EAP-GPSK

draft-ietf-emu-eap-gpsk-01

Charles Clancy
Hannes Tschofenig

EMU WG, IETF 67
Current Status

- draft-clancy-emu-shared-secret-02.txt became draft-ietf-emu-eap-gpsk-00.txt
- -00 available on IETF site
- -01 submitted
From draft-clancy-emu-eap-gpsk-01.txt to draft-ietf-emu-eap-gpsk-00.txt

Issue Tracker: http://www.tschofenig.com:8080/eap-gpsk/

- Issue#4: Delimiter for Identities in KDF
- Issue#3: KDFData
- Issue#6: Ciphersuites
- Issue#5: Error Handling
- Issue#2: Channel Binding
- Issue#1: Protected Results Indication

Thanks to Lakshminath Dondeti, David McGrew, Bernard Aboba, Michaela Vanderveen and Ray Bell for their input to the ciphersuite discussions. Thanks to Lakshminath for his detailed draft review.
Issue#4: Delimiter for Identities in KDF

- Lakshminath suggested change for KDF:
  - From:
    \[ \text{RAND}_{\text{Client}} \ || \ \text{RAND}_{\text{Server}} \ || \ \text{ID}_{\text{Client}} \ || \ \text{ID}_{\text{Server}} \]
  - To:
    \[ \text{RAND}_{\text{Client}} \ || \ \text{ID}_{\text{Client}} \ || \ \text{RAND}_{\text{Server}} \ || \ \text{ID}_{\text{Server}} \]

- Accepted.
Issue#3: KDFData

- KDFData_Client and KDFData_Server provided ways to include arbitrary data in the KDF.

- Concept removed.
### Issue#6: Ciphersuites

- **Changed from:**

```
+---------------------------------+---------------------------------+---------------------------------+---------------------------------+
|   CSuite/  |   KS   |  Encryption  |  Integrity  |  Key Derivation   |
|  Specifier |       |              |            |                  |
+---------------------------------+---------------------------------+---------------------------------+---------------------------------+
|   0x000001 |   16   |  AES-EAX-128 |  AES-CMAC-128 |  GKDF-128 |
+---------------------------------+---------------------------------+---------------------------------+---------------------------------+
```

- **To:**

```
+---------------------------------+---------------------------------+---------------------------------+---------------------------------+
|   CSuite/  |   KS   |  Encryption  |  Integrity  |  Key Derivation   |
|  Specifier |       |              |            |                  |
+---------------------------------+---------------------------------+---------------------------------+---------------------------------+
|   0x000001 |   16   |  AES-CBC-128 |  AES-CMAC-128 |  GKDF-128 |
+---------------------------------+---------------------------------+---------------------------------+---------------------------------+
```
Issue#2: Channel Binding

- Removed from draft
- Possible through extensions
KDF Inconsistencies

- Fixed in submitted -01
- KDF updated in chapter 4 but not chapter 6
- Allows use of arbitrary-length input key to KDF, rather than just truncating it to a certain size
Still Open

- **Issue#5: Error Handling**
  - What to do if MAC error?
  - Return EAP-Failure (i.e. PSK mismatch)
  - Silently discard packet

- **Issue#1: Protected Results Indication**
  - Define PRI within the document, rather than as something that could be added later
  - What results should be returned?
Next Steps

- Resolve remaining open issues
- Editorial polishing needed
- Target for WGLC: Late November 2006
Backup Slides
Design Goals

- **Simplicity**: easy to implement
- **Wide Applicability**: secure, embedded devices
- **Efficiency**: no PK ops, 2 round trips
- **Flexibility**: multiple ciphersuites
- **Extensibility**: secure data exchange with many applications
Protocol Overview

- 2 round trips
- Supports both HMAC and AES-based ciphersuites
  - AES: CBC-128, CMAC-128
  - HMAC: SHA256
- Authenticated data exchange
  - If AES used, also confidential
Keying Hierarchy

- PL-octet PSK
- CSuite
- RAND_C || ID_C || RAND_S || ID_S

\[ \text{KDF} \]

- KS-octet MK

\[ \text{KDF} \]

- 64-octet MSK
- 64-octet EMSK
- KS-octet SK
- KS-octet PK
KDF

\[
\text{GKDF-X (Y, Z) \{}
\text{n = int( X / size - 1 ) + 1;}
\text{M_0 = "";}
\text{result = "";}
\text{for i=1 to n \{}
\text{M_i = MAC_Y (M_{i-1} || Z || i || X);}
\text{result = result || M_i;}
\text{\} return truncate (result; X);}
\text{\}}}
\]
Protocol

SEC_SK(ID_C, ID_S, RAND_C, RAND_S, [ENC_PK(PD_Payload_1)])

SEC_SK(RAND_C, RAND_S, CSuite_Sel, [ENC_PK(PD_Payload_2)])

SEC_SK([ENC_PK(PD_Payload_3)])
Packet Formatting

- Protected data payloads are a series of TLV-encoded items
- Ciphersuite and PD types are 6 bytes
  - First 3 are vendor OID, IETF = 0x000000
  - Last 3 are the type specifier
Security Properties

✓ Mutual Authentication
+ Protected Result Indications
✓ Integrity Protection
✓ Replay Protection
✓ Reflection Attack Protection
✓* Dictionary Attack Protection
✓ Key Derivation
✓ Denial of Service Resistance
✓ Session Independence
X Perfect Forward Secrecy
N/A Fragmentation
+ Channel Binding
X Fast Reconnect
+ Identity Protection
✓ Protected Ciphersuite Negotiation
✓ Confidentiality
N/A Cryptographic Binding

✓ Supported
+ Use PD Channel
X Unsupported
N/A Not Applicable
* If the shared secret is randomly created.