第18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 profiling hosts in the intranet from network traffic traces. The goal of this theme is expansion of the MUD (Manufacturer Usage Description) concept to the management of general purpose devices. With an eye on Zero Trust to achieve enhanced security, the WG is working on developing a framework that expands the scope of information available for monitoring and management and is cost-aware too. As a community-support effort, the WG is working on development of tools to facilitate cyber patrolling of social networking services (SNSs).

第２章　Profiling hosts from network traffic traces

The WG is doing research and development on characterizing the behavior of network hosts. The basic approach is to apply the MUD concept for access control, typically used for IoT devices, to general purpose network devices such as PCs and smartphones. In this context the Manufacturer Usage Description of a host will give the expected communication profile of a host. Unlike IoT devices, the communication patterns of general purpose network devices are neither deterministic nor predictive. Thus, a Manufacturer Usage Description for a general purpose device needs to be generated and updated based on activities of the target host. To understand the activities of every host by examining network traffic traces, the WG is working on monitoring, analyzing, and visualizing network flows sent from and received by hosts in the intranet. The WG is exploring methodologies to visualize host profiles in an easy-to-understand manner. The progress of this work is presented in [68、69、70].

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　Towards Zero Trust: achieve increased transparency by expanding the scope of information available to management systems.

To make the network secure, it is necessary to implement the concepts of Zero Trust which essentially requires checking and confirming every facet of the network and in every possible detail. This would require exhaustive monitoring and management which, considering the practicalities of cost, is a very difficult target. As a first step towards Zero Trust, we expand the scope of transparency of interactions in the intranet and with the internet, while keeping an eye on cost and complexity.

o the scope of information on intranet interactions is expanded from the MAC and IP addresses of connected hosts to include the MAC and IP addresses of the (attempted) peer connections.

o the scope of information on internet interactions is expanded from traffic volume (counters for protocols, ports, hosts, destinations, etc.) to include the IP addresses (hosts/domains) and ports of the network flows seen at the entry point of the intranet.

The increased transparency provides a significantly deeper insight into network behavior of the hosts in the intranet. For instance, an attempted access/connection from a user terminal to another user terminal maybe considered suspicious and worth further examination. On the other hand, an access to a network in a domain or country may raise the level of suspicion and call for further investigation if not, blocking and/or quarantining the corresponding host in the intranet.

The (attempted) peer connections in an intranet may be detected by a single sensor in the intranet from broadcast packets and the internet interactions may be monitored by a single flow monitor at the entry point of the intranet. From the cost and complexity point of view that looks reasonable.

第４章　Development of tools for efficient cyber patrolling

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 "cyber patrol" i.e. find and report harmful SNS posts. The WG has been looking at supporting cyber patrols by developing tools that will make cyber patrolling easier.

The WG has developed a push-based system for asking volunteers to judge whether a post should be reported. The developed system conducts keyword searches on Twitter to find posts with harmful words. The system scores the degrees of harmfulness of posts based on machine-learning technology and sends posts with high degrees of harmfulness to volunteers. They just make a final judgment. This work is presented in [71、72].

In recent years, photo-sharing SNSs have become popular. In such SNSs, often harmful text messages are embedded in posted photos or images. Simple text based keyword search fail to detect such harmful texts. To address this issue, the WG has tested OCR (Optical Character Recognition) technology and shown its usability. We could detect harmful messages from a sample of 1,327 images using Google's Cloud Vision API with a success rate of 96%. This work is presented in [73、74].

第５章　Plans for 2023.

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. application of the MUD concept for access control of general purpose devices.
b. development of a cost-aware framework that expands the scope of monitoring and management, leads to enhanced transparency of the network dynamics and is closer to a realization of the Zero Trust concept.
c. development of tools to facilitate cyber patrolling

Copyright Notice