Measuring, Characterizing, and Tracking Internet Threat Dynamics

Michael Bailey, Farnam Jahanian, G. Robert Malan, Jose Nazario,
Dug Song and Robert Stone
Arbor Networks, Ann Arbor, MI, USA 48104

Networks are increasingly susceptible to a broad spectrum of vexing security and operational threats such as distributed denial of service attacks, zero-day worms, and routing exploits. The increasingly global scale of threats to the Internet demands a system capable of correlating data at a high level in order to identify and characterize these threats. In this talk we present an overview of a collaborative effort between Arbor Networks and Merit Network to develop, deploy and analyze data from a wide-area *blackhole monitoring system* whose goal it is to meet this new demand.

The unique properties of these threats have proved vexing for existing network and security measurement techniques and have prompted researchers to investigate new methods for tracing and characterizing these threats. However, for any new design to be effective, a monitoring system must deal with the several difficult properties of these new threats. First and foremost these threats are *globally scoped*, respecting no geographic or topological boundaries. Secondly, these threats exceptionally *virulent,* propagating to the entire vulnerable population in the Internet in a matter of minutes. This virulence has the effect of being exceptionally resource taxing creating side effects that pose problems for those that are outside the vulnerable population. To make matters worse, these threats often are *zero- day* threats, exploiting vulnerabilities for which not signature or patch has been developed.

To meet these design challenges we have proposed, built, and deployed a blackhole wide-area monitoring system for tracking Internet threat dynamics. Using this system we have been able to quantify Internet worm activities, measure wide-scale vulnerability probes by attackers, and estimate the type and severity of globally-scoped denial of service incidents. The Peakflow Blackhole system, which has been in active use since June of 2001, monitors a globally significant amount of address space ($1/256^{th}$), quickly identifying new threats and characterizes their scope all the while adaptively managing its available resources to continue to provide useful information during critical events. The system makes use of blocks of dark address space that while routable, contain no active hosts. Any traffic, then, is the result of some activity by an outside host, be it scanning, worm propagation, or backscatter. Like BGP off ramping techniques, this system takes advantage of existing low impact network infrastructure to provide a wealth of pre-filtered data for analysis. Two components of the system, the passive measurement module and the active measurement module manipulate this data. The passive module is responsible for watching for characterizing the traffic, looking for scans, backscatter, or the like, storing characteristics in a space-

conservative manner. The active module elicits payloads from an adaptively sampled number of end clients, reconstructing the client half of the payload and creating a finger print of the application request. These two modules work in conjunction with a third alerting module that looks for rapid changes in the characteristics of the overall network traffic as well as the rise of new types of signatures.

In this talk we will further describe the implementation of the Blackhole wide-area Internet monitor, a tool based on lightweight capture-distillation methodologies. We describe the components and their interactions, along with their role in threat analysis. We then discuss experimental results which measure the Internet-scale impact DoS events and worm propagation. We also present limitations of the proposed approach, as well as several future directions for the project.