges that have to be tackled in future work. First, we identified three important topics that could be subsumed as *node management* and should be dealt with jointly: monitoring, anomaly detection, and adaptation. Then, focusing on an exemplary Future Internet framework—the *Node Architecture* designed within the 4WARD project [8]—we analyzed how to integrate necessary functionality into the framework and developed a hierarchical management system that aggregates management information directed at higher levels and delegates management tasks directed at lower levels [9].

Challenges that have to be solved in future work are:

- At which level should anomaly detection be located and how should it be implemented? Since level-specific knowledge is only available at the respective level, e. g., protocol-specific knowledge at the protocol level, anomaly detection seems to be necessary at each level. However, the introduction of entire hierarchical anomaly detection instances at each level of the management hierarchy increases complexity.
- At which level should attack identification be located? For example, it could be sufficient to perform the identification on the topmost level only.
- How to integrate collaboration into a Future Internet framework that relies on various application-tailored networks and protocols per node? Collaboration with other network nodes may require knowledge about individual network characteristics and, thus, customized discovery/signaling mechanisms to allow for a suitable decision.

References

[1] Arbor Networks, "Worldwide Infrastructure Security Report 2009," http://www.arbornetworks.com/report, Jan. 2010.

[2] A. Lakhina, "Diagnosing Network-Wide Traffic Anomalies," in *Proc. of Applications, technologies, architectures, and protocols for computer communications*, Portland, Oregon, USA, Aug. 2004, pp. 219–230.

[3] G. Carl, G. Kesidis, R. R. Brooks, and S. Rai, "Denial-of-service attack-detection techniques," *IEEE Internet Computing*, vol. 10, no. 1, pp. 82–89, Jan. 2006.

[4] T. Gamer, "Anomaly-based Identification of Large-Scale Attacks," in *Proc. of Global Communications Conference (Globecom)*. Honolulu, HI, USA: IEEE, Dec. 2009.

[5] T. Gamer, M. Scharf, and M. Schöller, "Collaborative anomaly-based attack detection," in *Proc. of 2nd International Workshop on Self-Organizing Systems (IWSOS)*, English Lake District, UK, Sep. 2007, pp. 280–287.

[6] W. Zhang, S. Teng, and X. Fu, "Scan attack detection based on distributed cooperative model," in *Proc. of 12th Int. Conf. on Computer Supported Cooperative Work in Design (CSCW)*, Apr. 2008, pp. 743–748.

[7] C. Papadopoulos, R. Lindell, J. Mehringer, A. Hussain, and R. Govindan, "Cossack: Coordinated suppression of simultaneous attacks," in *Proc. of DARPA Information Survivability Conference and Exposition (DISCEX)*, Washington, DC, USA, Apr. 2003, pp. 2–13.

[8] "4WARD Project Homepage," http://www.4ward-project.eu/.

[9] H. Wippel, T. Gamer, and D. Martin, "A Hierarchical Node Management System for Application-tailored Network Protocols and Architectures," Presentation at the 5th GI/ITG KuVS Workshop on Future Internet, Stuttgart, Germany, Jun. 2010.