UDC 004.73 (043.2)

Miatovych R.
National aviation university, Kyiv

METHOD OF DETECTION EXTERNAL INTRUSIONS TO THE LAN

Computer networks bring us not only the benefits, such as more computing power and better performance for a given price, but also some challenges and risks, especially in the field of system security. During the past two decades, significant effort has been put into network security research and several techniques have been developed for building secure networks. Packet filtering plays an important role in many security-related techniques, such as intrusion detection, access control and firewall. A packet-filtering system constitutes the first line of defense in a computer network environment. The key issues in the packet-filtering technique are efficiency and flexibility. The efficiency refers to the ability of a filter to quickly capture network packets of interest, while the flexibility means the filter can be customized easily for different packet patterns.

In this thesis, presented a real-time packet-filtering module, which can be integrated into a large-scale network intrusion detection system. The important features of ASL that are not provided by other packet-filtering systems are protocol independence and type safety. ASL provides a number of new features that distinguish it from other languages used for intrusion detection and packet filtering, such as packet structure description and protocol constraint checking[1].

The methods used by network intrusions can be different from one to another. However, the nature of most network intrusions is based on “malicious” network traffic, which either has invalid value inside a field of a packet, or features incorrect combination or sequence of packet segments. With this observation, can use packet-filtering technique in building network intrusion detection systems.

However, packet filter faces new challenges for the intrusion detection purpose, like high-volume data, no packet dropping, and requirement for system flexibility and scalability. In this thesis, borrowed some idea from the adaptive pattern matching technique and applied it to our packet-filtering module for a large-scale intrusion detection framework. One of the key components in approach is a specification language ASL, which is used to describe the patterns for the packets to be captured. ASL provides a number of features in facilitating pattern writing and filter construction, such as packet structure description and automatic packet type checking.

Building an efficient filter is crucial to the overall system performance. Presented an elegant algorithm in filter construction. The main concern is how to select a variable or an offset inside a packet to be inspected at a node of a filter automaton. The primary goal is to minimize pattern matching time and the size of the automaton.

References

1. *Larry J. Hughes, Jr.* Actually Useful Internet Security Techniques, New Riders Publishing, Indianapolis, IN, 2005.

Supervisor – V.I. Nadtochiy, PhD