

radext IETF-75  
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)



- In Fingerprint mode
  - Clients identified by (set of) fingerprints
- In TLS-PSK mode
  - Clients identified by (set of) TLS-Identifiers
- In TLS-PKI mode
  - (next slide)

# Identifying clients (2)



- In TLS-PKI mode
  - Minimum required: identify clients by 2-tuple (CN, CA)
  - i.e. two connecting clients where tuple differs are not the same client
  - If implementation supports more criteria to identify clients (SHOULD criteria in draft):  
Tuple dimension extends to supported criteria



# 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 minimum profile treats A and B as same client
- Server with subjectAltName:URI support can distinguish them as different (if configured to)