11.7.28

An Authentication Method based on Certificate for DHCP

on behalf of
Yixian Xu, Serge Manning, Marcus Wong
Huawei Technologies
IETF 81, Quebec City

Background and Issues

- **For DHCP authentication, RFC3118 defines an delay authentication mechanism for DHCP. But it has vulnerabilities:**
  - It is vulnerable to denial of service attacks through flooding with DHCPDISCOVER messages, which are not authenticated by delay authentication protocol.
  - It overwhelms the DHCP server
  - Exhaust the addresses available for assignment by the DHCP server.

How to avoid these vulnerabilities

As we know, certificates which defined in RFC 5280 can be used for entity authentication, and certificates are used widely.

Does authentication based certificate can be used for DHCP?

Does the application of certificate has any limitation?

The limitation for certificate directly

1

The MTU in Ethernet is usually 1500bytes, while the certificate is usually as large as 1k or 2k bytes

2

DHCPDISCOVER messages and DHCPREQUEST messages are broadcast messages, these cannot be fragmented into several messages.

3

Thus, it is impossible to directly carry certificates in DHCP messages

The solution that we proposed

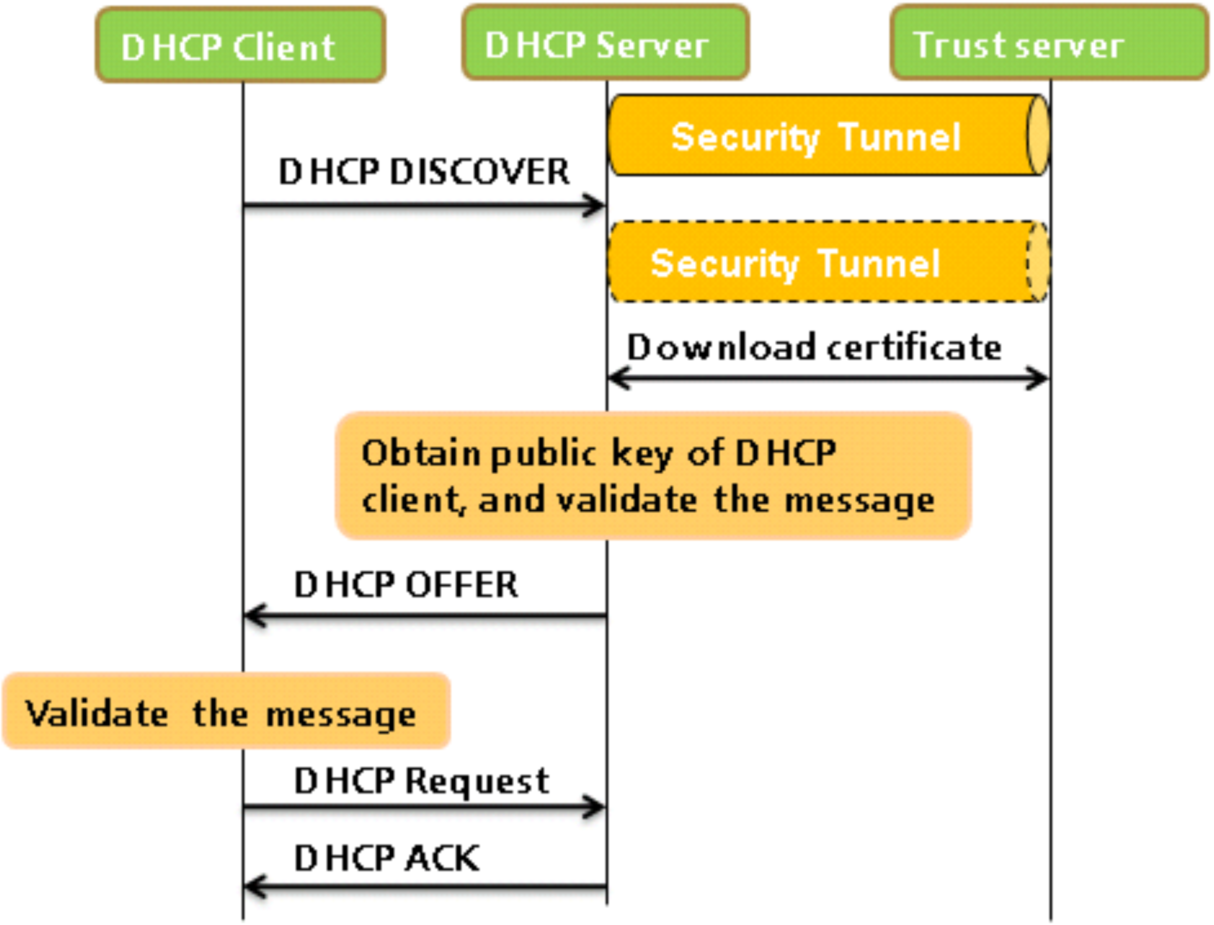
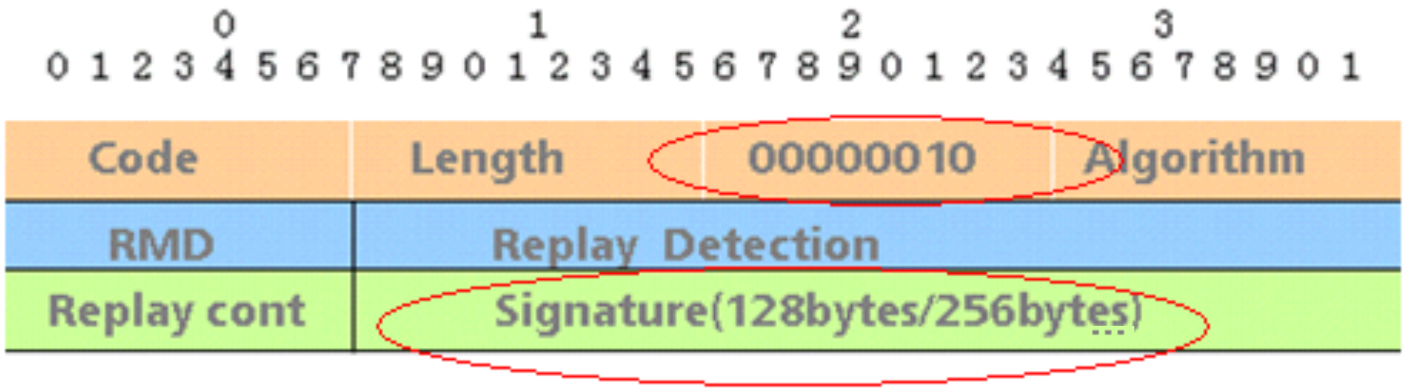


Fig 1.DHCP certificate authentication procedure

Certificate authentication option

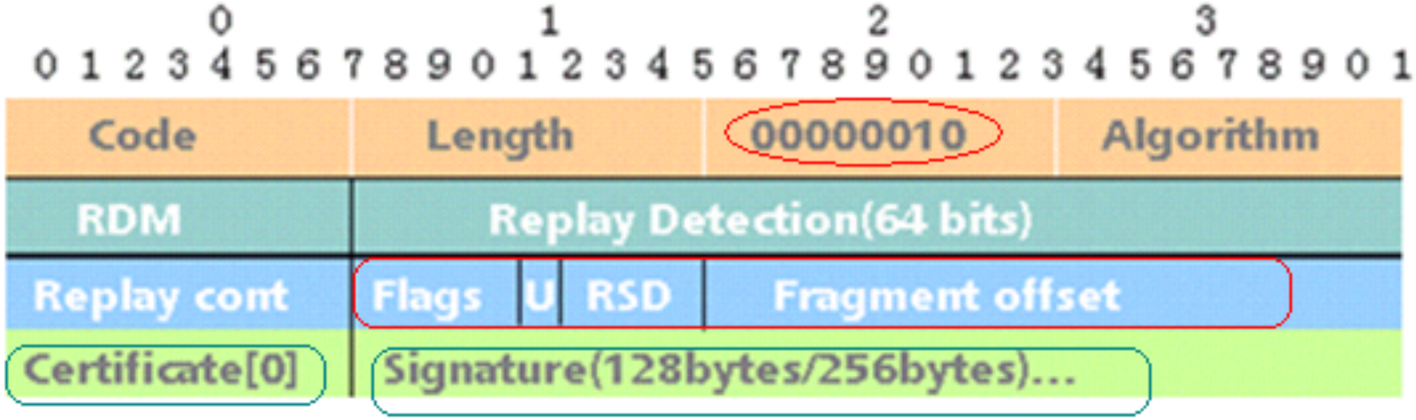


```
                    0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
```

Code	Length	00000010	Algorithm
RMD	Replay Detection		
Replay cont	Signature(128bytes/256bytes)...		

Fig 2. The format of the authentication request(DHCPDISCOVER/DHCPREQUEST/ DHCPINFORM)

Certificate authentication option



```
                    0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
| Code           | Length         | 00000010       | Algorithm      |
| RDM            | Replay Detection(64 bits)                         |
| Replay cont    | Flags | U | RSD | Fragment offset                 |
| Certificate[0] | Signature(128bytes/256bytes)...                   |
```

Fig 3. The format of the authentication information(DHCPOFFER/ DHCPACK)

The certificate of the DHCP Server is included in the Authentication Option

If the length exceeds the MTU, it can be fragmented with several messages[RFC3396]

Thank you