Computer Networks 80 (2015) 66–88

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

DEFIDNET: A framework for optimal allocation of cyberdefenses in Intrusion Detection Networks

Sergio Pastrana *, Juan E. Tapiador, Agustin Orfila, Pedro Peris-Lopez

Computer Security (COSEC) Lab, Department of Computer Science, Universidad Carlos III de Madrid, Avda. Universidad 30, 28911 Leganés, Madrid, Spain

ARTICLE INFO

Article history:
Received 12 July 2014
Received in revised form 14 November 2014
Accepted 20 January 2015
Available online 4 February 2015

Keywords:
Cooperative cyberdefense
Evasion attacks
Resilient cyberdefenses
Adversarial settings

ABSTRACT

Intrusion Detection Networks (IDN) are distributed cyberdefense systems composed of different nodes performing local detection and filtering functions, as well as sharing information with other nodes in the IDN. The security and resilience of such cyberdefense systems are paramount, since an attacker will try to evade them or render them unusable before attacking the end systems. In this paper, we introduce a system model for IDN nodes in terms of their logical components, functions, and communication channels. This allows us to model different IDN node roles (e.g., detectors, filters, aggregators, correlators, etc.) and architectures (e.g., hierarchical, centralized, fully distributed, etc.). We then introduce a threat model that considers adversarial actions executed against particular IDN nodes, and also the propagation of such actions throughout connected nodes. Based on such models, we finally introduce a countermeasure allocation model based on a multi-objective optimization algorithm to obtain optimal allocation strategies that minimize both risk and cost. Our experimental results obtained through simulation with different IDN architectures illustrate the benefit of our framework to design and reconfigure cyberdefense systems optimally.

1. Introduction

Intrusion Detection Systems (IDS) constitute a primary component for securing computing infrastructures. An IDS monitors activity and seeks to identify evidence of ongoing attacks, intrusion attempts, or violations of the security policies [1]. IDSs have evolved since the first model proposed in the late 1980s [2], and the current threat landscape makes the classical approach[1] for intrusion detection no longer valid. Moreover, intrusion detection must also deal with emerging paradigms in computing and communications. For example, performing detection in wireless nodes such as smartphones [3] or wearable sensing devices [4], requires lightweight procedures that do not consume much resources like energy or memory.

Detection paradigms and architectures have also evolved to cope with the requirements of complex network infrastructures. Rather than standalone components strategically placed to protect a complete network or system, the current trend is to rely on a distributed network of detection nodes. Intrusion Detection Networks (IDN) [5] are composed of different IDS nodes distributed among a network to perform local detection functions and sharing information with other nodes in the IDN. One of the major advantages of IDNs is that, since the detection function is distributed across different network locations, so is the workload. Classical intrusion detection components such as Snort [6] must be implemented in a single device.

* Corresponding author. Tel.: +34 91 624 6260; fax: +34 91 624 9429.
E-mail addresses: spastran@inf.uc3m.es (S. Pastrana), jestevez@inf.uc3m.es (J.E. Tapiador), adiaz@inf.uc3m.es (A. Orfila), pperis@inf.uc3m.es (P. Peris-Lopez).

[1] By classical approach we mean one where a standalone IDS protects a small local area network with no collaboration with any other IDSs.

http://dx.doi.org/10.1016/j.comnet.2015.01.012
1389-1286/

Therefore, this host is in charge of gathering the data (monitor the network), pre-process it, running detection algorithms and generating responses accordingly. This approach is inappropriate both for resource-constrained scenarios and for large networks. The problem becomes even harder in the worst-case scenario, where an adversary forces the detection algorithm to behave the worst in terms of performance, thus forcing the IDS to spend a large amount of resources. This may facilitate evasion, for example if the IDS discards packets. One way of achieving this is by constructing carefully crafted payloads that make the signature matching algorithm to repeatedly backtrack during inspection may render packet processing rates million of times slower than in the average case [7,8].

IDNs attempt to solve this problem by distributing the tasks among different nodes. Depending on their role in the network, some nodes gather local data and send it to another node, probably with more resources, who correlates the data and performs actual detection. This separation of duties makes IDNs a suitable solution for distributed systems, including mobile ad hoc networks (MANETs), where there are no central nodes and every host must collaborate to ensure a proper network behavior [9]. IDNs are also used in networks geographically separated to allow different entities to collaborate and mitigate large scale attacks [10]. Current attacks are capable of infecting simultaneously various networks or incorporating evasion techniques to pass undetected [11]. Moreover, many zero-day attacks target simultaneously a huge number of systems worldwide [12], leaving little time to patch other networks. Thus, to prevent threats from propagating through different domains, collaboration between different IDNs is essential.

1.1. Motivation and contributions

Due to the connectivity of the nodes in an IDN, threats affecting one node may propagate and affect the entire network. To completely mitigate such threats, it is required to protect every single node which is at risk. In many scenarios this is not possible due to resource constraints (in terms of time, human and financial costs, etc.) and the problem turns into optimally investing in security measures to minimize the residual risk. Similarly, given an acceptable level of the residual risk, the budget spent can be minimized.

In this sense, the placement of countermeasures in IDNs plays an important role. Deciding what has to be protected—i.e., where to allocate countermeasures—is a complex task. This decision depends on many factors, such as the adversarial model, the impact of the attacks, or the cost of implementing the countermeasures. These factors vary considerably even within the same network. For example, the cost in terms of time and energy of implementing cryptography mechanisms for wireless communications is different depending on the operating system and the software used [13]. Similarly, the impact of a denial of service attack on a Security Operations Center (SOC) is typically higher than that of an anti-virus solution for a personal computer.

Due to the wide variety and complexity of IDNs proposed in the literature, the risk-rating of these networks is typically done in an ad hoc manner, what makes it expensive and error prone. In this paper, we develop a generic risk-rating framework for IDNs called DEFIDNET. This framework uses a generic system model tailored to IDNs that allows to define generic cyberdefense components that compose the network as well as the adversarial model. Then, it incorporates procedures to asses the risk of the IDN. Concretely, considering that some nodes may be targeted by an adversary, the framework evaluates the propagation of intrusive actions through the network considering the influences between nodes. It then estimates the impacts of such actions regarding different attack strategies. Overall, this provides a global picture of the IDN risk considering the impacts and likelihood of attacks. Finally, the framework provides a search-based optimization module that provides the set of optimal countermeasures in terms of cost and mitigated risk. To illustrate the benefits of DEFIDNET, we provide experimental results using different network architectures and a case study using a complex cooperative network.

In summary, the main contributions of this work are:

1. A system model that defines the elements of an IDN. It is composed of a model for IDN nodes in terms of their logical components, functions, and channels. Then, depending on which of these components are implemented in a node, several roles are presented. Finally, the architecture of the IDN is defined regarding the connections and influences between nodes.
2. A threat model that indicates sequences of intrusive actions that an adversary can execute against an IDN. The model considers not only actions against a single node, but also the propagation of such action throughout connected nodes and provides a global picture of the risk to which the IDN is exposed.
3. An allocation model based on a multi-objective optimization algorithm to obtain optimal allocation of countermeasures with respect to both risk and cost.
4. Experimental results obtained through simulation for different IDN architectures and a detailed case study illustrating the benefits of DEFIDNET.

Our experiments have been conducted with a prototype implementation of a tool based on the proposed framework that is freely available for download.[2]

1.2. Organization

The paper is organized as follows. In Section 2 we provide some background and related work. In Section 3 we describe the system model to define IDNs, and in Section 4 we describe the framework in detail, including the threat, risk-rating and allocation modules. We provide experimental results in Section 5 and in Section 6 we present a case study with DEFIDNET. Finally, Section 7 presents the conclusions.

[2] See http://www.seg.inf.uc3m.es/spastran/defidnet/DEFIDNET_GUI.zip.