Keynote Speaker

Detection System for Anomaly Attacks using Statistical Methods

Takuo Nakashima^{a,*}

^aTokai University, Kumamoto, Japan

*Corresponding Author: taku@ktmail.tokai-u.jp

Abstract

The computer systems connected to the Internet are exposed the threats of DoS/DDoS attacks aiming to destroy the server functions. The malicious users hijack the vulnerable PCs and generate the attacking PCs called as BOT. A large number of BOTs sends a huge number of anomaly packets to paralyze the server functions. The early detection methods for these anomaly packets are required to sustain the damage of DoS/DDoS attacks. Our previous researches have clarified that the source IP address and destination port number are efficient statistical variables to view the anomaly packet property.

In this speech, we show EMMM (Entropy-based Multidimensional Mahalanobis-distance Method) method for entropy value and CSDM (χ square based Space Division Method) method for χ square value using multi statistical variables. The experiments to verify our two proposed methods were conducted using source IP address, destination port number and arriving interval of packets. We could extract the following results. Firstly, EMMM could decrease the value of False-Positive and False-Negative. Secondly, CSDM could increase the F-metric. In the experiments using the same condition of parameters such as probability valuables and window width, CSDM enlarges the F-metric compared to EMMM.