Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: September 22, 2016

R. Moskowitz
HTT Consulting
S. Hares
L. Xia
Huawei
March 21, 2016

Security alerts over the first MILE
draft-moskowitz-firstmile-00.txt

Abstract

This document describes a pub/sub styled protocol to send security alerts to a security monitor that can feed into MILE and other management platforms. It uses data structures from NETCONF, MILE, and IPFIX to manage the reporting and report security alerts.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on September 22, 2016.

Table of Contents

1. Introduction

This document proposes a set of protocols to automate the reporting of security alerts to the various monitoring systems. The intent is primarily to automate the input of security events to the MILE environment (RID [RFC6545] and IODEF [I-D.ietf-mile-rfc5070-bis]). Any authorized monitoring system can subscribe to any of the security alerts reports.

An Internet security defense device first registers with a security alert monitoring system. At this point the content and protocol used has not been identified. Since such a registration is normally at 'quiet time', the registration does not occur during a network congested time and can use some HTTPS-based service. At this time both systems exchange their X.509 identifiers to be used for the sub/pub security and identification.

Once a defense device is registered, the monitoring system can subscribe to it for those alerts in needs to receive. The subscription protocol should use NETCONF [RFC6536] with the publication/subscription push service [I-D.ietf-netconf-yang-push]. If the system needs a "pull" service, the NETCONF and I2RS subscription service could be expanded to support a pull service.

Any secure NETCONF transport that this pub/sub service support can be used.

The defense device publishes security alerts to subscribed monitors using IODEF or IPFIX [RFC7011] data structures. The protocol(s) for these reports are discussed within this document.

2. Terms and Definitions

2.1. Requirements Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

3. Problem Space

At the time of developing this document, there is no IETF defined set of standardized security alert messages and protocols. Administrators of systems which provide MILE service currently use "cut-and-past" where they cut selected messages from proprietary monitoring systems and past these messages into their MILE environment. The intent here is to standardize and automate this process. It is recognized that many of these alerts are too detailed to be actionable. Some implementations of the alert monitor will include analytic tools to select the actionable information from the alerts. Alerts which are too detailed to be actionable or alerts which include analytical tools are outside of any standardizing process.

Many of the needed alerts are scattered throughout the various standards like IPFIX and IODEF, but are not collected together as recognized security alerts that should be aggregated into a reporting framework.

4. The first mile of security alerts

There are three components to the first MILE process

- Register
- Subscribe
- Publish

4.1. Register

An Internet security defense device first registers with a security alert monitoring system. This is typically done at the time the device is installed, but may occur later as the device is registered to more monitoring systems. There is no theoretical limit on the

number of monitors a device is registered to. The limit within a system are practical limits based on internal limits within the device.

Most monitors will be commercial and the registration will be based on existing business relationships. One such example is the ISP's security monitor. It is possible that a CERT may accept direct registration without a business relationship. However this may require more study to ensure that this will not introduce potential attacks of false reporting to CERTs.

The actual content of the registration has not been determined. Minimally it needs to include

- Identifiers (e.g. X.509 certificates)
- Reports available from device (i.e. what to subscribe to)
- Subscription protocols(s)
- Publication protocols(s)

A device can alter any of its registered information at any time as well as cancel a registration.

4.2. Subscribe

Once a defense device is registered, the monitoring system can subscribe to it for those alerts in needs to receive. This is typically done via NETCONF, but is controlled by what the device registered as supported subscript protocols.

A monitor can subscribe or unsubscribe for reports at any time. With the first subscription, a secure communication transport will be enabled from the device to the monitor. See Section 4.3 for more on the this secure transport.

4.3. Publish

The defense device publishes security alerts to subscribed monitors. The reports will be sent over the subscribed protocol using the subscribed data model, either IODEF or IPFIX.

Since these alerts may be reported during an attack that degrades communications, many of the DOTS requirements [I-D.ietf-dots-requirements] apply here. One that doesn't is the bi-directional requirement. Even so, the same security and transport design used for DOTS should be used here.

5. first MILE data model

The data model will support the constraints of the NETCONF publication/subscription model [I-D.ietf-netconf-yang-push], and the NETCONF module library function [I-D.ietf-netconf-yang-library] which indicates pub/sub support within a model. If the MILE service which to utilize non-persistent (aka ephemeral) data that disappears on reboot, the netconf publication/subscription model will support non-persistent configuration.

Work on the data model is an open item.

6. IANA Considerations

No IANA considerations exist for this document at this time.

7. Security Considerations

An attacker that can disable first MILE may be able to attack a device at will as those monitoring it expect these attacks to show up on their monitor. As such each part of the firstMILE system will need the complete security services that are defined or referenced here.

8. Contributors

TBD

9. References

9.1. Normative References

[I-D.ietf-netconf-yang-library]
Bierman, A., Bjorklund, M., and K. Watsen, "YANG Module Library", draft-ietf-netconf-yang-library-04 (work in progress), February 2016.

[I-D.ietf-netconf-yang-push]
Clemm, A., Prieto, A., Voit, E., Tripathy, A., and E. Einar, "Subscribing to YANG datastore push updates", draft-ietf-netconf-yang-push-01 (work in progress), February 2016.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

9.2. Informative References

[I-D.ietf-dots-requirements]
Mortensen, A., Moskowitz, R., and T. Reddy, "DDoS Open Threat Signaling Requirements", draft-ietf-dots-requirements-00 (work in progress), October 2015.

[I-D.ietf-mile-rfc5070-bis]
Danyliw, R., "The Incident Object Description Exchange Format v2", draft-ietf-mile-rfc5070-bis-17 (work in progress), March 2016.

[RFC6536] Bierman, A. and M. Bjorklund, "Network Configuration Protocol (NETCONF) Access Control Model", RFC 6536, DOI 10.17487/RFC6536, March 2012, <http://www.rfc-editor.org/info/rfc6536>.

[RFC6545] Moriarty, K., "Real-time Inter-network Defense (RID)", RFC 6545, DOI 10.17487/RFC6545, April 2012, <http://www.rfc-editor.org/info/rfc6545>.

[RFC7011] Claise, B., Ed., Trammell, B., Ed., and P. Aitken, "Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of Flow Information", STD 77, RFC 7011, DOI 10.17487/RFC7011, September 2013, <http://www.rfc-editor.org/info/rfc7011>.

Authors' Addresses

Robert Moskowitz
HTT Consulting
Oak Park, MI 48237

Email: rgm@labs.htt-consult.com

Susan Hares
Huawei
7453 Hickory Hill
Saline, MI 48176
USA

Email: shares@ndzh.com

Liang Xia
Huawei
No. 101, Software Avenue, Yuhuatai District
Nanjing
China

Email: Frank.xialiang@huawei.com