Available online at www.sciencedirect.com

SciVerse ScienceDirect

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

Computers & Security

Operational experiences with anomaly detection in backbone networks

Maurizio Molina [a,1], Ignasi Paredes-Oliva [b,*], Wayne Routly [a], Pere Barlet-Ros [b]

[a] DANTE, 126-130 Hills Road, Cambridge CB2 1PQ, United Kingdom
[b] Dept. of Computer Architecture, UPC BarcelonaTech, Campus Nord, Edif. D6, C. Jordi Girona, 1-3, 08034 Barcelona, Spain

ARTICLE INFO

Article history:
Received 24 March 2011
Received in revised form
26 September 2011
Accepted 28 January 2012

Keywords:
Network security
Anomaly detection
Benchmarking
NetFlow
Network management

ABSTRACT

Although network security is a crucial aspect for network operators, there are still very few works that have examined the anomalies present in large backbone networks and evaluated the performance of existing anomaly detection solutions in operational environments. The objective of this work is to fill this gap by reporting hands-on experience in the evaluation and deployment of an anomaly detection solution for the GÉANT backbone network. During this process, we analyzed three different commercial tools for anomaly detection and then deployed one of them for several months in the 18 points-of-presence of GÉANT. We first explain the general requirements that an anomaly detection system should satisfy from the point of view of a network operator. Afterwards, we describe the evaluation of the tools and present a study of the anomalies found in a continental backbone network after operationally using the finally deployed tool for half a year. We think that this first hand information can be of great interest to both professionals and researchers working on network security and can also guide future research towards more practical problems faced by network operators.

1. Introduction

Network operators have always been interested in keeping track of the anomalies happening in their network. Traditionally, they have focused on operational (e.g., link faults), or traffic and routing anomalies, observable via SNMP. More recently, there has been a business driver for observing anomalies related to security issues, network abuse, or IPR violation.

The reason for investing in security, even in core networks, is that offering a more secure network (i.e., protecting customers from external or internal threats) is becoming a differentiating factor for ISPs, already offering managed security services to their business customers. Furthermore, commercial peering agreements between ISPs often include commitments to avoid transferring potentially harming traffic (e.g., DoS attacks).

Detecting security anomalies requires a more granular visibility of the network than what can be provided by SNMP traffic counters. NetFlow (Cisco Systems, 2000) is becoming one of the primary sources of information for security services.

GÉANT (2011) is a multi-Gigabit backbone network interconnecting the European National Research and Education Networks (NRENs). DANTE (2011), as the operator of GÉANT, is uniquely positioned to provide added value to the security

* Corresponding author. Tel.: +34 934017182; fax: +34 934017055.
E-mail addresses: maurizio.molina@gmail.com (M. Molina), iparedes@ac.upc.edu (I. Paredes-Oliva), wayne.routly@dante.net (W. Routly), pbarlet@ac.upc.edu (P. Barlet-Ros).
[1] Present address: Open Systems AG, Räffelstrasse 29, 8045 Zurich, Switzerland.

0167-4048/$ – see front matter © 2012 Elsevier Ltd. All rights reserved.
doi:10.1016/j.cose.2012.01.009

work of NREN CERTs.[2] For example, Distributed DoS attacks can be mitigated and filtered closer to the source of the attack. Worm spreading patterns can also appear more clearly when observed on the backbone network interconnecting all the European NRENs rather than separately on each of them.

During fall 2008, DANTE analyzed three commercial tools for anomaly detection. One year after (fall 2009), one of those tools was permanently deployed in the GÉANT network. This work reports on the benchmarking of the tools and the results obtained after using the finally deployed software for half a year.

The novelty of this paper is twofold. First, we report on the limitations of current commercial tools and discuss some aspects that still need further research from the perspective of a network operator. Second, we provide a long-term study of the anomalies occurring in a continental backbone network. Although there is already considerable work in the design of anomaly detection methods, information regarding the type and characteristics of network anomalies in operational networks is rather scarce in the literature. To the best of our knowledge, this is the first study that provides this sort of feedback.

After manually analyzing more than 1000 attacks, we found that, surprisingly, the overlap among the anomalies detected by different tools is extremely low. This is a clear indicator that false negatives are still significant even when comparing commercial tools that are supposed to detect the same sort of anomalies. In addition, our study reveals that *Network Scan* attacks are the most persistent and shows that there are certain geographical regions that are predominant when looking at the top attackers or targets respectively.

We believe that the analysis and results provided in this paper are particularly interesting for both practitioners and researchers working on anomaly detection. For professionals (other operators or companies) willing to deploy a similar solution, this work can provide very useful information ranging from the requirements used to build the list of anomaly detection tools for the trial, to the evaluation of the tools and the followed methodology. Concerning researchers, the most relevant part of this paper lies on the long-term analysis of anomalies, which can help them in better directing their efforts towards limitations of current commercial products and real threats happening in backbone networks. Additionally, the knowledge on the requirements of a network operator is of great importance and can serve as a guideline to design algorithms able to work in real-world environments. Furthermore, we must take into account that having access to commercial solutions is rather uncommon, especially for researchers.

The remainder of this paper is organized as follows. Section 2 describes the requirements used by DANTE to build a short-list of suitable anomaly detection tools. Afterwards, Section 3 reports on the differences found among those tools during the evaluation phase in terms of usability, true and false positives, false negatives and also regarding the different types of anomalies detected. Section 4 presents a study of the network anomalies found in GÉANT along with their properties after using the selected tool for approximately six months. Finally, Section 5 explains in more detail the anomaly detection approaches used by each tool while Section 6 summarizes and concludes the paper.

[2] A CERT (Computer Emergency Response Team) is a group of experts that takes care of any security-related event threatening a NREN.

2. Scenario and requirements

In this section, we first describe the GÉANT network scenario, where the tools have been analyzed. Then, the requirements used by DANTE to build the short-list of anomaly detection tools are explained and, finally, the selected tools are presented.

2.1. Context and scenario

DANTE is a non-profit organization that plans, builds and operates the GÉANT backbone network. GÉANT is a/19 transit network connecting 34 European NRENs with 18 points-of-presence (PoPs) spread over Europe (with 10 Gb/s links almost everywhere), a dozen of non-European NRENs, and two commercial providers (Telia and Global Crossing). It is the main interconnection point for inter-NREN traffic. For a certain subset of NRENs, GÉANT is also the primary gateway to the commercial Internet (other NRENs have their own connection to the non-research world). Although it is a R&E network, more than half of the traffic is towards commercial providers. The overall handled traffic is more than 50 Gb/s.

DANTE collects Sampled NetFlow (Cisco Systems, 2011) from every router interface with an external peering network. As GÉANT is a purely transit network, this setup is sufficient to account for all the traffic.

During fall 2008, DANTE started looking for a solution to enhance the security of its network, and of its customer networks, by analyzing three different anomaly detection commercial products. After evaluating the performance of each tool with the same input data for several months, one of them was permanently deployed in the GÉANT backbone network (mid November 2009).

At the beginning of this study, the sampling rate in Sampled NetFlow was set to 1/1000. Later on, the routers were replaced, which allowed to migrate to 1/100 sampling. Therefore, we must take into account that the analysis of the tools presented in Section 3 (fall 2008) and the study presented in Section 4 (2009–2010) were done under different sampling rates (1/1000 and 1/100 respectively).

NetFlow v5 was used since anomaly detection tools require visibility on very granular flows (the ones defined by the 5-tuple src/dst IP, src/dst port and protocol), which is the default (and only one) provided by NetFlow v5. The NetFlow traffic is exported to a single fanout box duplicating it towards multiple destinations (see Fig. 1). This setup allowed us to evaluate all the anomaly detection tools using exactly the same input data.

2.2. Tool requirements

In order to start the process to select one tool for anomaly detection, three candidate tools were short-listed on the basis