Self-Descriptive SACM Telemetry based on YANG push/NETCONF and XMPP

IETF99 Hackathon Report
July 2017, Prague

Participants

Fraunhofer SIT: Henk Birkholz, Christoph Vigano
Huawei: Guangying (Walker) Zheng
Cisco: Nancy Cam-Winget

Goal

Create a prototype to expose available information from YANG/NETCONF enabled devices to facilitate posture collection and assessment in SACM. In particular, to enable timely exposure and availability of information, the use of YANG based notifications facilitated via the use of https://datatracker.ietf.org/doc/draft-ietf-netconf-yang-push/, https://datatracker.ietf.org/doc/draft-ietf-netconf-subscribed-notifications/, https://datatracker.ietf.org/doc/draft-ietf-netconf-netconf-event-notifications/, and to orchestrate and facilitate the availability of such information for SACM via use of XMPP https://datatracker.ietf.org/doc/draft-ietf-mile-xmpp-grid/.

Further, the hackathon prototype was also setup to prove feasibility and applicability by meeting the following SACM requirements:

- G-007 Data Partitioning
- G-009 Information Discovery
- G-011 Push and Pull Access
- G-012 SACM Component Interface
- G-013 Endpoint Location and Network Topology
- G-015 Data Access Control

Report Summary

The ability of the prototype to support the listed SACM requirements indicates that YANG push is a viable method to provide the desired security capabilities and deliver corresponding security-related telemetry timely.

Detailed Report

To realize the proof of concept, two pieces of network equipment were used, located in their respective remote location (PRC & USA), taking on the role of "data source" using YANG push as the acquisition method: a Cisco 3850 Catalyst Switch and a Huawei NE40E Router. YANG subscriptions are used to aggregate the corresponding NETCONF XML notifications via SACM collectors (the virtual component artifacts created as proof-of-concept on-site). Both consumption of periodic and on-change notification emission is implemented, successfully. Correspondingly, notifications are consumed and brokered via SACM collectors, successfully.

In regard to Event-Terminology, the resulting stream of subscribed notifications can be considered an Event-Stream. In the context of this Hackathon, we established the intermediate term "SACM Telemetry". The components that assess the "relevance" of content are the SACM Collectors. SACM Collectors retain the filter expressions used to create YANG subscription state on the data source. In consequence, they take on the "observer role" in respect to Notification-Streams and effectively are the decision points that decide "what is of interest" and broker the resulting Event-Streams via the corresponding security-information sharing domain.

SACM collectors encapsulate the incoming NETCONF XML notification telemetry in self-descriptive statements (an experimental proof-of-concept data model derived from the current SACM Information Model I-D https://datatracker.ietf.org/doc/draft-ietf-sacm-information-model/). Both message types – the NETCONF notifications and the SACM statements – are expressed in XML—at this point of implementation.

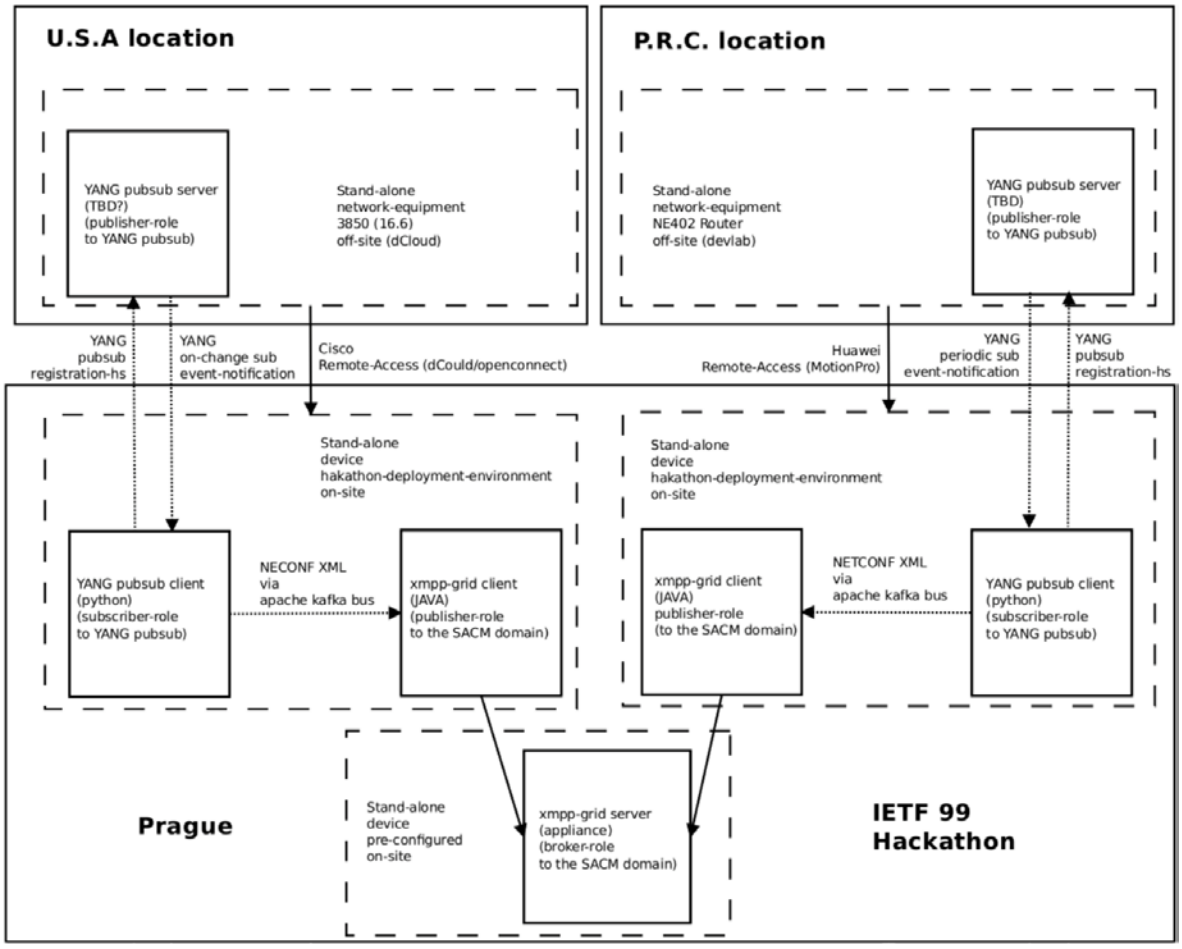
YANG push state and corresponding metadata is effectively confined to the application association of the YANG publisher and YANG subscriber. In order to facilitate solicited brokering of this vital metadata in conjunction with the pushed content itself, the SACM statements are used.
SACM statements compose self-describing bundles of data source output. YANG push in this effort is the only implemented data source. Hence, the focus of this SACM Hackathon effort is brokering self-descriptive messages about network equipment in a security automation domain.

A corresponding draft, illustrating the use of YANG push output in a SACM domain and including the experimental PoC data model was submitted during the IETF meeting: https://datatracker.ietf.org/doc/draft-birkholz-sacm-yang-content/.

Entities & Functions used in particular:

- Cisco Switch: using YANG Push to expose network topology information
- SACM Collector (Cisco): to expose YANG Push information to the XMPP-Grid
    - YANG Push client: attached to Cisco Switch to expose its information to the SACM Component (Collector) via on-change updates
    - XMPP-Grid client: attached to the XMPP-Grid broker to expose its information to the SACM Domain
- Huawei Router: using yang-push to expose session and routing information (ISIS & OSPF)
- SACM Collector (Huawei): to expose YANG Push information to the XMPP-Grid
    - YANG Push client: attached to Huawei Router to expose its information to the SACM Component (Collector) via periodic updates.
    - XMPP-Grid client: attached to the XMPP-Grid broker to expose its information to the SACM Domain
- XMPP-Grid Controller: to arbitrate and orchestrate the availability of the YANG Push information

The topology and the physical geo-locations are illustrated below:



Christoph was able to successfully augment the Cisco-XMPP-Client to receive push-notifications from both types of network equipment and made them available via the XMPP-Grid controller. Similarly, Walker and Christopher augmented the employed version of the NETCONF client software to create flows of on-change and periodic notifications originating from the network equipment as the data source.

To simplify next steps and integration of additional function, an internal kafka bus limited to the internal scope of each individual the SACM component prototypes was deployed. Kafka bus interfaces were implemented in each software function (i.e. ncc(lient) and xmpp-grid client) to enable interoperability of functions written in multiple languages (most prominently, JAVA, Python and C).