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 has focussed on the security aspect of Internet of Things (IoT) and proposed an operational model which has built-in security. The WG is working on network traffic traces to detect events in the network. The WG is also working on automatic generation of maps showing network configuration in SDN-based intranets.

第２章　Societal model for Internet of Things

For securing IoT, the WG proposed the societal model, a simple operational model which has built-in security. Its requirements were examined and its feasibility was established using off-the-shelf technology available in the Internet standard network management framework. The WG has been working on the practical prototype implementation of the model. This year, the WG attempted to develop an advanced prototype implementation that supports bulk data transfer and can handle large multimedia data such as images and photos efficiently. The progress of this work is presented in [99]. The WG is attempting to develop a new prototype implementation adopting new Internet standard network management protocol, NETCONF. Preliminary results are presented in [100].

The WG will continue work on providing elemental technologies of the model to make the model practical.

第３章　Mining for events in network traffic traces

The WG attempted to detect events by examining network traffic traces from the darknet and from an operational intranet (a livenet). For efficient event detection in darknet traffic, the WG is trying to automate the traffic analysis and its reporting. The progress of this works is presented in [101]. The WG analyzed UDP packets in darknet traffic by focusing on the similarity of packet payloads to find collaborative scanners. The progress of this work is presented in [102].

For livenet traffic, the WG is attempting to analyze the interaction pattern among terminals in the intranet by examining the source addreses in ARP (Address Resolution Protocol) requests and the address for which ARP resolution is requested. The detected interaction pattern will be useful in detecting abnormal activities e.g. scanning, in the intranet. The progress of this work is presented in [103]. Also, the WG is working on the monitoring and analysis of packets destined to unused IP addresses in the intranet for uncovering hidden, potentially malicious, activity. The progress of this work is presented in [104].

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

第４章　Visualization of SDN-based intranet topology

SDN (Software Defined Networking) technology enables an operator to control the network topology dynamically. This feature is being increasingly deployed for flexible topology construction, even in intranets. Network management and monitoring systems must adapt to this quasi-dynamic nature of SDN-based intranets. The WG is working on a prototype implementation for automatic generation of maps for visualizing the dynamic topology in SDN-based intranets. The WG has confirmed that the network topology for a simple network with several SDN switches can be visualized with our prototype implementation. The progress of this work is presented in [105].

第５章　Plans for 2021.

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. a security model for Internet of Things

b. mining for events in network traffic traces

c. visualizing topology of SDN-based intranets

Copyright Notice