Network Device Threat Surface Management Modeling and Netconf/YANG

draft-hu-opsawg-network-element-tsm-yang-00

Feifei Hu, Danke Hong — China Southern Power Grid
Liang Xia — Huawei

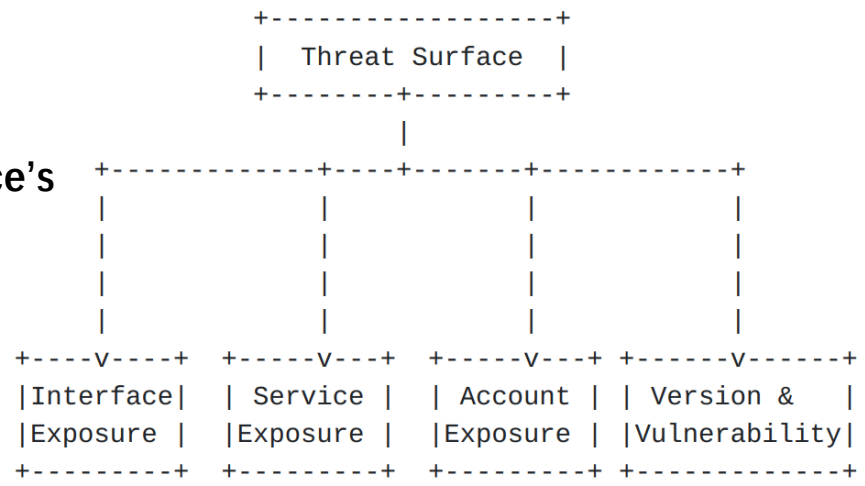
IETF 121
Dublin, Ireland

Background

- Goal: reduce network security risks during the usage of devices
- Method:
  - ✓ Security development: Define and implement its security posture/baseline.
  - ✓ Security OAM: increase security visibility. One specific and effective way is to monitor and manage the thread surface.
- What is thread surface:
  - ✓ Definition: the interface/service exposed to network and may potentially be attacked, which can be attack surface if it is both exposed and exploitable by adversaries.
  - ✓ A real attack surface example: the insecure SNMPv2 protocol with weak crypto algorithm (i.e., MD5, DES…)
- Similar IETF work:
  - ✓ Concluded Network Endpoint Assessment (NEA) and Security Automation and Continuous Monitoring (SACM) working groups [RFC5209][RFC8248].
  - ✓ [RFC9472] -- the extended MUD YANG model for SBOM and vulnerability information of devices, [I-D.ietf-opsawg-mud-tls] -- the extended MUD YANG model for (D)TLS profiles for IoT devices.

Network Device Threat Surface Modelling

Define: network device's threat surface information model



Interface Exposure: Unused Interfaces (physical or logical), IP interface exposure…

Service Exposure: Insecure protocols, Abnormal service IP address, Weak service security configuration, Abnormal Service Port…

Account Exposure: …

Version and Vulnerability: hardware revision, software revision, software patch revision

---

Define: how to collect all of this information (already defined in IETF interface yang DM, IP management yang DM…) via Netconf/yang interface

IP interface exposure information can be retrieved with NETCONF [RFC6241] Subtree Filtering mechanism:

```
<rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="101">
<get-data xmlns="urn:ietf:params:xml:ns:yang:ietf-netconf-nmda"
xmlns:ds="urn:ietf:params:xml:ns:yang:ietf-datastores">
<datastore>ds:operational</datastore>
<subtree-filter>
<interfaces xmlns="urn:ietf:params:xml:ns:yang:ietf-interfaces">
<interface> <name/> <type/> <enabled/> <oper-status/> <admin-status/> <if-index/> <phys-address/>
<ipv4> <address/> </ipv4> <ipv6> <address/> </ipv6>
</interface> </interfaces>
</subtree-filter> </get-data>
</rpc>
```

The realtime change of the above information can be notified on time with NETCONF pub/sub mechanisms [RFC8639][RFC8640] [RFC8641] :

```
<netconf:rpc xmlns:netconf="urn:ietf:params:xml:ns:netconf:base:1.0"
message-id="101"> <establish-subscription
xmlns="urn:ietf:params:xml:ns:yang:ietf-subscribed-notifications"
xmlns:yp="urn:ietf:params:xml:ns:yang:ietf-yang-push">
<yp:datastore xmlns:ds="urn:ietf:params:xml:ns:yang:ietf-datastores">
ds:operational </yp:datastore> <yp:datastore-subtree-filter>
<interfaces xmlns="urn:ietf:params:xml:ns:yang:ietf-interfaces">
<interface> <name/> <type/> <enabled/> <oper-status/> <admin-status/> <if-index/> <phys-address/>
<ipv4> <address/> </ipv4> <ipv6> <address/> </ipv6>
</interface> </interfaces> </interfaces>
</yp:datastore-subtree-filter> <yp:on-change/>
</establish-subscription> </netconf:rpc>
```

YANG Data Models for Security Configuration Check

draft-hu-opsawg-sec-config-yang-00

Feifei HU, Yu HUANG — China Southern Power Grid
Lei YAN — Huawei

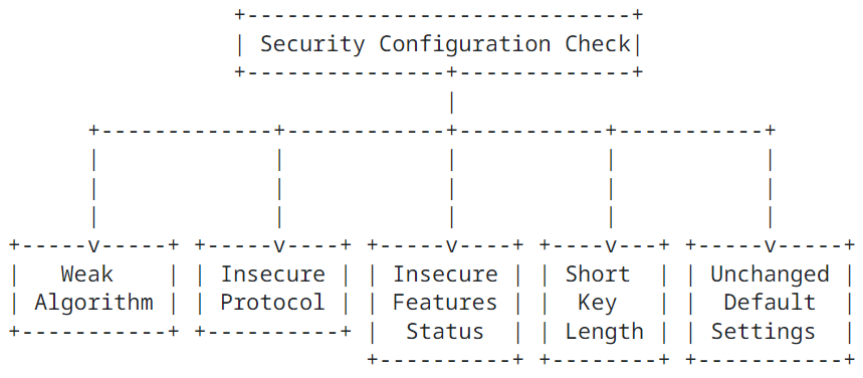
IETF 121
Dublin, Ireland

Background

- Goal: reduce network security risks during the usage of devices
- Method:
  - ✓ Security configuration collection: the manager collects security configuration information from devices..
  - ✓ Benchmark comparison: the collected configuration information will be compared with the security configuration benchmark to determine whether the configuration of devices is secure.
- Top 3 high-risk configuration items:
  - ✓ Default password: makes it easy for attackers to guess and successfully access the network.
  - ✓ Unnecessary opened ports: increase the exposed surface of the attack.
  - ✓ Insecure protocols or algorithms: greatly reduce the attack difficulty.
- Similar IETF work:
  - ✓ Concluded Network Endpoint Assessment (NEA) and Security Automation and Continuous Monitoring (SACM) working groups [RFC5209][RFC8248].
  - ✓ The security configuration benchmark of the management plane [I-D.lin-sacm-nid-mp-security-baseline] has been defined in SACM.

Network Device Security Configurations Modelling

Define: network device' security configurations information model



Weak algorithm: insecure algorithms, such as MD5, 3DES
Insecure protocol: the protocol without security mechanisms, such as TCP and HTTP, or the older version of the protocols, such as TLSv1.1 and SNMPv1
Insecure Features Status: all interfaces listening or binding, unconfigured security configurations, disabled security functions.
Short Key length: the key is not long enough to meet the security requirement.
Unchanged Default Settings: unchanged default certificates/PKI domains/keys/ports

---

Define: how to collect all of this information (some parts already defined in IETF) via Netconf/yang interface

Protocols	YANG models
TLS/DTLS	[RFC9645]
SNMP	[RFC7407]
SSH	[RFC9644]
IPsec	[RFC9061]
HTTP	[I-D.ietf-netconf-http-client-server]
TCP	[RFC9648]
UDP	[I-D.ietf-netconf-udp-client-server]

Algorithms supported by TLS can be retrieved with NETCONF [RFC6241] Subtree Filtering mechanism:

```
<rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="101">
<get-data xmlns="urn:ietf:params:xml:ns:yang:ietf-netconf-nmda"
xmlns:ds="urn:ietf:params:xml:ns:yang:ietf-datastores">
<datastore>ds:operational</datastore>
<subtree-filter>
<hello-params xmlns="urn:ietf:params:xml:ns:yang:ietf-tls-common“
xmlns:tlscmn="urn:ietf:params:xml:ns:yang:ietf-tls-common">
  <cipher-suites>
    <cipher-suite> <cipher-suite/> </cipher-suite>
  </cipher-suites>
 </hello-params>
</subtree-filter> </get-data></rpc>
```

The realtime change of the above information can be notified on time with NETCONF pub/sub mechanisms [RFC8639][RFC8640] [RFC8641] :

```
<netconf:rpc xmlns:netconf="urn:ietf:params:xml:ns:netconf:base:1.0"
message-id="101"> <establish-subscription
xmlns="urn:ietf:params:xml:ns:yang:ietf-subscribed-notifications"
xmlns:yp="urn:ietf:params:xml:ns:yang:ietf-yang-push">
<yp:datastore xmlns:ds="urn:ietf:params:xml:ns:yang:ietf-datastores">
ds:operational </yp:datastore> <yp:datastore-subtree-filter>
<hello-params xmlns="urn:ietf:params:xml:ns:yang:ietf-tls-common“
xmlns:tlscmn="urn:ietf:params:xml:ns:yang:ietf-tls-common">
  <cipher-suites>
    <cipher-suite> <cipher-suite/> </cipher-suite>
  </cipher-suites> </hello-params>
</yp:datastore-subtree-filter> <yp:on-change/>
</establish-subscription> </netconf:rpc>
```

Next Step for 2 Drafts

- More clear use case description
- More clear proposed modelling, and NETCONF/YANG definition
  - ✓Potentially, necessary extension to existing IETF YANG models, or new YANG data model definition.
- Check OPSAWG WG interest
- Welcome comments and collaboration