Chapter 3
Synthesis of Supervised Approaches for Intrusion Detection Systems

Ahmed Chaouki Lokbani
Taher Moulay University of Saida, Algeria

Ahmed Lehireche
Djillali Liabes University of Sidi Bel Abbes, Algeria

Reda Mohamed Hamou
Taher Moulay University of Saida, Algeria

Abdelmalek Amine
Taher Moulay University of Saida, Algeria

ABSTRACT

Given the increasing number of users of computer systems and networks, it is difficult to know the profile of the latter, and therefore, intrusion has become a highly prized area of network security. In this chapter, to address the issues mentioned above, the authors use data mining techniques, namely association rules, decision trees, and Bayesian networks. The results obtained on the KDD ’99 benchmark have been validated by several evaluation measures and are promising and provide access to other techniques and hybridization to improve the security and confidentiality in the field.

INTRODUCTION AND PROBLEMATIC

Currently computers and the Internet in particular play an increasingly important role in our society. Networks and computer systems have become today an indispensable tool for the proper functioning and development of most companies. Thus, computer systems and networks are deployed in various fields such as banking, medicine or the military. The increasing interconnection of these various systems and networks has made them accessible to a diverse population of users that continues to increase. These users, known or unknown, not necessarily full of good intentions to these networks. In fact, they may be trying to access sensitive information to read, modify or
Intrusion detection consists in discover or identify the use of a computer system for purposes other than those intended. Many mechanisms have been developed to ensure the security of computer systems and particularly to prevent intrusions, unfortunately, these mechanisms have limitations. In fact, computer systems have vulnerabilities that allow attackers to bypass prevention mechanisms. For this, a second line of defense is necessary: intrusion detection. For each system, a security policy must be defined to guarantee the security properties that must be made by the latter. This policy is expressed by rules, setting three distinct objectives:

- The confidentiality—that is to say, the non-occurrence of unauthorized disclosure of information;
- Integrity that is to say, the non-occurrence of improper alterations of information;
- The availability is to say being ready to use.

In this study, we define intrusion, a violation of one of these three objectives. Several approaches have been developed to ensure that the security policy defined for a computer system is respected. It can indeed be circumvented by a malicious user or simply a lack of design can be the source of a breach of it. Artificial intelligence has seen many methods such as data mining and its various techniques that will be used for intrusion detection.

In this article we are experiencing some data mining techniques namely association rules, Bayesian networks and decision trees in the area of intrusion detection. The intrusion detection system designed and will be tested on a benchmark called KDD’99 which is a structured database that will be detailed later.

**STATE OF THE ART**

Intrusion detection is another procedure used by security personnel to protect the company against attacks. In his concept, intrusion detection tries to detect hackers trying to penetrate a system. Theoretically, detection systems trigger an alarm only when an attack succeeds. Intrusion detection can also help to proactively identify threats, because it provides guidance and gives warning of the threat of an attack is intercepted.

The concept of intrusion detection system was introduced in 1980 by James Anderson. But the subject has not been very successful. It was not until the publication of an intrusion detection model by Denning in 1987 to mark, really the start of the field.

The research in the field is then developed, the number of prototypes has increased enormously. A lot of money has been invested in this type of research in order to increase the safety of its machines. Intrusion detection has become an industry mature and proven technology: almost all the simple problems have been solved, and no major progress has been made in this area in recent years, software vendor’s focus more improves the existing detection techniques.

Some tracks remain relatively unexplored:

- Mechanisms to respond to attacks,
- The architecture for intrusion detection systems distributed
- Standards for interoperability between different systems, intrusion detection,
- The search for new paradigms to perform intrusion detection.
Related Content

Digital Evidence
[www.igi-global.com/chapter/digital-evidence/43810?camid=4v1a](www.igi-global.com/chapter/digital-evidence/43810?camid=4v1a)

Globalization and Data Privacy: An Exploratory Study
[www.igi-global.com/article/globalization-data-privacy/46101?camid=4v1a](www.igi-global.com/article/globalization-data-privacy/46101?camid=4v1a)

Fair Electronic Exchange Based on Fingerprint Biometrics
[www.igi-global.com/article/fair-electronic-exchange-based-fingerprint/37584?camid=4v1a](www.igi-global.com/article/fair-electronic-exchange-based-fingerprint/37584?camid=4v1a)

Global Analysis of Security and Trust Perceptions in Web Design for E-Commerce
[www.igi-global.com/article/global-analysis-security-trust-perceptions/64343?camid=4v1a](www.igi-global.com/article/global-analysis-security-trust-perceptions/64343?camid=4v1a)