IETF-75

radext 31 jul 2009

RADIUS over TCP/TLS (RadSec) Update

Draft status

- Rev -05 published
- Includes changes from WGLC
- Includes most comments from the room at IETF 74
  - making wording TCP-agnostic doesn't seem possible in a clean way
  - Standing issue: client identification profile text
  - Standing issue: preventing bidding-down

Prevention of bidding down

- Idea on ML: prevent bidding down by having server maintain state on client's transport capabilities (“set a flag once client connects with better transport”)
- Can not be done completely transparent to server config, unless TLS-Id == IP; TLS-pass == MD5-pass
- Not favoured on ML; keep TLS-Id and TLS-pass different
- Needs manual config intervention

Server config (1) (UDP only)

```
client erebus {
        ipaddr = 1.2.3.4
        secret = tooweak4u
}
```

Server config (2)
TLS added, but not seen yet

```
client erebus {
        ipaddr = 1.2.3.4
        secret = tooweak4u
        TLS-Id = Gallente
        TLS-pass = doomsday
}
```

Server State: client capabilities unknown

Server config (3)
TLS seen from client

```
client erebus {
        ~~ipaddr = 1.2.3.4~~
        ~~secret = tooweak4u~~
        TLS-Id = Gallente
        TLS-pass = doomsday
}
```

Server State: client TLS capable → disable UDP

Identifying clients (1)

- RADIUS:
  - Client uniquely identified by IP, shared-secret
  - But: clients can be clustered in configuration

    client 1.2.3.0/24 → 255 clients treated as one
- TLS:
  - Multiple operation modes: fingerprint, TLS-PSK, TLS with PKI
  - Different ways to uniquely identify; desire to cluster still exists

Identifying clients (2)

- In Fingerprint mode
  - Clients identified by fingerprint
  - Clustering by: (set of) fingerprints
- In TLS-PSK mode
  - Clients identified by TLS-Identifier
  - Clustering by: (set of) TLS-Identifiers
- In TLS-PKI mode
  - Clients identified by 2-tuple (Subject; CA)
  - Clustering by: arbitrary criteria within Subject

Identifying clients (3)

- Clustering criteria
    - Supported criteria implementation-specific
    - “anything goes”
- WG indicated that guidelines would be good
- Since Subject (as a whole) is the only way to uniquely persistently identify a client, using any subset of Subject clusters more than one client together
- Example: all certificates with same 2-tuple (CN,CA) are treated as same
- Example 2: all certificates with subjectAltName:URI=.*eduroam.* are treated as same

Example

A

CN=Foo-Proxy
CA=ExtraSign Ltd.
subjectAltName:DNS=
  foo.bar.com
subjectAltName:URI=
  http://x.y.z/primary

B

CN=Foo-Proxy
CA=ExtraSign Ltd.
subjectAltName:DNS=
  foo2.bar.com
subjectAltName:URI=
  http://x.y.z/secondary

- Server with which clusters with (CN/CA) treats A and B as same client
- Server with subjectAltName:URI criterion support can distinguish them as different (if configured to)