FSU: Identity-based
Authenticated Key Exchange

draft-kato-fsu-key-exchange-00.txt
draft-kato-optimal-ate-pairings-00.txt
draft-kasamatsu-bncurves-01.txt

KATO, Akihiro
NTT Software Corp

CFRG, IETF 94, Yokohama
2015 November 2nd
Management of credentials on IoT

- Typical credentials.
  - Pre-Shared
  - Raw Public Key
  - Certificate

- 2-3 billion devices will be wirelessly connected by 2020.
- A management of credentials will be one of problem.
PSK-Based Credential

- Example 1. Venders set both of ID and PW as “Admin”. Users change PW and ID.
- Example 2. Venders set both of ID and PW as complicated one. Users should not change ID and PW.
- Example 3. Venders set both of ID and PW as complicated one. Users change PW and ID.

Problems for management of a large number of credentials.
- Management cost of ID and PW, for Ex1 and EX3, will enlarge.
- Security level reduced by list-based attack.
PKI-Based Credential

Merit of PKI-based solution
- Low Management cost at server, comparison with PSK.
- Credentials are automatically chosen at random.
ID-Based Credential

1. Gen ID
2. Ship device
3. ID, ID'
4. sk
5. Encrypted Connection

Factory
Auth. of Entity
KGC
Authentication Server
Device
User

Just ID
Merit of ID-Based for large number of Cred.

- Low cost of generation of sk and pk for Device and Factory.
- Centralization of key generation.
- ID can be ruled.
- If ID lists are provided, KGC can previously generate secret keys.
FSU Key Exchange Protocol

- FSU is an identity-based authenticated key exchange (ID-AKE) protocol.
- FSU is only 2-pass scheme.

![FSU Key Exchange Diagram]

Initiator (I)
- Static secret key for I
- Ephemeral public key by I
- Compute session key

KGC
- Master secret key
- ID_I, epk_I

Responder (R)
- Static secret key for R
- Ephemeral public key by R
- Compute session key

ID_R, epk_R
Security of FSU

- FSU is proven to be secure in id-eCK security model.
- id-eCK security model is one of the most strongest security model against secret key leakage.
- Session key will be safe, even if attacker get any non-trivial combination of master key, static key, and ephemeral key.

```
Initiator (I) -------- Master secret key -------- Responder (R)
Static secret key    Static secret key
Ephemeral secret key Ephemeral secret key

○: Secure combination of leakage
```
Protection of session key

• Id-eCK security implies resistance of following security threats:
  – MitM(resistance to man in the middle attacks)
  – wPFS(weak perfect forward security)
  – KCI(resistance to key compromise impersonation attacks)
  – RLE(resilience to leakage of ephemeral private keys)
Comparison with other ID-AKE

1. RFC6539:IBAKE
2. ISO/IEC FDIS 11770-3 p68 F.3 IBAKE following Smart-Chen-Cheng (SCC)

<table>
<thead>
<tr>
<th></th>
<th>Security Model</th>
<th>Connection times</th>
<th>Pairing times</th>
<th>Key Size (Oct)</th>
<th>Payload Size(Oct)</th>
</tr>
</thead>
<tbody>
<tr>
<td>FSU</td>
<td>eCK</td>
<td>2</td>
<td>8</td>
<td>32</td>
<td>98</td>
</tr>
<tr>
<td>IBAKE</td>
<td>CK</td>
<td>3</td>
<td>$3 \times (\text{ENC}+\text{DEC})^*$</td>
<td>32</td>
<td>414</td>
</tr>
<tr>
<td>SCC</td>
<td>CK</td>
<td>2</td>
<td>4</td>
<td>32</td>
<td>33</td>
</tr>
</tbody>
</table>

*1: Pairing times of IBAKE depends Enc and Dec of IBE.
Security of IBAKE and SCC

Security Model of IBAKE

- Master secret key
- Initiator (I)
- Static secret key
- Ephemeral secret key
- Responder (R)

Security Model of SCC

- Master secret key
- Initiator (I)
- Static secret key
- Ephemeral secret key
- Responder (R)
Why we wrote three IDs.

Pairing and BN Curves layer can be used by other protocols.

Elliptic Curve selection requirement is different from ECC.

Pairing-based Crypto

- FSU Key Exchange
- Pairing function
- BN Curves (Elliptic Curves)

Elliptic Curve Crypto

- EdDSA
- Scalar Multiply
- Ed25519
Our selects.

• Pairing
  
  We choose:
  – Optimal Ate Pairing that is fastest pairing algorithm now.
    • Its computation time is about ten-times or more as fast as Tate Pairing which is defined by Boneh-Franklin (RFC5091).
    • \textit{draft-kato-optimal-ate-pairings} specifies algorithms and test vectors which are suitable four BN-curves.

• Elliptic Curves
  
  We choose:
  – Barreto-Naehrig curves (BN-curves) that have 128-bit security and are suitable for pairing-based cryptography.
    • \textit{draft-kasamatsu-bncurves} specifies domain parameters of four 254-bit BN-curves.
Security of Pairing over BN-curves

- Pairing map $G_1 \times G_2 \rightarrow G_T$
  - $G_1$, $G_2$ are group of elliptic curve.
  - $G_T$ is finite field $F_{p^{12}}$.

- All BN-curves have (written in our draft) have 128-bit security.
  - The order of $G_1$ and $G_2$ is 254-bit.
  - The order of $G_T$ is $254 \times 12$-bit.
  - Hardness of ECDLP and FFDLP is 128-bit security.
Future work

• We are going to standardize key generation center for ID-based Crypto.
Any comments and questions?

- draft-kato-fsu-key-exchange-00.txt
- draft-kato-optimal-ate-pairings-00.txt
- draft-kasamatsu-bncurves-01.txt

My office is here ;-).

We are here.