EAP-FAST Version 2

draft-zhou-emu-eap-fastv2-00.txt

Hao Zhou
Nancy Cam-Winget
Joseph Salowey
Stephen Hanna

March 2011

EAP-FASTv2 Overview

- Inherited from EAP-FAST Version 1 (RFC4851)
- TLS based Tunnel EAP method with
  - TLV encapsulation inside protected tunnel - flexible and extensible
  - Built-in basic password authentication
  - Chained inner EAP methods
  - Supports provisioning of credentials

EAP-FASTv2 Features

- Secure – provided by TLS
  - Mutual authentication
  - Integrity protection
  - Confidentiality
  - Replay protection
  - Dictionary attack protection
  - Fragmentation
  - Identity Protection
  - Protected termination & acknowledged result indication
- Crypto-agility – cipher, hash, PRF negotiation
- Crypto-binding of the tunnel and inner method
- Flexible and extensible – TLV layer within the protected tunnel
- Built-in basic password authentication
- Channel binding support
- Efficiency– server stateful or stateless session resumption
- EAP Sequences

Changes from Version 1

- Support TLS 1.2 for crypto-agility
- Key derivation makes use of TLS keying material exporters [RFC5705]
- Comply with TLS Ticket extension [RFC5077]
- Basic password authentication defined in base protocol.
- Additional TLV types: Identity Type TLV and Channel- Binding TLV

EAP-FASTv2 Advantages

- Based on existing EAP method with broad deployment base
- No backward compatibility issue (thru version negotiation)
- Server stateless session resumption (RFC5077)
- Basic password authentication defined in base protocol
- 100% compliant with EAP Tunnel Method Requirements (draft-ietf-emu-eaptunnel-req-09.txt)
- Crypto-agile
- TEAM draft is somewhat incomplete

Differences with TEAM

Item	EAP-FASTv2	TEAM
EAP Type	43 (based on existing EAP)	TBD (a new one)
Tunnel Key Derivation	TLS-PRF	TLS-PRF-128 as defined in EAP-TLS, not crypto-agile
Inner Session key derivation	TLS-PRF	HDKF specified, but no hash function specified
Master Session key	Use specific label	Use the same label for key derivation as in EAP-TLS
Outer TLV and protection of outer data	A-ID	Outer TLV, EAP type, version included in crypto-binding
Password Authentication	Built-in, support password change	Using EAP-GTC with EAP-PWC.
Peer-ID. Server-ID, Session ID	Defined	Not defined
URI TLV	Not defined	Not clear about the purpose Potential security issue

Call for Action

- Adopt EAP-FAST v2 as WG item
  - Based on existing EAP method with broad deployment base
  - 100% compliant with EAP Tunnel Method Requirements
  - Fully specified

Questions?

Requirement Compliance Matrix

Requirement	Compliance	Notes
4.1.1 RFC Compliance	✔	RFC 3748, RFC 4017, RFC 5247, and RFC 4962
4.2.1 TLS Requirements	✔	Supports TLS 1.2
4.2.1.1.1 Cipher Suite Negotiation	✔	Provided by TLS
4.2.1.1.2 Tunnel Data Protection Algorithms	✔	One mandatory cipher with at least 128 bit AES
4.2.1.1.3 Tunnel Authentication and Key Establishment	✔	Provided by TLS
4.2.1.2 Tunnel Replay Protection	✔	Provided by TLS
4.2.1.3 TLS Extensions	✔	Supports TLS Certificate Status Request and SessionTicket extension
4.2.1.4 Peer Identity Privacy	✔	Provided by TLS
4.2.1.5 Session Resumption	✔	Supports stateful and stateless (RFC5077)

Requirement Compliance Matrix (2)

Requirement	Compliance	Notes
4.2.2 Fragmentation	✔	Provided by TLS
4.2.3 Protection of Data External to Tunnel	✔	Inclusion of version number in crypto-binding
4.3.1 Extensible Attribute Types	✔	Extensive TLV, vendor type
4.3.2 Request/Challenge Response Operation	✔	Multiple TLVs in a request and response packet
4.3.3 Indicating Criticality of Attributes	✔	Mandatory bit in TLV
4.3.4 Vendor Specific Support	✔	Vendor TLV
4.3.5 Result Indication	✔	Result and IM-Result TLV
4.3.6 Internationalization of Display Strings	✔	Support UTF-8 in password authentication request and response
4.4 EAP Channel Binding Requirements	✔	Supports channel binding
4.5.1.1 Confidentiality and Integrity	✔	Provided by TLS

Requirement Compliance Matrix (3)

Requirement	Compliance	Notes
4.5.1.2 Authentication of Server	✔	Mandatory of TLS cipher
4.5.1.3 Server Certificate Revocation Checking	✔	Supports TLS Certificate Status Request extension
4.5.2 Internationalization	✔	Supports UTF-8 in password exchanges
4.5.3 Meta-data	✔	Identity Type TLV
4.5.4 Password Change	✔	Supports in basic password request and response
4.6.1 Method Negotiation	✔	Protected by TLS
4.6.2 Chained Methods	✔	Supports EAP chaining
4.6.3 Cryptographic Binding with the TLS Tunnel	✔	Crypto-binding mandatory
4.6.4 Peer Initiated	✔	Request-Action TLV
4.6.5 Method Meta-data	✔	Identity Type TLV