The Bi-directional Approach for Logical Traffic Isolation Forensic Model

[1]Innocentia Dlamini, [2]Martin Olivier, [1]Sihle Sibiya

Information and Computer Security Architectures Research Group (ICSA)
Department of Computer Science, University of Pretoria
[1](idlamini, ssibiya@csir.co.za), [2]molivier@cs.up.ac.za

Abstract— Network forensics involves capturing, recording and analysing network activity in discovering the source of security policy violations or information assurance. The network forensic system that is described in this paper is called the "Catch-it-as-you-can" system, which seizes all packets passing through a certain traffic point, captures and writes them to the storage. The main aim of this paper is to address some of the challenges faced by the Logical Traffic Isolation (LTI) model, more specifically the incompleteness of evidence-gathering process. This study proposes the Bidirectional Logical Traffic Isolation model (BLTI) to improve evidence completeness by recording both the request and the response of the suspicious communication; rather than only the request (suspicious data) as Logical Traffic Isolation (LTI) did. The BLTI uses indexing methods to improve information recording and retrieval. Future research will continue with the evaluation of the BLTI model performance not covered in this paper.

Index Terms—Network Forensics, Bidirectional Logical Traffic Isolation, Differentiated Services

I. INTRODUCTION

In 2006, Strauss *et al.* [1] proposed a scheme that utilises Differentiated Services (DiffServ) to isolate malicious traffic in a logical fashion from normal traffic. Since DiffServ is a standard technique, this could well reduce cost. More importantly, if a DiffServ infrastructure was already in place where an investigation needs to be performed, evidence collection could be facilitated with minimal changes to the network. The DiffServ approach allows network forensic investigators to attach both their marking station (ingress router) and preservation station to a cyber victim's network to investigate the case at hand. The advantage of this approach is minimal network downtime and minimal network reconfiguration.

The preservation station ensures forensic soundness and system reliability by recording all the packets marked by the marking station as suspicious. The two clients generate normal and suspicious traffic, and then forward these packets onto the DiffServ domain. The ingress edge router at the entrance boundary of the DiffServ domain is the first domain recipient and serves as a marking station. This router is responsible for packet classification and has marking, shaping and dropping capabilities. The ingress router marks the suspicious traffic with the help of the packet classifier and forwards them to the nearest core router. The core routers are found within the centre of the DiffServ domain. They forward traffic towards the egress router, while the egress router is found at the exit boundary of the DiffServ domain. The latter unmarks the traffic and decides the destination of each network packet according to its behaviour: the copy of the compromised traffic is forwarded to the preservation station, while the entire traffic is sent to the destination node. In a network-related cyber incident, the investigator searches the preservation station when conducting his/her investigation and captures all recorded suspicious network packets as evidence.

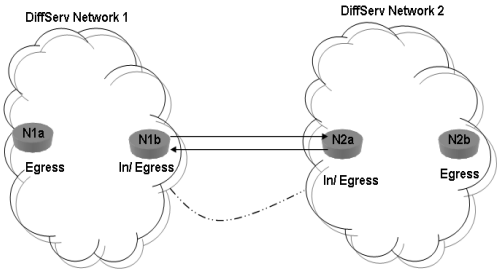
This paper further extends the design of the concept of a forensic model for Logical Traffic Isolation (LTI) based on Differentiated Services (DiffServ) as proposed by Strauss et al. [1] by recording both the request and the response of the suspicious communication, instead of recording the request only [2] as did the previous LTI model. This technique improves the completeness of evidence recorded. Since the LTI model is unidirectional, it preserves only the traffic from the node that was detected as suspicious. This raises concerns about the issues of evidence completeness. A model that will consider all the parties communicating with the suspicious node is proposed in this study. The rest of the paper is structured as follows: Section 2 discusses the architecture of the BLTI model and Section 3 serves as a conclusion.

II. THE BI-DIRECTIONAL LTI MODEL

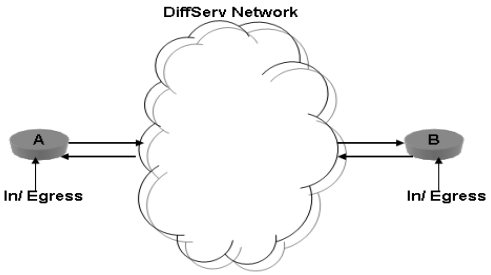
In [2] the architectural design of the DiffServ model for isolating suspicious traffic is simulated. Some of the significant components in this model are the marking station and the preservation station. When an intrusion has been detected, the ingress node from the DiffServ network is used as a marking station and the egress as the unmarking station. Once the traffic has been marked, it is easily isolated from the general traffic within the network, and it is easily preserved in the preservation station. The BLTI model marks only the traffic from the node that is suspected to be generating suspicious traffic. This raises issues about evidence completeness concerning the other node/s that is/are communicating with the detected node.

In solving this issue, each edge router from the DiffServ network can be considered as both ingress and egress router. Thus, each of these nodes can either mark or unmark the traffic to and from the detected node. Figure 1a) considers two Diffserv networks, with nodes N1b and N2a acting as both ingress and egress nodes (depending on the relationship between these networks). Whenever one network detects an intrusion generated from the other, it can create a channel

(dotted line) and so the two can notify each other about such incidents. Figure 1b) depicts the network with the edge routers on either side acting as both ingress and egress routers. The marking station is enhanced to be bi-directional and the LTI model in turn becomes bi-directional as stated before. The marking station is one of the most significant nodes in this model.



a) Edge Router as both In-/ Egress from Different Networks



b) Edge Router as both In-/ Egress for a Network

Fig. 1 The Bi-directional Marking Stations from DiffServ

Figure 2 shows an abstract view of the proposed BLTI model, which is discussed in the following subsections. The BTLI model divides the users into two categories, namely suspicious users and normal users. These users transmit traffic that is either suspicious or normal. The BLTI model does not focus on different types of intrusion detection, as different organisations may use different means to detect intrusion. Whenever an intrusion has been detected, the ingress router marks the packets that have been found to be suspicious. These packets are then forwarded to the preservation station to be recorded. A node communicating with the suspicious node is considered to generate suspicious traffic too. Both nodes use the DiffServ network for communication. Figure 2 shows the suspicious node as A3 and the normal node as A1-A2, B1-B3, and C1-C3.

Each of these nodes can initiate communication with any other node. The BLTI model utilises the DiffServ approach to isolate malicious traffic from normal traffic, and this includes the response from and to the suspicious node. The suspicious response is isolated through the use of destination identification, while the suspicious traffic from the suspicious node is identified through the use of source identification. The preservation station is positioned close to the source-suspicious node so as to record all traffic from and to the suspicious node, as well as to avoid packet loss of any packets of forensic interest.

Some of the challenges that will be dealt with include the storage size of the preservation station. To address this issue, Artificial Intelligent filtering methods will be used in the DiffServ network to ensure that any traffic isolated is indeed the actual traffic that has been detected as suspicious. However, in order to minimise network transmission problems such as transmission delays and high volumes of network traffic, the preservation station proposes to store only records that have been filtered to malicious traffic [4].

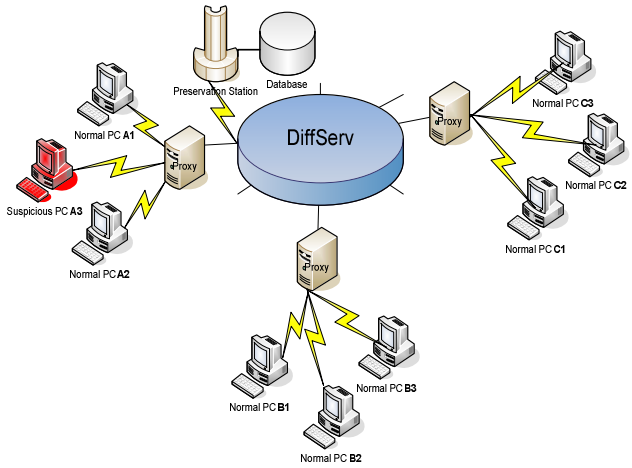


Fig. 2 The abstract view of the Bi-directional LTI Model

While the proposed BLTI system seems plausible, it has not yet been tested to prove its viability. The results are expected to prove that the proposed BLTI model improves support for the preservation, gathering and completeness of evidence in communication networks. The model discussed in this paper should therefore make a direct contribution to the enhancement of the Network Forensics discipline.

III. Conclusion

This paper presents the BLTI model as an extension of the LTI model that uses DiffServ to isolate suspicious traffic from normal traffic. The LTI model preserves only traffic from the suspicious node, while the BLTI model aims to address issues of evidence incompleteness. It also improves evidence gathering through bidirectional message recording. This work is still in progress and its performance has not yet been tested. A branch marking approach is used to determine the performance of this model and compare it with the unidirectional LTI model.

IV. References

[1] Strauss, T., Olivier, M.S. & Kourie, D.G. 2006, Differentiated Services for Logical Traffic Isolation, in M.S. Olivier and S. Shenoi (Eds), Advances in Digital Forensics II, pp. 229-237, Springer.

[2] Dlamini, I., Olivier, M.S. & Grobler, M. 2009, A Simulation of Logical Traffic Isolation Using Differentiated Services, *Digital Forensics & Incident Analysis (WDFIA 2009) unpublished.*

[3] Solomon, M.G., Barrett, D. & Broom, N. 2005, *The Need for Computer Forensics*, in L. Newman and W.G. Kruse (Eds), Computer Forensics Jump Start, pp 01-20, SYBEX inc.

[4] Corey, V., Peterman, C., Shearin S., Greenberg, M.S. & Van Bokkelen, J. 2002, Network Forensics Analysis, Internet Computing, Volume 6, pp. 60- 66, IEEE.

[5] Casey, E. 2002, *Handbook of Computer Crime Investigation*, Forensic tools and technology, pp 201-282, Elsevier Ltd.

I.Z. Dlamini is a MSc Computer Science student in the University of Pretoria. Her research interest includes Digital Forensics and Information Security. She completed her honours degree at the University of Zululand in November 2007 and her Undergraduate studies in 2006. She currently works for Defence, peace, safety and security (DPSS).