March 2022

METHOD TO PROVIDE TRUSTWORTHINESS TO SGT EXCHANGE PROTOCOL

NIRANJAN M M

METHOD TO PROVIDE TRUSTWORTHINESS TO SGT EXCHANGE PROTOCOL

AUTHOR:
NIRANJAN M M

ABSTRACT

SGT eXchange Protocol (SXP) is used to propagate Security Group Tag (SGT) information across the network devices. SXP connections are point-to-point and uses TCP as the underlying transport protocol with roles as Speaker, Listener or Both. There are techniques to provide message authentication, key-exchange, and integrity to the SXP connections. But, if the Speaker or Listener is compromised, i.e., it is no longer a trusted entity, which could create harm to the network by allowing "malicious Speaker to send the wrong IP-to-SGT binding to the valid Listener" or "valid Speaker to send the correct IP-to-SGT binding to the malicious Listener". Hence, SXP connection endpoints i.e., Speaker and Listener need to know whether the peer device is trustworthy or not before establishing connection. The techniques presented herein propose attestation method to SXP protocol messages for providing Proof of Integrity of SXP connection between devices.

DETAILED DESCRIPTION

SGT eXchange Protocol (SXP) is used to propagate Security Group Tag (SGT) information across the network devices. SGT provides software-defined segmentation and policy enforcement. SXP is included in the Open Daylight SDN controller, which allows other vendors to integrate at Controller level instead of network. With this background, SXP connections are point-to-point and uses TCP as the underlying transport protocol with roles as Speaker (i.e., device that sends the IP-to-SGT binding), Listener (i.e., device that receives the IP-to-SGT binding) or Both.

Currently SXP connection uses following methods for providing message authenticity and integrity:

- Using MD5: It requires pre-configured key (password) on both sides of the point-to-point link and uses TCP-MD5 option with MD5 Digest.
- Using TCP-AO: It requires pre-configured keychain on both sides of the point-to-point link and uses TCP-AO option with HMAC.

There are techniques in which SXP can use Dot1x for authentication and key exchange. But, if the Speaker or Listener is compromised, i.e., it is no longer a trusted entity, which could create harm to the network by allowing "malicious Speaker to send the wrong IP-to-SGT binding to the valid Listener" or "valid Speaker to send the correct IP-to-SGT binding to the malicious Listener". Hence, SXP connection endpoints i.e., Speaker and Listener need to know whether the peer device is trustworthy or not before establishing connection.

Currently SXP protocol does not include any capabilities to exchange trust information between Speaker and Listener to prove the peer was not tampered. In other words, trustworthiness of the Speaker and Listener must be verified before the connection is established. This includes an integrity check for both, the software as well as hardware of the SXP protocol participants i.e., Speaker and Listener.

The techniques presented herein propose attestation method to SXP protocol messages for providing Proof of Integrity of SXP connection between devices. SXP messages between the peers (i.e., Speaker and Listener) are extended with extensions that carry Proof of Integrity. TPM functionality is used as root of trust and as Proof of Integrity of SXP connection. Both SXP end points gather below integrity measurements from the peer device:

- Hardware
- Software - micro loader, BIOS, boot loader, kernel, operating system
- Runtime - application binaries, libraries, config/manifest files

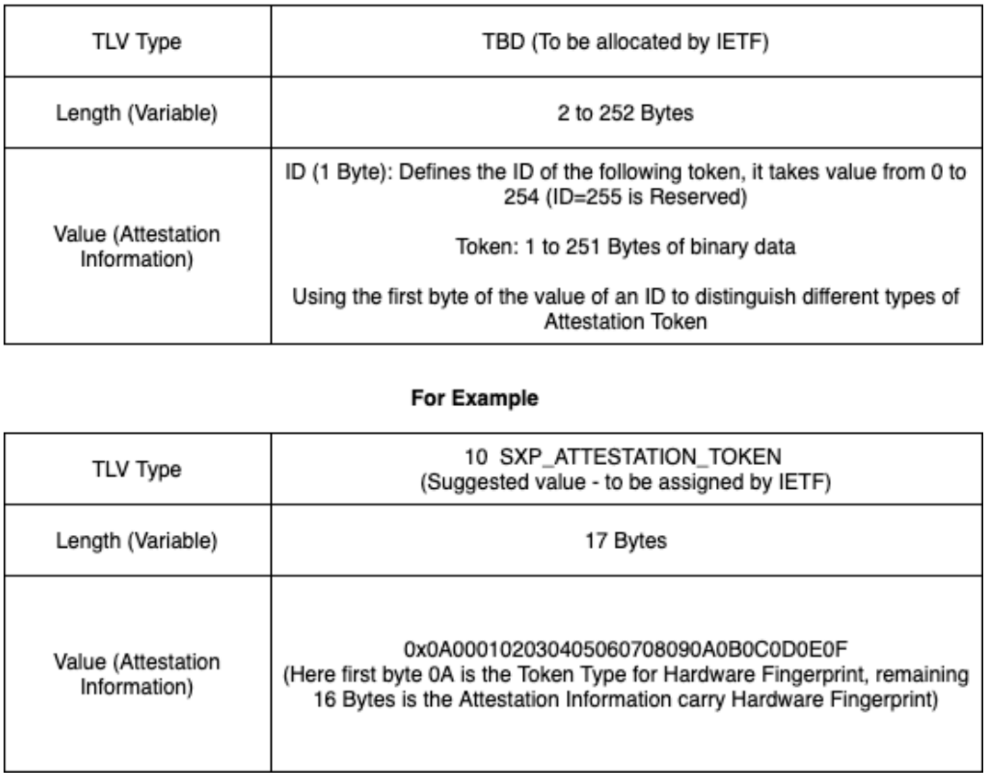
These measurements are verified against the device fingerprint (e.g., imprinted in the device identity certificate issued by the manufacturer - SUDI). The result of verification determines the decision to allow SXP connection establishment between the peers.

This method adds attestation information to the SXP protocol as an extension that embeds:

- A hardware fingerprint (derived from SUDI or similar, stored securely in tamper proof chip e.g., ACT2/TAM)
- Platform information such as PCR, counters, time-ticks etc.,

SXP provides "Other Optional Attributes TLV" in "OPEN", "OPEN_RESP", "UPDATE" and other messages as defined in IETF. This proposed method adds attestation information as TLV in these messages. The device who is participating in SXP connection will use this attestation information to verify whether the peer device who sent the "OPEN", "OPEN RESP" or "UPDATE" message is trustworthy or not.

Figure-1 define “Other Optional Attributes TLV” of SXP OPEN/OPEN_RESP message carrying attestation information.



TLV Type	TBD (To be allocated by IETF)
Length (Variable)	2 to 252 Bytes
Value (Attestation Information)	ID (1 Byte): Defines the ID of the following token, it takes value from 0 to 254 (ID=255 is Reserved) Token: 1 to 251 Bytes of binary data Using the first byte of the value of an ID to distinguish different types of Attestation Token

For Example

TLV Type	10 SXP_ATTESTATION_TOKEN (Suggested value - to be assigned by IETF)
Length (Variable)	17 Bytes
Value (Attestation Information)	0x0A000102030405060708090A0B0C0D0E0F (Here first byte 0A is the Token Type for Hardware Fingerprint, remaining 16 Bytes is the Attestation Information carry Hardware Fingerprint)

Figure-1

The techniques presented herein define method to provide trustworthiness to SXP protocol messages ("OPEN", "OPEN_RESP" etc.,) exchanged between devices of the peer-to-peer SXP connection. Moreover, trust is required in SXP connection, which propagate an SGT information across the network devices. Especially, with SXP standard being available in IETF, multiple vendors would implement in their products, providing trust would be one of the major contributors for adoption. Also, with SXP being included in the Open Daylight SDN controller, which allows other vendors to integrate at Controller level instead of network, we need to establish trust among devices of SXP connection. Additionally, with Open Source SXP implementation being available via GitHub, which allows other vendors to use to implement in their own products, newer developments especially related to security and trust, would likely to happen, they can use this method to provide trustworthiness among peer-devices of SXP connection.