On the Design and Use of Internet Sinks for Network Abuse Monitoring

Vinod Yegneswaran\(^1\), Paul Barford\(^1\), and Dave Plonka\(^2\)

\(^1\) Dept. of Computer Science, University of Wisconsin, Madison
\(^2\) Dept. of Information Technology, University of Wisconsin, Madison

Abstract. Monitoring unused or dark IP addresses offers opportunities to significantly improve and expand knowledge of abuse activity without many of the problems associated with typical network intrusion detection and firewall systems. In this paper, we address the problem of designing and deploying a system for monitoring large unused address spaces such as class A telescopes with 16M IP addresses. We describe the architecture and implementation of the Internet Sink (iSink) system which measures packet traffic on unused IP addresses in an efficient, extensible and scalable fashion. In contrast to traditional intrusion detection systems or firewalls, iSink includes an active component that generates response packets to incoming traffic. This gives the iSink an important advantage in discriminating between different types of attacks (through examination of the response payloads). The key feature of iSink’s design that distinguishes it from other unused address space monitors is that its active response component is stateless and thus highly scalable. We report performance results of our iSink implementation in both controlled laboratory experiments and from a case study of a live deployment. Our results demonstrate the efficiency and scalability of our implementation as well as the important perspective on abuse activity that is afforded by its use.

Keywords: Intrusion Detection; Honeypots; Deception Systems

1 Introduction

Network abuse in the form of intrusions by port scanning or self propagating worms is a significant, on-going threat in the Internet. Clever new scanning methods are constantly being developed to thwart identification by standard firewalls and network intrusion detection systems (NIDS). Work by Staniford \textit{et al.} [27] and by Moore \textit{et al.} [18] project and evaluate the magnitude of the threat of new classes of worms and the difficulty of containing such worms. The conclusions of both papers is that addressing these threats presents the research and operational communities with serious challenges. An important step in protecting networks from malicious intrusions is to improve measurement and detection capabilities.

One means for improving the perspective and effectiveness of detection tools is to monitor both used and unused address space in a given network. Monitoring the unused addresses is not typically done since packets destined for those addresses are often dropped by a network’s gateway or border router. However, tracking packets sent to unused addresses offers two important advantages. First, other than misconfigurations, packets destined to unused addresses are almost always malicious, thus false positives
On the Design and Use of Internet Sinks for Network Abuse Monitoring

– a significant problem in NIDS – are minimized. Second, unlike NIDS that monitor traffic passively, a detection tool that monitors unused addresses can actively respond to connection requests, thus enabling the capture of data packets with attack-specific information. The possibility for unused address space monitoring is perhaps most significant in class A and class B networks where the number of unused addresses is often substantial. The idea of monitoring unused address space has been adopted in a number of different studies and on-going projects including the DOMINO project [31], the Honeynet project [29], LaBrea tarpits [14] and in the backscatter analysis conducted by Moore et al. in [19].

This paper makes two contributions. The first is our description of a new system architecture and implementation for measuring IP traffic. An Internet Sink or iSink, is a system we developed for monitoring abuse traffic by both active and passive means. The key design requirements of an iSink are extensibility of features and scalability of performance since it is meant to be used to monitor potentially large amounts of IP address space.

Our design of an iSink includes capabilities to trace packets, to actively respond to connection requests, to masquerade as several different application types, to fingerprint source hosts and to sample packets for increased scalability. The passive component of our implementation (which we call Passive Monitor) is based on Argus [3] – a freely available IP flow measurement tool. The active component of our implementation (which we call Active Sink) is based on the Click modular router platform [12]. Click is an open-source toolkit for building high performance network systems on commodity hardware. The focus of Active Sink’s development was to build a set of stateless responder elements which generate the appropriate series of application level response packets for connections that target different network services including HTTP, NetBIOS/SMB and DCERPC (Windows RPC Service).

The second contribution of this paper is a measurement and evaluation case study of our iSink implementation. We use the results from the case study to demonstrate the scale and diversity of traffic characteristics exposed by iSink-based monitoring. These results provide validation of our architectural requirements and rationale for subsequent evaluation criteria. We also deployed the iSink in situ to monitor four class B address spaces within our campus network for a period of 4 months and one entire class A address space to which we have access. From these data sets we report results that demonstrate the iSink’s capabilities and the unique information that can be extracted from this measurement tool. One example is that since the traffic characteristics from our class B monitor are substantially different from those on the class A monitor, we conclude that the location of the iSink in IP address space is important. Another example is that we see strong evidence of periodic probing in our class A monitor which we were able to isolate to the LovGate worm [2]. We also uncovered an SMTP hot-spot within the class A network that has been unreported prior to our study. We were able to attribute that anomaly to misconfigured wireless routers from a major vendor. Finally, we assess basic performance of the iSink in controlled laboratory experiments and show that our implementation has highly scalable response capability.

These results demonstrate that our iSink architecture is able to support a range of capabilities while providing scalable performance. The results also demonstrate that