第18部

ネットワーク管理とセキュリティ

Glenn Mansfield Keeni、Hiroshi Tsunoda

1 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 in the development of MIB modules for multicast in BGP/MPLS L3 and L2 VPN networks.

2 Societal model for Internet of Things

For securing IoT, the WG has proposed the societal model, a simple operational model which has built-in security. The requirements of the societal model has been examined and its feasibility is established using off-the-shelf technology available in the Internet standard network management framework.

The societal model does look attractive with security risks greatly reduced by moving the onus of handling security related matters from the potentially resource-constrained IoT device to a security proficient guardian IoT device. The difference between the societal model and traditional security measures in the Internet are examined. The results are presented in [52].

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

3 Mining for events in network traffic traces

The WG attempted to detect events by examining network traffic traces from the darknet and from the operational Internet. The WG analyzed the stability of darknet traffic and compared the traffic data for stable and unstable time slots from the viewpoint of the randomness of IP addresses and ports by evaluating the normalized entropy. The WG also attempted to adopt a network-state evaluation method which focuses on the occurrence probability matrices of the correlation coefficient of traffic observables for event detection in darknet traffic. Analysis results showed that events like backscatters and scans could be detected, using the above techniques, in the darknet.

The results are presented in [53, 54].

The WG will continue to examine the information that can be mined from the network about network devices and their activities.

4 Managing multicast in BGP/MPLS L3 and L2 VPN

The BGP (Border Gateway Protocol) Enabled ServiceS (BESS) working group in IETF is working on defining, specifying, and extending network services based on BGP.

WIDE-Netman WG has worked on management aspect of the protocols and is developing MIB modules related to management of multicast in BGP/MPLS L3 and L2 VPN

(Virtual Private Network).

Two documents have been published as proposed standards.

o RFC 8502 [55] defines textual conventions (TCs) and common managed objects that will be used by other Management Information Base (MIB) modules for monitoring and/or configuring BGP/MPLS L2 and L3 VPN that support multicast.

o RFC 8503 [56] defines managed objects to configure and/or monitor MVPNs (Multicast VPNs). Most of the managed objects are common to both PIM-MVPN (MVPN using Protocol Independent Multicast for exchanging customer multicast routing information) and BGP-MVPN (MVPN using BGP for exchanging customer multicast routing information) and some managed objects are BGP-MVPN specific.

5 Plans for 2019.

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. activity monitoring in intranets
d. collecting connection information from network devices, using the information for network visualization and for efficient rechability checking

6 Copyright Notice