Chapter XIII
Designing Light Weight Intrusion Detection Systems: Non-Negative Matrix Factorization Approach

Václav Snášel
VSB—Technical University of Ostrava, Czech Republic

Jan Platoš
VSB—Technical University of Ostrava, Czech Republic

Pavel Krömer
VSB—Technical University of Ostrava, Czech Republic

Ajith Abraham
Norwegian University of Science and Technology, Norway

ABSTRACT

Recently cyber security has emerged as an established discipline for computer systems and infrastructures with a focus on protection of valuable information stored on those systems from adversaries who want to obtain, corrupt, damage, destroy or prohibit access to it. An Intrusion Detection System (IDS) is a program that analyzes what happens or has happened during an execution and tries to find indications that the computer has been misused. This chapter presents some of the challenges in designing efficient ad light weight intrusion detection systems, which could provide high accuracy, low false alarm rate and reduced number of features. Finally, the authors present the Non-negative matrix factorization method for detecting real attacks and the performance comparison with other computational intelligence techniques.

INTRODUCTION TO INTRUSION DETECTION SYSTEMS

Intrusion detection system were proposed to complement prevention-based security measures. An intrusion is defined to be a violation of the security policy of the system; intrusion detection thus refers to the mechanisms that are developed to detect violations of system security policy. Intrusion detection is based on the assumption that intrusive activities are noticeably different from normal system activities and thus detectable. Intrusion detection is not introduced to replace prevention-based techniques such as authentication and access control; instead, it is intended to complement existing security measures and detect actions that bypass the security monitoring and control component of the system. Intrusion detection is therefore considered as a second line of defense for computer and network systems. Generally, an intrusion would cause loss of integrity, confidentiality, denial of resources, or unauthorized use of resources. Some specific examples of intrusions that concern system administrators include (Bishop, 2003):

- Unauthorized modifications of system files so as to facilitate illegal access to either system or user information.
- Unauthorized access or modification of user files or information.
- Unauthorized modifications of tables or other system information in network components (e.g. modifications of router tables in an internet to deny use of the network).
- Unauthorized use of computing resources (perhaps through the creation of unauthorized accounts or perhaps through the unauthorized use of existing accounts).

Some of the important features an intrusion detection system should possess include:

- Be fault tolerant and run continually with minimal human supervision. The IDS must be able to recover from system crashes, either accidental or caused by malicious activity.
- Possess the ability to resist subversion so that an attacker cannot disable or modify the IDS easily. Furthermore, the IDS must be able to detect any modifications forced on the IDS by an attacker
- Impose minimal overhead on the system to avoid interfering with the normal operation of the system.
- Be configurable so as to accurately implement the security policies of the systems that are being monitored. The IDS must be adaptable to changes in system and user behavior over time.
- Be easy to deploy: This can be achieved through portability to different architectures and operating systems, through simple installation mechanisms, and by being easy to use by the operator.
- Be general enough to detect different types of attacks and must not recognize any legitimate activity as an attack (false positives). At the same time, the IDS must not fail to recognize any real attacks (false negatives).

An IDS maybe be a combination of software and hardware. Most IDSs try to perform their task in real time. However, there are also IDSs that do not operate in real time, either because of the nature of the analysis they perform or because they are meant for forensic analysis (analysis of what happened in the past to a system). There are some intrusion detection systems that try to react when they detect an unauthorized action. This reaction usually includes trying to limit the damage, for example by terminating a network connection.

Since the amount of audit data that an IDS needs to be examined is very large even for a small network, analysis is difficult even with