第19部

ネットワーク管理とセキュリティ

Glenn Mansfield Keeni、Hiroshi Tsunoda

第１章　Introduction

The WIDE-Netman WG has been carrying out research and development to make the Internet more manageable and secure. The WG is working on network traffic traces to detect events in the network. With an eye on Zero Trust to achieve good security, the WG is also working on developing a framework that expands the scope of management and monitoring and is cost-aware too. As a community-support effort the WG is working on development of tools that will facilitate cyber patrolling of social networking services (SNSs).

第２章　Mining for events in network traffic traces

The WG attempted to detect events by examining network traffic traces from an operational intranet. The WG has been working on monitoring and analysing packets destined to unused IPv4 addresses in the intranet for uncovering hidden, potentially malicious, activities. This year, the WG extended the monitoring system to include packets destined to unused addresses in the IPv6 intranet. The progress of this work is presented in [174].

The WG is also working on monitoring traffic sent and received by an individual host in an intranet. The monitored traffic will be analyzed in conjunction with the log information on the host in order to obtain a more complete understanding of the host's behavior. Currently, the WG is prototyping the monitoring and analysis system. The progress of this work is presented in [175].

The WG will continue to explore and examine available data for information that can be mined about network devices and their activities.

第３章　Exhaustive management and monitoring to achieve Zero Trust

To make the network secure, it is necessary to implement the concepts of Zero Trust which essentially require checking and confirming every facet of the network. This would require exhaustive management and monitoring which, considering the practicalities of cost, is a very difficult target. In continuation of our research and development work to make the Internet more manageable and secure, we have set our targets as follows:

- o make management effective by minimizing cost of management and maximizing scope of information available for management.

- o use the information made available by effective management to obtain a better sense of the network and its dynamics for security.

The increased transparency will be a significant step towards Zero Trust networks.

第４章　Tools for efficient cyber patrolling of social networking services (SNSs)

Social networking services (SNSs) foster quick and easy

communication among people, but there is a downside too. There are posts offering to sell illegal drugs, soliciting child prostitution and the like. In the country, prefectural police headquarters are seeking the help of civilian volunteers to find and report harmful SNS posts. This activity is called "cyber patrolling". The WG is looking at supporting cyber patrols by developing tools that will make the activity easier. As a starter, the WG has developed a simple GUI application that allows volunteers to report harmful posts, easily. This work is presented in [176].

第 5 章　Plans for 2022.

The WIDE-Netman WG will continue the investigation on data collection on a large scale and from small devices. We will continue working on

a. mining for events in network traffic traces
b. developing a cost-aware framework that expands the scope of management and monitoring, leads to enhanced transparency of the network dynamics and realization of the Zero Trust concept.
c. development of tools to facilitate cyber patrolling

Copyright Notice