MUD (D)TLS profiles for IoT devices

draft-ietf-opsawg-mud-tls-03

Nov 2020

T. Reddy (McAfee)

D.Wing (Citrix)

B.Anderson (Cisco)

Agenda

- Updates to address comments from OPSAWG and TLS
- Questions & Comments

Updates to draft: GREASE

- Two changes to support GREASE/-like behavior:
  1. tls-dtls-profiles parameters MUST NOT include GREASE values
     - Allows random values in future TLS parameters
  2. Network security services can only enforce *known* parameters

Updates to draft

- Rules to Process of the MUD (D)TLS profile by a network security service:
  - Malware Detected: (D)TLS parameter is not specified in the MUD (D)TLS profile but recognized by the firewall.

Cipher Suite	(D)TLS profile	Firewall	Action
CHACHA20_POLY1305_SHA256	Not specified	Known	Block the flow/ Quarantine the IoT device

Updates to draft

- Rules to Process of the MUD (D)TLS profile by a network security service:
  - **No action:** (D)TLS parameter is not specified in the MUD (D)TLS profile and not recognized by the firewall.

Cipher Suite	(D)TLS profile	Firewall	Action
CHACHA20_POLY1305_SHA256	Not specified	Unknown	Ignore

Updates to draft

- Rules to Process of the MUD (D)TLS profile by a network security service:
  - **Alert:** Updated MUD (D)TLS profile parameters not recognized by firewall.

Cipher Suite	(D)TLS profile	Firewall	Action
CHACHA20_POLY1305_SHA256	specified	Unknown	Alert to admin/ firewall vendor

TLS version	(D)TLS profile	Firewall	Action
TLS 1.3	specified	Unknown	Alert to admin/ firewall vendor

- Firewall must be readily updatable recognize the new parameters. If firewall is not readily updatable, protection efficacy decreases with time.

Updates to YANG Modules

- The (D)TLS profile Extension to the ACL YANG Model
- IANA (D)TLS profile YANG Module to include (D)TLS versions and (D)TLS parameters

```
module: ietf-acl-tls
  augment /acl:acls/acl:acl/acl:aces/acl:ace/acl:matches:
    +--rw client-profile {match-on-tls-dtls}?
       +--rw client-profile
          +--rw tls-dtls-profiles* [profile-name]
             +--rw profile-name                    string
             +--rw supported-tls-versions*         ianatp:tls-version
             +--rw supported-dtls-versions*        ianatp:dtls-version
             +--rw cipher-suites* [cipher hash]
             |  +--rw cipher    ianatp:cipher-algorithm
             |  +--rw hash      ianatp:hash-algorithm
             +--rw extension-types*
             |       ianatp:extension-type
             +--rw acceptlist-ta-certs*
             |       ct:trust-anchor-cert-cms
             +--rw spki
             |  +--rw spki-pin-sets*         ianatp:spki-pin-set
             |  +--rw spki-hash-algorithm?   iha:hash-algorithm-type
             +--rw psk-key-exchange-modes*
             |       ianatp:psk-key-exchange-mode
             |       {tls-1-3 or dtls-1-3}?
             +--rw supported-groups*
             |       ianatp:supported-group
             +--rw signature-algorithms-cert*
             |       ianatp:signature-algorithm
             |       {tls-1-3 or dtls-1-3}?
             +--rw signature-algorithms*
             |       ianatp:signature-algorithm
             +--rw application-protocols*
             |       ianatp:application-protocol
             +--rw cert-compression-algorithms*
             |       ianatp:cert-compression-algorithm
             |       {tls-1-3 or dtls-1-3}?
             +--rw certificate-authorities*
                     ianatp:certificate-authority
                     {tls-1-3 or dtls-1-3}?
```

Updates to YANG Modules

- MUD (D)TLS Profile Extension

```
module: ietf-mud-tls
  augment /ietf-mud:mud:
    +--rw is-tls-dtls-profile-supported?   boolean
```

Updates to IANA (D)TLS Profile YANG module

- The values for all the parameters in the "iana-tls-profile" YANG module are defined in the TLS and DTLS IANA registries excluding the **tls-version, dtls-version, spki-pin-set, and certificate-authority** parameters.
- The values of spki-pin-set and certificate-authority parameters are specific to the IoT device.
- (D)TLS versions and (D)TLS parameters registries
  - ❑ The TLS and DTLS IANA registries do not maintain (D)TLS version numbers.
- YANG module is updated by IANA by updating the (D)TLS versions and (D)TLS parameters registries using expert review

draft-ietf-opsawg-mud-tls-03

- Comments and suggestions are welcome