March 2022

TRUSTWORTHINESS FOR LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL

NIRANJAN M M

TRUSTWORTHINESS FOR LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL

AUTHOR:
NIRANJAN M M

ABSTRACT

Authentication using external authentication servers is commonly used to provide network access, including wired and wireless deployments. Both authentication server and authenticating client need to know whether the connecting peer is trustworthy or not. If the authentication server or client is compromised i.e., it is no longer a trusted entity, which could create harm to the network by allowing malicious server to authenticate the client or malicious client (attacker) to access the network. Lightweight Directory Access Protocol (LDAP) is an extensible protocol, whose specification is defined in RFC4510, and protocol details are defined in RFC4511. Currently LDAP does not include any capabilities to exchange trust information between LDAP client and LDAP server to prove to either server or client that the peer was not tampered. The techniques presented herein describe method to have trustworthiness between LDAP client and LDAP server by having attestation information in all LDAP messages. This method incorporates attestation information to LDAP messages exchanged between LDAP client and LDAP server. In other words, LDAP messages between LDAP client and LDAP server are extended with extensions that carry Proof of Integrity and intent to validate Proof of Integrity.

DETAILED DESCRIPTION

One of the fundamental requirements for security is to provide user/client authentication. With the enterprise deployments, the user/client authentication is done through Switch/Router (wired deployment) or WLC (wireless deployment). But authentication of user/client using local user-database is not scalable. Hence most of the deployments would be configured with external authentication method, with authentication servers being Radius, Diameter or LDAP server. And provided options to configure multiple external authentication servers.

Authentication using external authentication servers is commonly used to provide network access, including wired and wireless deployments. Both authentication server and authenticating client need to know whether the connecting peer is trustworthy or not.

If the authentication server or client is compromised i.e., it is no longer a trusted entity, which could create harm to the network by allowing malicious server to authenticate the client or malicious client (attacker) to access the network.

Lightweight Directory Access Protocol (LDAP) is an extensible protocol, whose specification is defined in RFC4510, and protocol details are defined in RFC4511. Currently LDAP does not include any capabilities to exchange trust information between LDAP client and LDAP server to prove to either server or client that the peer was not tampered.

There are techniques to provide trustworthiness to Radius and Diameter authentication protocols., but not for LDAP protocol used for user/client authentication.

The techniques presented herein describe method to have trustworthiness between LDAP client and LDAP server by having attestation information in all LDAP messages.

This method incorporates attestation information to LDAP messages exchanged between LDAP client and LDAP server. In other words, LDAP messages between LDAP client and LDAP server 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 as Proof of Integrity of LDAP client and LDAP server. Both LDAP client and LDAP server 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). The result of verification determines the decision to allow LDAP connection establishment between LDAP client and LDAP server.

Freshness of the Proof of Integrity: Along with Proof of Integrity, Freshness of the Proof of Integrity is also considered. As LDAP is a request-response type of protocol where each request is followed by a response, Proof of Integrity can 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. This would help in detecting the replay of old evidence via a "nonce". A nonce is a random number provided by the entity making the request. This nonce is passed into the TPM. Results coming out of the TPM include a signature based on the nonce. The result is the output from the TPM which could not have been generated before that nonce was provided.
Example: “Bind” is the LDAP message to allow authentication information to be exchanged between the LDAP client and LDAP server. The operation consists of the Bind Request and the Bind Response. Bind Request from LDAP client contains random data/nonce, it is extended to carry intention to validate Proof of Integrity. Bind Response from LDAP server carries an extension to its Proof of Integrity along with a signature over random data/nonce received in Bind Request. Similar thing would be done from the other side i.e., from LDAP server to LDAP client as well in the next message exchange.

This can be achieved by extending LDAP with a new
Extension https://tools.ietf.org/html/rfc4511#section-4 (4. Elements of Protocol, ASN.1) and by adding the attestation information in explicit Extended Request and Extended Response as defined in https://tools.ietf.org/html/rfc4511#page-37 (4.12. Extended Operation).

Figure-1 depicts the LDAP protocol extended with attestation information to provide Trustworthiness between LDAP client (Switch/Router/WLC) and LDAP server (Authentication server).

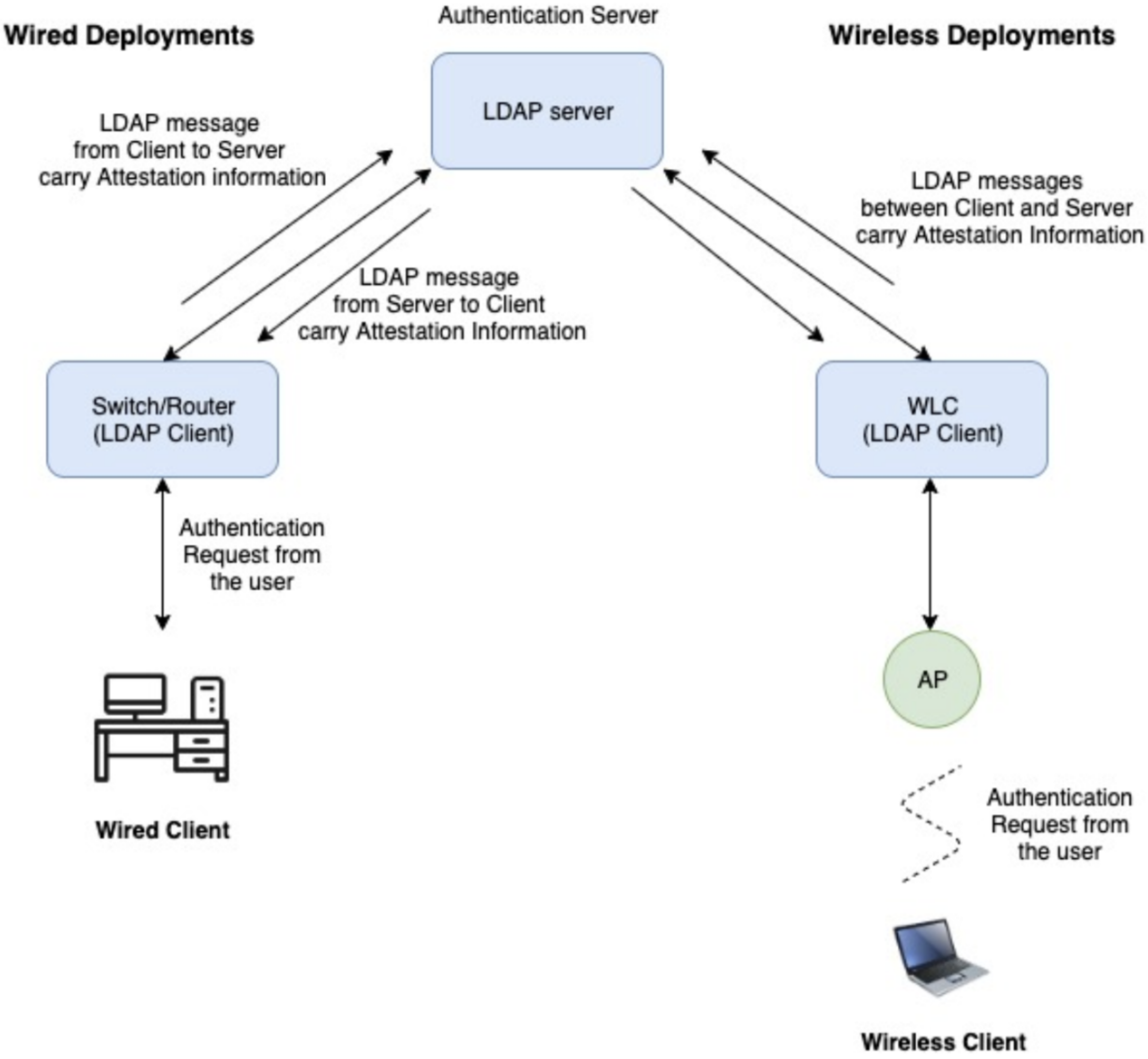
Wired Deployments
Authentication Server
LDAP server
Wireless Deployments
LDAP message from Client to Server carry Attestation information
LDAP messages between Client and Server carry Attestation Information
LDAP message from Server to Client carry Attestation Information
Switch/Router (LDAP Client)
WLC (LDAP Client)
Authentication Request from the user
AP
Wired Client
Authentication Request from the user
Wireless Client

Figure-1

The method proposes to add attestation information to the LDAP 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.

LDAP client and LDAP server will use this information against the device fingerprint, to verify whether the peer is trustworthy or not.
Integrity information can be added to the following LDAP messages:
BindRequest, BindResponse, UnbindRequest, SearchRequest, SearchResultEntry, SearchResultDone, SearchResultReference, ModifyRequest, ModifyResponse,

AddRequest,AddResponse, DelRequest, DelResponse, ModifyDNRequest, ModifyDNResponse, CompareRequest, CompareResponse, ExtendedRequest, ExtendedResponse.

Depending on the outcome of the verification, the LDAP client/server can decide, whether connectivity to the remote device should be considered or not. That is, if the verification is successful, LDAP session is established.
LDAP client can use level of trustworthiness to decide which LDAP server (if more than one LDAP is configured/available) to authenticate using attestation-based selection criteria (want more secure/trust, least loaded LDAP etc., based on configuration/requirement).

In short, 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.,). LDAP server and LDAP client will use this information to verify the peer is trustworthy or not before LDAP connection is established. The techniques presented herein provides trustworthiness to LDAP protocol used in wired and wireless deployments.