IKE DH–Less Encryption Mode

Ran Canetti   Hugo Krawczyk   Pau-Chen Cheng

August 24, 1998

42nd IETF

Motivation

A **LOW COST** SA establishment mechanism for applications whose primary concern is to protect information integrity rather than long–term secrecy.

- Busy **SERVERS** providing public information : digital library, on–line catalog, yellow page, stock quoting.
- Low–end, mobile **CLIENTS** accessing these servers.
- anything you can suggest.

Protocol Highlight

- Like the IKE "Revised Public Key Encryption Mode" without exchanging Diffie–Hellman public values.

- Use the secret nonces, N_i and N_r, as the key to PRF through which SKEYID is derived.

- define g^{xi}, g^{xr} and g^{xy} to be an octet of zero so the definitions of HASH_I, HASH_R, SKEYID_d, SKEYID_a and SKEYID_e remain unchanged.

I R

HDR, SA$_{proposal}$

$\longrightarrow$

HDR, SA$_{choice}$

$\longleftarrow$

HDR, [Hash(1)], $< N_i\_b >_{PK_R}, < ID_{ii}\_b >_{Ke\_i},$
$[< Cert - I\_b >_{Ke\_i}]$

$\longrightarrow$

HDR, $< N_r\_b >_{PK_I}, < ID_{ir}\_b >_{Ke\_r}$

$\longleftarrow$

HDR*, $HASH\_I$

$\longrightarrow$

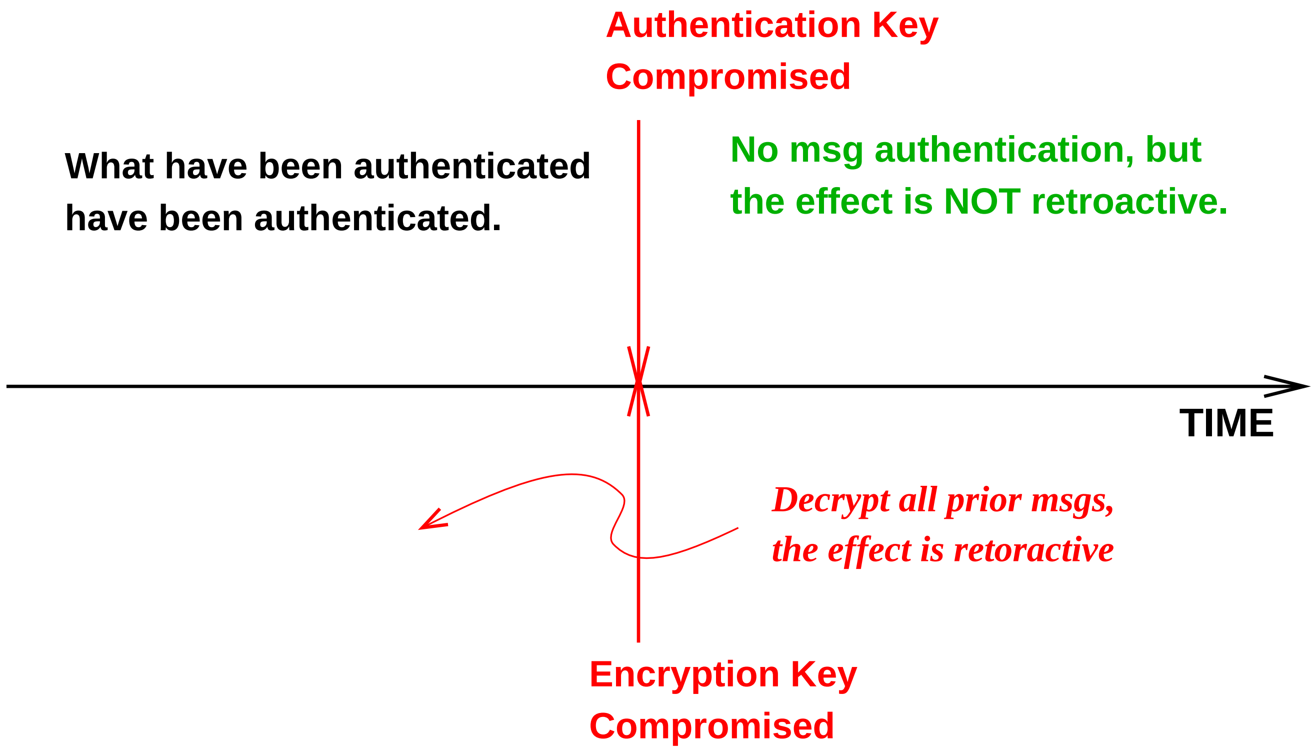
HDR*, $HASH\_R$

$\longleftarrow$

Pro's and Con's

- **Pro's** : lower computation cost : 2 modular exponentiations (RSA encryption/decryption) versus 4 modular exponentiations (RSA encryption/decryption + DH).

- **Con's** : no PFS (no DH); BUT
  - does NOT matter for **Authentication Only** operations.
  - suitable when only **Short–Term Secrecy** is needed.


Authentication Key
Compromised
What have been authenticated
have been authenticated.
No msg authentication, but
the effect is NOT retroactive.
TIME
Decrypt all prior msgs,
the effect is retoractive
Encryption Key
Compromised

A Note on PKCS#1

- the original PKCS#1 format is not secure against chosen ciphertext attacks (Daniel Bleichenbacher, "Chosen Ciphertext Attacks Against Protocols Based on the RSA Encryption Standard PKCS #1", Crypto'98).

- RSA encryptions in all IKE public–key encryption modes should use the new PKCS#1 specification employing OAEP (Optimal Asymmetric Encryption Padding), which is believed to be secure against chosen ciphertext attacks.

  `http://www.rsa.com/rsalabs/pkcs1/index.html`

  `http://www.rsa.com/rsalabs/pkcs1/oem_counter.html`

  OAEP patch to RSA BSAFE toolkit is available from

  `http://support.rsa.com`