Research on Background Radiation Packets over the Internet and Threat Detection Methods

by

MASAKI　ISHIGURO

Submitted to
Japan Advanced Institute of Science and Technology
In partial fulfillment of the requirements
For the degree of
Doctor of Philosophy

Supervisor: Professor Dr. Yoichi Shinoda

School of Information Science
Japan Advanced Institute of Science and Technology

March 2009

Abstract

Network attacks caused by computer worms or fraudulent accesses pose great threats to today's information-communication society. We propose new methods for early detection and warning of threats such as outbreaks of new types of worms based on analyses of malicious packets monitored over the Internet. We can capture malicious packets over the Internet by monitoring IP addresses where any network service is provided, because any legitimate packets are not supposed to be sent to those not-used IP addresses. By monitoring multiple IP addresses widely over the Internet, we can detect threats earlier than by just monitoring their own internal network by using traditional intrusion detection system and take some measures to protect their network before suffering damage. We monitor malicious packets targeted to network ports in which vulnerability of network software is publicly fixed by patch. Those packets are not considered to be critical. However, it is strongly demanded to detect highly critical packets among other non critical malicious packets. In order to respond to this demand, statistical characteristics and trend of non critical packets should be clarified and method to evaluate threat level from malicious packets including non critical and critical packets.

In this research, we analyzed distribution of malicious packets over the IP address space and provide experimental evidence of extreme locality of packets distribution and periodical time-series trends. Then, we present our systematic classification of threat detection methods based on a dimension of macroscopic threat analysis and microscopic threat analysis and another dimension of time feature analysis and space feature analysis. In macroscopic threat analysis, we consider source of malicious packets as a population of attackers and detect change of population. In microscopic threat analysis, we separate time-series events of malicious packets by source IP addresses and detect change of behavioral pattern of attacks. In time-feature analysis, we detect change of features based on time-series pattern. In space-feature analysis, we detect change of features based on special distribution of packets over the Internet.

We propose the following new kinds of methods covering four domain of analysis method classified as described:

- An anomaly detection method based Baysian estimation and trend analysis.
- An anomaly detection method based on time-frequency analysis.
- A threat detection method based on structural analysis of access graph
- An anomaly detection method based on auto-correlation analysis

We evaluate these methods by applying them to malicious packets monitored in real-world Internet and compare the methods with traditional method to show their effectiveness and advantage. Based on these evaluation, we discuss the effect obtained by combinational application of our methods.