

第17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. The WG continues to work on Syslog management.

2. Operational model for secure Internet of Things

The WG proposed a simple operational model for IoT, the societal model [117]. The basic concept of the model is borrowed from human society - infants are protected by adults. This natural security mechanism works very well for IoT networks which seem to have inherently weak security mechanisms. The WG discussed the requirements of the societal model and presented a practical solution that fulfills the core requirements. The WG established the feasibility of the model through a proof-of-concept implementation. 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 concept of traffic stability was used in the analysis. The WG analyzed the stability of darknet traffic at different timescales. Analysis results showed that some suspicious events like backscatters, scans were found from darknet. The results are presented in [118] [119].

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

4. Management information bases for multicast in BGP/MPLS L3 and L2 VPN

BGP (Border Gateway Protocol) Enabled ServiceS (BESS) working group in IETF working on defining, specifying, and extending network services based on BGP. BESS working group is working on providing data models for modeling, managing, and operating multicast in BGP/MPLS (Multi-Protocol Label Switching) Layer 3 (L3) and Layer 2 (L2) VPNs (Virtual Private Networks). Netman WG is working on management aspect of the protocols and is developing MIB modules [120] [121] related to management of multicast in BGP/MPLS L3 and L2 VPN.

5. Managing syslog

The WG has discussed the necessity and importance of monitoring and managing logging systems. A logging system must be monitored and managed just like any other component of the ICT infrastructure, to ensure that logs are being collected and archived as desired. The WG is working on the basic design of a Management Information Base module which will

make it possible to monitor and control syslog applications [122].

6. Plans for 2018.

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

- a. a security model for Internet of Things
- b. mining for events in network traffic traces
- c. activity monitoring in intranets
- d. efficient reachability testing based on network configuration information
- e. management information bases for multicast in BGP/MPLS L3 and L2 VPN

Copyright Notice

Copyright (C) WIDE Project 2018. All Rights Reserved.