Chapter 18

PITWALL: Tools, Techniques and Metrics for the Optimization of Enterprise Network Defense Systems

Subrata Acharya
Towson University, USA

ABSTRACT

The continuous growth in the Internet’s size, the amount of data traffic, and the complexity of processing this traffic give rise to new challenges in building high performance network devices. Such an exponential growth, coupled with the increasing sophistication of attacks, is placing stringent demands on the performance of network Information Systems. These challenges require new designs, architecture, and algorithms for raising situational awareness, and hence, providing performance improvements on current network devices and cyber systems. In this research, the author focuses on the design of architecture and algorithms for optimization of network defense systems, specifically firewalls, to aid not only adaptive and real-time packet filtering but also fast content based routing (differentiated services) for today’s data-driven networks.

INTRODUCTION

The conventional security of the Internet has been static, perimeter based and is oblivious to traffic dynamics in the network. The above model causes the lack of knowledge to identify, address and prevent anomalous behavior and maintain the desired operation of current network defense systems. In recent years, there has been tremendous effort towards the design and development of several techniques and strategies to deal with the above shortcomings. Unfortunately, the current solutions have been able to address only some aspects of security. This is primarily due to the lack of adaptation and dynamics in the design of such solutions.

To this effect, this research presents various algorithmic and architectural techniques that aims to address the shortcomings in terms of adaptation, speed of operation (under attack or heavily...
loaded conditions), and overall operational cost-effectiveness of such network defense systems. The dynamic network behavior and events in such networks can be measured and analyzed to aid the design of efficient systems. The proposed research presents approaches for Tier-I ISP networks and filtering routers to correlate the dynamic metrics and achieve situational awareness required to protect critical network infrastructure and data driven operations over the Internet. Thus, the overall goal is the design of reliable and survival network defense systems. The tools proposed also aim to offer the flexibility to include new approaches, and provide the ability to migrate or deploy additional entities for attack detection and defense.

Data communication networks have become an indispensable infrastructure for most industrial and academic institutions. Today’s Internet has undoubtedly become the largest public data network, enabling and facilitating both personal and business communications worldwide. The volume of traffic moving over the Internet, including all corporate networks, is expanding exponentially every day. As social dependence on such information systems continues to grow exponentially, a similar growth in threats is concurrently taking place. Traffic anomalies and attacks are commonplace in today’s network information systems. Attacks span the spectrum from computer worms and individual, localized intrusions aimed at gaining access to information and system resources, to coordinated and distributed attacks aimed at disrupting services and disabling critical infrastructure.

Furthermore, the number and frequency of these attacks has been increasing dramatically (Symantec Internet Security Report 2011), as the knowledge and tools required to carryout these devastating attacks are readily available on the Internet. As these attacks proliferate and grow in scope and sophistication, different institutions find themselves under growing pressure to place significant restrictions on open Internet access and collaboration. In this regard, institutions and organizations rely heavily on Intrusion Detection Systems (IDSs) for most network defense operations.

While such network defense systems have been designed, they are not geared towards extremely challenging network environments, which require support for high performance applications and open access policy for collaboration. Furthermore, these systems lack the critical on-time network aware information to identify and address the highly dynamic network environment while ensuring reliable, guaranteed and efficient network operation. Additionally, many of the existing intrusion detection systems are reactive in nature, and as such, are not practical in these dynamically changing environments. To overcome the above shortcoming, most of the Internet service providers still rely on offline traffic analysis and manual detection to deal with the various security threats and attacks. Current Tier-1 network defense systems are also limited by their lack of flexibility to deal with the ever-evolving characteristics of the attacks, in terms of diversity and intensity. While the use of machine learning based approaches holds promise, the schemes remain offline in nature, with potentially prohibitive high overhead in providing the real-time and situational significant knowledge for the efficient functioning of these network devices (Xiang et al 2005, Zhao et al 2003).

A comprehensive solution towards ensuring a practical defense against intrusions and attacks for such high-performance collaborative environments (i.e. Internet) must include a proactive, real-time, and adaptive solution aimed at the design of efficient and survival network systems. The necessary design goals that the design must meet are as follows:

- Accurate attack detection in real-time with minimal false alarms,