March 2022

METHOD TO PROVIDE TRUSTWORTHY BETWEEN ACCESS POINT AND WIRELESS LAN CONTROLLER

Niranjan M M

METHOD TO PROVIDE TRUSTWORTHY BETWEEN ACCESS POINT AND WIRELESS LAN CONTROLLER

AUTHOR:
Niranjan M M

ABSTRACT

Currently Access Point (AP) needs to join to the Wireless LAN Controller (WLC) before it can serve the wireless clients. AP would communicate with the WLC over CAPWAP-DTLS tunnel. The AP or WLC, could have become compromised so that they are no longer a trusted entity. For these CAPWAP-DTLS tunnels that can influence how the wireless LAN is deployed, configured, and used, it is important to establish DTLS connections only with the devices that can be verified to be trusted. Currently CAPWAP-DTLS tunnel does not offer a way to understand whether the discovered WLC or connected AP is a trustworthy device or not. The techniques presented herein applies attestation method to CAPWAP-DTLS communication between AP and WLC, wherein CAPWAP-DTLS messages between AP and WLC are extended with extensions that carry Proof of Integrity and intent to validate Proof of Integrity.

DETAILED DESCRIPTION

Currently Access Point (AP) needs to join to the Wireless LAN Controller (WLC) before it can serve the wireless clients. AP would communicate with the WLC over CAPWAP protocol, initial messages (discovery request/response) are unencrypted, and subsequent messages (join/config) are encrypted with the DTLS tunnel. When AP and WLC establishes communication channel using DTLS, they do mutual authentication across network based on certificates, public key infrastructure. But this is not enough. The AP or the WLC (especially with cloud deployments), could have become compromised so that they are no longer a trusted entity. For these CAPWAP-DTLS tunnels that can influence how the wireless LAN is deployed, configured, and used, it is important to establish DTLS connections only with the devices that can be verified to be trusted.

Currently CAPWAP-DTLS tunnel does not offer a way to understand whether the discovered WLC or connected AP is a trustworthy device or not. Trustworthiness of the AP and WLC must be verified before the connection is established. This includes an integrity check for

both, the software as well as the hardware of the CAPWAP protocol participants i.e., AP and WLC. There are other deployment methods to provision/configure APs directly from the cloud through GRPC protocol. In these scenarios also trust should be established between AP and software running on the cloud before provisioning the policies on the AP.

Following is one of the CAPWAP discovery vulnerability (denial of service attack) found in the National Vulnerability Database: https://nvd.nist.gov/vuln/detail/CVE-2018-0443. As per above vulnerability, an attacker could exploit by sending malicious CAPWAP Discovery Request packets to the Cisco WLC Software. Many similar types of vulnerabilities can be resolved by having trustworthiness between AP and WLC.

Currently AP joins to WLC using CAPWAP (Control and Provisioning of Wireless Access Points) protocol, part of RFC 5415 and RFC 5416. AP Configurations, wireless client specific confidential information etc., are exchanged over CAPWAP protocol, which is over UDP and plain text. Hence to provide security, DTLS (Datagram Transport Layer Security) tunnel is established before exchanging any of these messages between WLC and AP. Even DTLS is having vulnerabilities related to certificate forgery which could be used to conduct man-in-the-middle attack.

CAPWAP protocol is having following phases:

- Discovery phase: In this phase, broadcast Discovery Request would be sent from AP to WLC, and unicast Discovery Response sent back from WLC to AP in plain text.
- DTLS tunnel establishment phase: In this phase, DTLS tunnel is established between AP and WLC (they use device certificate for authentication).
- Join phase: In this phase, Join Request would be sent from AP to WLC, and Join Response sent back from WLC to AP over DTLS tunnel established in previous phase.
- Image download phase: In this phase, if any mismatch in the image version between AP and WLC then AP image will be downloaded from WLC to AP.
- Configuration Request/Response phase: In this phase, Configurations such as Policies, WLANs, ACLs etc., are sent from WLC to AP.
- Moved to RUN state and handing keep-alive, control and data messages: In this phase, Echo Request/Response are exchanged which are part of keep-alive and client related control and data packets (which includes association, L2 and L3 authentication messages, DHCP etc.,) are exchanged between AP and WLC. Apart from these, PMK (Pairwise

Master Key) cache for fast roaming support, WIPS (Wireless Intrusion Prevention System) profile for threat detection and mitigation, AVC (Application Visibility and Control_ protocol pack for deep packet inspection (DPI) etc., are sent over this tunnel.

To address possible vulnerabilities in the above phases of CAPWAP-DTLS protocol between AP and WLC, we need to have trustworthiness between AP and WLC by having attestation information in CAPWAP and DTLS packets.

The techniques presented herein applies attestation method to CAPWAP-DTLS communication between AP and WLC. CAPWAP-DTLS messages between AP and WLC are extended with extensions that carry Proof of Integrity and intent to validate Proof of Integrity.

Proof of Integrity:

TPM functionality is used as root of trust and Proof of Integrity of an AP and WLC. Both AP and WLC gather below integrity measurements from the peer device:

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

These measurements are verified against the device fingerprint (e.g., imprinted in the device identity certificate issued by the manufacturer - SUDI) and against the Known Good Values (KGV). The result of verification determines the decision to allow CAPWAP-DTLS connection establishment between AP and WLC.

Freshness of the Proof of Integrity:

Along with Proof of Integrity, Freshness of the Proof of Integrity should also be considered. For CAPWAP discovery request/response packets, which are being initial messages, uni-directional attestation would be applied. Here, Proof of Integrity will also be accompanied with freshness of the Proof of Integrity using Counter and/or Log method. For DTLS packets, which are being certificate exchange messages, bi-directional Attestation would be applied. Here, Proof of Integrity will also be accompanied with a signature to prove freshness of the Proof of Integrity i.e., by adding a signature over random data/nonce presented by the peer.

Example: DTLS Client Hello from AP contains random data/nonce, it is extended to carry intention to validate Proof of Integrity. DTLS Server Hello from WLC carries an extension to its Proof of Integrity along with a signature over random data/nonce received in DTLS Client Hello. Similar thing would be done from the other side i.e., from WLC to AP as well. This can be achieved

by extending DTLS with a new ExtensionType as defined in https://tools.ietf.org/html/rfc8447#section-7 (TLS ExtensionType Values).

This method adds attestation information to the CAPWAP-DTLS messages as an extension that embeds:

- Hardware Fingerprint - Derived from SUDI or similar.
- Software - OS, BIOS, kernel, Version, application binaries/libraries etc.,
- Platform Information - PCR (Platform Config Registers), time-ticks, signature.

AP and WLC will use this information against the device fingerprint and Known Good Values, to verify whether the peer is trustworthy or not. Depending on the outcome of the verification, the AP/WLC can decide, whether connectivity to the remote device should be considered or not. If the verification is successful, DTLS session is established.

Figure-1 explains the attestation of CAPWAP protocol.

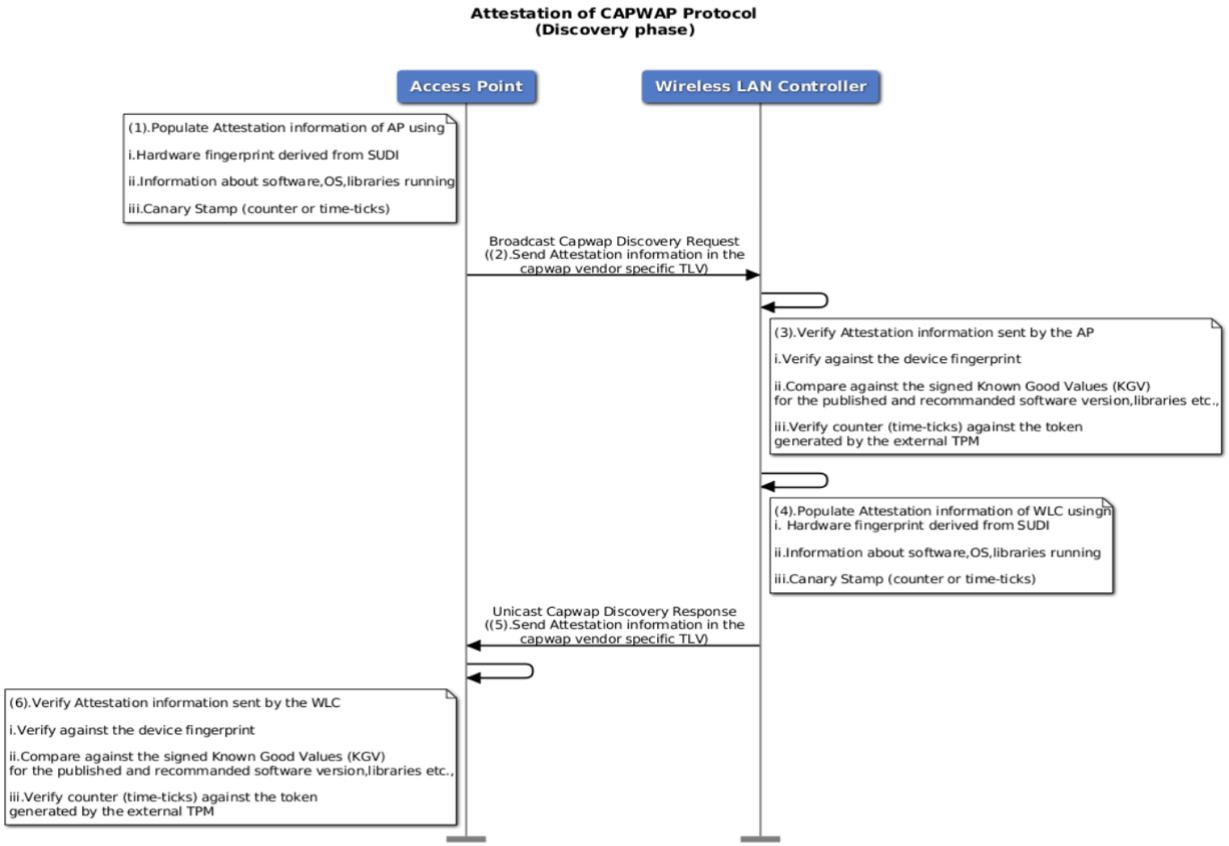

Figure-1

Figure-2 explains the attestation of DTLS protocol.

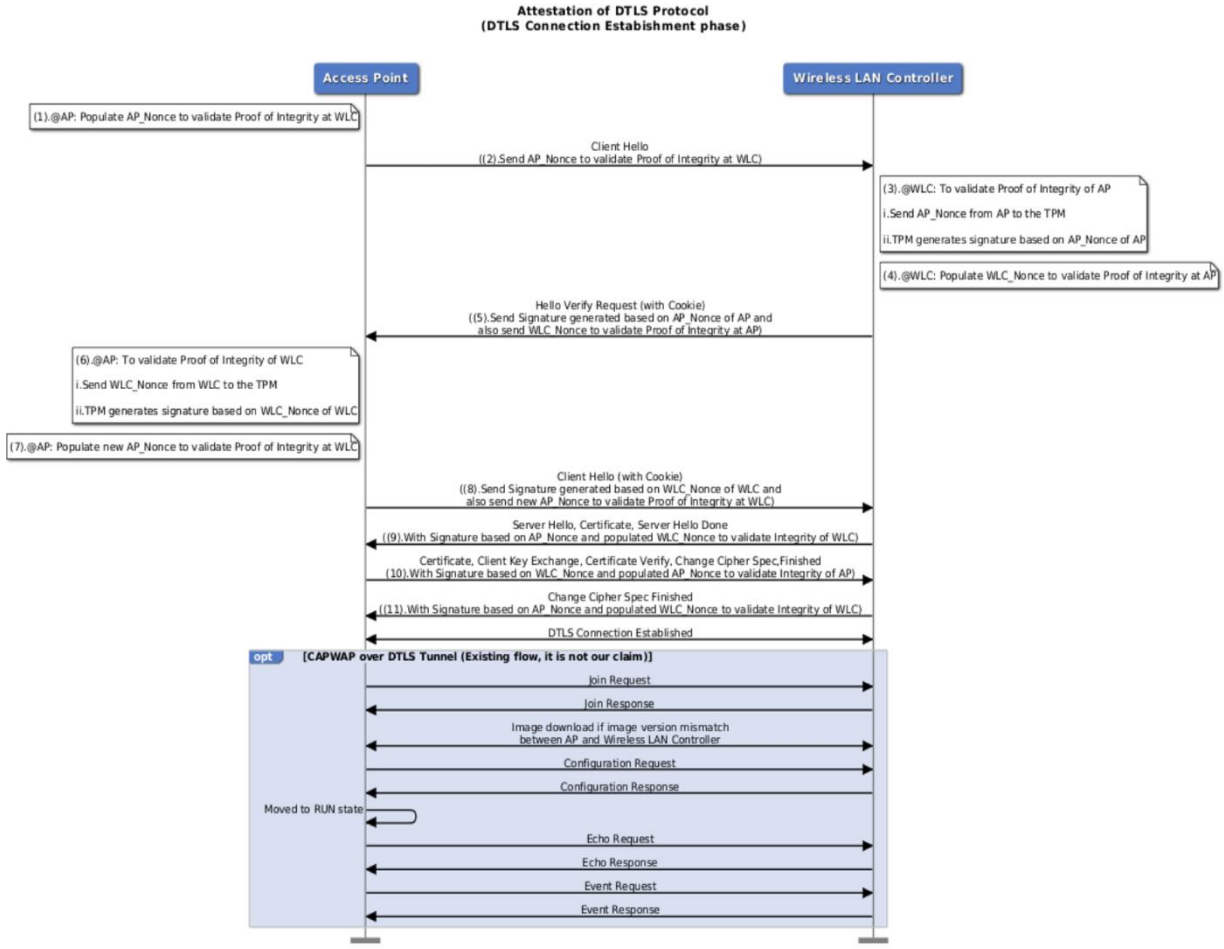

Figure-2

Trustworthiness between AP and WLC is must when APs are deployed on-premises (enterprise) and virtual WLC instances are deployed in Cloud. For example, if WLC get compromised, then whole Wi-Fi deployment would get compromised i.e., compromised WLC can push configurations/policies which can allow rogue APs/Clients to join, removing any data rate limits, wrongly configured AVC profiles etc., AP can use level of trustworthiness to decide which WLC (if more than one WLC is discovered) to connect using Attestation based selection criteria (want more secure/trust, least loaded WLC etc.,). Here, attestation information would include Hardware Fingerprint which is derived from SUDI certificate stored securely in ACT2 chip, Software information (version, OS, BIOS, kernel, application binaries/libraries etc.,) and platform information (counter, time-ticks, signature etc.,). WLC and AP will use this information to verify

the peer is trustworthy or not, before CAPWAP/DTLS tunnel establishment. There are methods to provision/configure APs from Cloud through GRPC which can utilise similar extension for validating and make policy decision to establish/drop the connection. Same is applicable to any other config modelling using RESTConf, NETCONF, REST APIs/HTTPS etc.,

This method would ensure all the messages (which includes control and data packets of wireless clients such as association, L2 and L3 authentication, DHCP etc., and feature specific information such as PMK cache, WIPS profile, AVC protocol pack etc.,) sent over this CAPWAP-DTLS tunnel are Trustworthy. Moreover, this method is applicable among WLCs in Mobility Domain. Additionally, this method is applicable for Mesh deployments, i.e., for providing trustworthiness between APs i.e., Mesh AP (MAP) and Root AP (RAP).