MIKEY [RFC3830]

MIKEY design principles

- End-to-end security
  - Only the participants involved in the communication have access to the generated key(s)

- Simplicity

- Efficiency
  - Low bandwidth consumption, low computational workload, small code size, and minimal number of roundtrips

- Tunneling
  - Possibility to integrate MIKEY in session establishment protocols

- Independence
  - Independent from any specific security functionality of the underlying transport
MIKEY Updates

- RFC 4650 - HMAC-Authenticated Diffie-Hellman for Multimedia Internet KEYing (MIKEY)
- RFC 4738 - MIKEY-RSA-R: An Additional Mode of Key Distribution in Multimedia Internet KEYing (MIKEY)
Motivation

What is missing?

MIKEY mode that provides

- Mutual authentication of involved parties
- All parties involved contribute to the session key generation
- Perfect forward and backward secrecy
- Only the participants involved in the communication have access to the session key
  - No key escrow
- Based on asynchronous cryptography without certificate-based PKI
Solution

**MIKEY-IBAKE**

- IBAKE: Identity Based Authenticated Key Agreement
  - *Identity Based Systems:* A new step in public key cryptography
  - Mutual authentication of endpoints
  - Establishment of the end-to-end security
  - Perfect forward and backward secrecy

- Expected application domains
  - Media plane security in the 3GPP IP Multimedia Subsystem (IMS)
  - Managed Services for Enterprises
Solution Framework

Based on an Identity Based asymmetric cryptographic framework

- Every participant has a public and a private key
- Public key (PubK) is identity based (e.g., IMSIdentity||date)
- Private key (PrK) corresponding to Public key is issued by a trusted Key Management Service (KMS)
- Participants obtain private keys from KMS offline
  - Example: Participants contact their KMS once a month (more generally for the length of the subscription)
  - Security association between KMS and participant is pre-provisioned
- Encryption and Decryption of messages during key exchange based on Identity Based Encryption (IBE)
  - Reference: Boneh et al., RFC 5091, RFC 5408, RFC 5409
Private Keys

Assumption: Initiator and Responder have security associations with their corresponding KMSs.

These exchanges take place periodically.

- Key_Request(Initiator_ID)
- Key_Request(Responder_ID)
- Key_Response
- Key_Response

Initiator’s private key (I_PrK)

Responder’s private key (R_PrK)
MIKEY-IBAKE Basic Operation

- Initiator's public key (I_PubK)
- Responder's public key (R_PubK)
- Initiator's private key (I_PrK)
- Responder's private key (R_PrK)
- Public parameter: a known point on a known elliptic curve

**Identity Based Authenticated Key Exchange**

- **Initiator**
  - Chooses random $a$, and computes $aP$
  - Decrypts the message using $I_PrK$ and verifies received $aP$
  - IBE($R_PubK$, $I_ID$ | $R_ID$ | $aP$)

- **Responder**
  - Chooses random $b$, and computes $bP$
  - IBE($I_PubK$, $I_ID$ | $R_ID$ | $aP$ | $bP$)
  - IBE($R_PubK$, $I_ID$ | $R_ID$ | $bP$)
  - Verification
  - Both Initiator and Responder generated the same session key ($abP$)
MIKEY-IBAKE Discussion

- Exchanged Elliptic Curve Diffie-Hellman (ECDH) values are IBE encrypted
- Session Key (abP) known only to Initiator and Responder
  - Due to hardness of the elliptic curve Diffie-Hellman problem
- Protocol necessitates three-way exchange
  - Session key can be generated after second message
MIKEY-IBAKE securely supports following features

- **Forking** - delivery of a request to multiple endpoints
  - Established session key is known only to the Initiator and the endpoint that answered the call

- **Retargeting** - request sent to one endpoint but delivered to a different endpoint
  - Established session key is known only to the Initiator and the endpoint that answered the call

- **Deferred delivery** - session content cannot be delivered to the destination at the time that it is being sent
  - Encrypted session content/media is stored
  - Stored media can be decrypted only by the intended Responder
Possible Extensions

Group Communication

- Group key not known to the Conference Server
- Adding a new participant
  - Group key changes after new user is admitted
- Participant exits the call
  - Group key changes after participant exits the call
Next Step

Specify MIKEY-IBAKE in msec WG