EAP Applicability
IETF-86

Joe Salowey

Open Issues

- Open Issues with Retransmission and re-authentication
- Remove text about lack of differentiation in Network Access

Proposed Retransmission Text

- 2.1 Retransmission

In EAP, the authenticator is responsible for retransmission. By default EAP assumes that the lower layer (the application in this context) is unreliable. The authenticator can send a packet whenever its retransmission timer triggers. In this mode, applications need to be able to receive and process EAP messages at any time during the authentication conversation.

Alternatively, EAP permits a lower layer to set the retransmission timer to infinite. When this happens, the lower layer becomes responsible for reliable delivery of EAP messages. Applications that use a lock-step or client-driven authentication protocol might benefit from this approach.

Proposed Retransmission Text

In addition to retransmission behavior applications need to deal with discarded EAP messages. For example, whenever some EAP methods receive erroneous input, these methods discard the input rather than generating an error response. If the erroneous input was generated by an attacker, legitimate input can sometimes be received after the erroneous input. Applications MUST handle discarded EAP messages, although the specific way in which discarded messages will be handled depend on the characteristics of the application. Options include failing the authentication at the application level, requesting an EAP retransmit and waiting for additional EAP input. *These options may require the EAP methods to notify the application when an EAP message is discarded.*

Specifications of how EAP is used for application authentication SHOULD document how retransmission and message discards are handled.

Proposed Re-authentication Text

2.2 Re-Authentication

EAP lower layers MAY provide a mechanism for re-authentication to happen within an existing session [RFC 3748]. Diameter standardizes a mechanism for a AAA server to request re-authentication [RFC 4005]. Re-authentication permits security associations to be updated without establishing a new session. For network access, this can be important because interrupting network access can disrupt connections and media.

Some applications might not need re-authentication support. For example if sessions are relatively short-lived or if sessions can be replaced without significant disruption, re-authentication might not provide value. Protocols like HypertextTransport Protocol (HTTP) and Simple

Proposed Re-authentication Text

Mail Transport Protocol (SMTP) are examples of protocols where establishing a new connection to update security associations is likely to be sufficient.

Re-authentication is likely to be valuable if sessions or connections are long-lived or if there is a significant cost to disrupting them.

Another factor may make re-authentication important. Some protocols only permit one part in a protocol (for example the client) to establish a new connection. If another party in the protocol needs the security association refreshed then re-authentication can provide a mechanism to do so.

Applications SHOULD describe whether re-authentication is provided and which parties can initiate it.