Identity-Based Signatures for MANET Routing Protocols

draft-dearlove-manet-ibs-00

Christopher Dearlove

Presented by Ulrich Herberg

Status

Personal draft, intended for WG adoption, Standards Track.

Updates RFC 7182 that:

- Defined an ICV TLV for RFC 5444 packets/messages.
- Included crypto function and hash function codepoints.
- Used shared secret key in most specified cases.
- Is partially mandated for implementation using OLSRv2/ NHDP (by RFC 7183).

Draft defines two related new crypto function codepoints.

Identity-based signature

Defines an identity-based signature (IBS).

- All routers individually keyed.
  - Potentially less harm when router compromised.
  - Possible revocation, information in identity (beyond scope).
- Routers independently keyed by trusted authority (KMS).
  - No need to know any other router's identity in advance.
  - Additional routers can be added in future, no changes needed.
- Trusted authority not needed during network operation.
  - Authority can be kept "out of harm's way".

Good fit to characteristics of many ad hoc networks.

Drawbacks

Trusted authority has to be completely trusted:

- It can sign anything as anybody.
  - Possible to destroy it if no new keys will be needed.

Implementations based on elliptic curve mathematics:

- Need suitable mathematical library.
- Signatures computationally relatively expensive.
- Signatures larger at same strength than shared key.

More that one possible implementation, tradeoff.

Selection

RFC 6507: Elliptic Curve-Based Certificateless Signatures for Identity-Based Encryption (ECCSI)

- Accepted informational RFC.
- Draft repeats RFC 6507 elliptic curve recommendation.
  - Also needs hash function, SHA-256 recommended.
- Does not use “pairings” (bilinear function from elliptic curve to another group) unlike some other IBS cases.
  - Pairings are expensive, this is faster than cases using them.
- Larger signature than some IBS cases.
  - With recommended elliptic curve, signature length is 129 octets (to be compatible with RFC 6507, allows code reuse).
  - Cannot truncate, need whole signature to verify.
  - Security level 128 bits (similar to HMAC-SHA-256, 32 octets).

Identity

Identity can be anything tied to router.

- Natural choice is IP address.
  - Originator address for messages, IP source address for packets.
  - These may not be suitable (originator address may not be present, source address may not be unique on router).
  - Also need an option not based on address.
- Also may want to add to address, e.g. added validity.
- Can use `<key-id>` from RFC 7182.
- Two options: just `<key-id>`, address + `<key-id>`.
  - These are the two crypto functions: `ECCSI` and `ECCSI-ADDR`.
  - Like HMAC, these define how to use hash, not just composed.
  - Verify function, rather than re-sign (impossible) and compare.

Next Steps

- **I hereby ask the WG chairs to call for WG adoption of this document.**