DTLS over SNMP

Wes Hardaker

14 November 2008

1. Background

2. SNMP over DTLS: Details

3. Issues

Motivation

- Support X.509 Certificate Authentication
- Support for a UDP based security solution
  - TCP vs UDP performance in bad networks is still a problem

The Resulting Document

- draft-hardaker-isms-dtls-tm-01
- Closely aligns in structure the SSH document
- Compliant with the TSM security model expectations

DTLS

- Defined in RFC4347
- DTLS is functionally identically to TLS
- Uses the same on-the-wire format
    - X.509 certificates for authentication.

(Editor's Note: I'm not a DTLS expert; hopefully Eric is here!)

DTLS Architecture Overview

```
Client                                               Server

ClientHello                  -------->
                                                ServerHello
                                               Certificate*
                                         ServerKeyExchange*
                                        CertificateRequest*
                             <--------      ServerHelloDone
Certificate*
ClientKeyExchange
CertificateVerify*
[ChangeCipherSpec]
Finished                     -------->
                                         [ChangeCipherSpec]
                             <--------             Finished
Application Data             <------->     Application Data
```

DTLS Considerations

- TLS relies on TCP for session demultiplexing
  - Does not contain an in-protocol session identifier
- UDP doesn't provide session demultiplexing

- Result: we have to define how to demultiplex multiple connections
  - Need a unique key to latch to a DTLS session
  - Key: src addr, srt port, dst addr, dst port

X509 Certificates to securityName

- X509 Certificates use a very different naming structure
- The *Issuer:* field identifies who handed out the certificate
- The *Subject:* field typically identifies a user and contains:
  - Location information (C: Country, ST: State)
  - Organization information (O: Name, OU: Unit)
  - Personal Information (CN: Common Name)

Client X.509 Certificate Examples

Example: My Fedora User Certificate

- Subject: C=US, ST=North Carolina, O=Fedora Project, OU=Fedora User Cert, **CN=hardaker/emailAddress=wjhns174@hardakers.net**
- Issuer: C=US, ST=North Carolina, L=Raleigh, O=Fedora Project, OU=Fedora Project CA, CN=Fedora Project CA/emailAddress=admin@fedoraproject.org

Example: Fedora CA

- XXX...

Server X.509 Certificate Examples

Example: The Fedora Server Certificate

- Subject: C=US, ST=North Carolina, L=Raleigh, O=Fedora Project, OU=Fedora Project CA, **CN=Fedora Project CA/emailAddress=admin@fedoraproject.org**
- Issuer: C=US, ST=North Carolina, L=Raleigh, O=Fedora Project, OU=Fedora Project CA, CN=Fedora Project CA/emailAddress=admin@fedoraproject.org

Example: The www.ietf.org HTTPS Certificate

- Subject: O = *.ietf.org, OU = Domain Control Validated, CN = ***.ietf.org**
- Issuer: CN = Starfield Secure Certification Authority, OU = http://certificates.starfieldtech.com/repository, O = Starfield Technologies, Inc., L = Scottsdale, ST = Arizona, C = US

X.509 Subject to securityName Mapping

- The *Subject* field **is** the identifying field.
- The *Common Name (CN)* tag within it is typically the *account name*
- It is paired with the *Issuer* field to be unique
- Potential ways to be mapped into a securityName:
  - Take the **CN** in raw form
  - Map the **CN** to a securityName
- This mapping is configured through DTLSTM-MIB tables

DTLSTM-MIB

- Domain and Address definitions
- Counters
- Configuration
  - dtlstmCertificateToSNTable
  - dtlstmParamsTable
- Conformance statements

Incoming securityName Selection

- The dtlstmCertificateToSNTable maps incoming certificates to securityNames.
- Two modes:
    - Accept the CN directly from trusted CAs
    - Map a Subject to specific securityName

dtlstmCertificateToSNTable

Column	Value
dtlstmCertID(1)	1
dtlstmCertIssuerDN(2)	Fedora...
dtlstmCertMapType(3)	specified (or byCN)
dtlstmCertIssuer*	...
dtlstmCertSubject*	C=US, ST=North Carolina ...
dtlstmCertSecurityName(4)	wes
dtlstmCertStorageType(5)	nonVolatile
dtlstmCertRowStatus(6)	createAndGo

Outgoing Certificate Selection

- The dtlstmParamsTable maps an outgoing securityName to a certificate.
- The certificate is referenced by a Issuer and Subject

dtlstmParamsTable

Column	Value
snmpTargetParamsName(1)	wes
dtlstmCertIssuer*	...
dtlstmParamsSubject(1)	C=US, ... CN=hardaker...
dtlstmParamsStorageType(2)	nonVolatile
dtlstmParamsRowStatus(3)	createAndGo

Issues

- A few MIB changes needed
- Awaiting completion of the other documents before WG consideration
- Need people to review it
- DTLS implementations are still few
  - OpenSSL: implemented but poorly documented
  - GnuTLS: not implemented