

Methodologies for Intrusion Detection in Communication Networks

Report of Activities 2008/2009

Eduardo Rocha, Paulo Salvador and António Nogueira
University of Aveiro/Instituto de Telecomunicações
Aveiro, Portugal
e-mails: {eduardorocha, salvador, nogueira}@ua.pt

1 Abstract

In the recent years, we have witnessed a huge increase in the number and variety of Internet applications. Consequently, the need for an accurate mapping of this new traffic to their corresponding applications has also increased in order to allow Service Providers (SPs) to provide better Quality-of-Service (QoS) standards, implement traffic engineering methodologies. Moreover, we have also witnessed a growth on the number and diversity of security attacks to network users and systems. Indeed, in the recent years, several new forms of attacks have taken place in the Internet and these are becoming more distributed and consequently, more difficult to detect and prevent. Therefore, ISPs need to gain a better understanding of the traffic flowing in their networks in order to deploy efficient security strategies.

Research in Intrusion Detection is a very mature field that has developed over the years. In fact, methodologies used on an initial stage became inappropriate due to the evolution of Internet services and applications. As a consequence, new methodologies incorporate new methods of analysis of the traffic/host activities. However, there are still several flaws existing in the current Intrusion Detection research. First of all, the lack of a tool able to perform detection in both encrypted and non-encrypted traffic scenarios. In the presence of encrypted traffic, network-based IDSs (NIDS), which analyze network traffic in search for known or anomalous activities, are not able to access packet's headers and payloads. This fact obstructs such systems from performing Intrusion Detection. On the other hand, on non-encrypted traffic scenarios, a larger quantity of information is available and there is a lack of tools and methodologies able to analyze such amount of data and to perform correlation between the most important. Such flaw will be addressed in our proposal since we include the study of methodologies able to perform the detection of unknown and stealth threats in encrypted and non-encrypted traffic scenarios. Moreover, the real-time detection of such threats is of crucial importance to provide protection to hosts and networks. Thus, the mentioned methodologies will be analyzed and compared in a real-time classification scenario. In this presentation we will describe the work developed during this year's research. This consists of the development of methodologies for traffic classification and for the identification of Internet attacks based on the analysis of multiscale characteristics extracted from raw traffic statistics. Since all the analyses are based on statistical informations, the methodology is able to perform identification on encrypted scenarios.