IKEv2: Internet Key Exchange, version 2

authentication based on digital signatures

Protocol Purpose

IKE is designed to perform mutual authentication and key exchange prior to setting up an IPsec connection.

IKEv2 exists in several variants, the defining difference being the authentication method used.

This variant, which we call IKEv2-DS, uses digital signatures.

Definition Reference

[Kau03]

Model Authors

- Sebastian Mödersheim, ETH Zürich, December 2003
-

```
                SA2(3)}(f(Ni(1),Nr(2),SA1(1),exp(exp(g,DHY(2)),DHX(1))))
i -> (b,3): {a,{SA1(1),exp(g,DHX(1)),Ni(1),Nr(2)}inv(ka),
                SA2(3)}(f(Ni(1),Nr(2),SA1(1),exp(exp(g,DHX(1)),DHY(2))))
(b,3) -> i: {b,{SA1(1),exp(g,DHY(2)),Nr(2),Ni(1)}inv(kb),
                SA2(3)}(f(Ni(1),Nr(2),SA1(1),exp(exp(g,DHX(1)),DHY(2))))
```

This attack is of questionable validity, as the intruder has not actually learned the key that *b* believes to have established with *a*

```
%% parameters.  Alice sends a nonce SAi1, which is meant to
%% model Alice sending only a single crypto-suite offer.  Bob must
```

```
init  State := 1
```

```
      ka, kb, ki : public_key,
      g:text, f       : function

intruder_knowledge = {g,f,a,b,ka,kb,i,ki,inv(ki)
                      }

composition

      session(a,b,ka,kb,g,f)
```

Protocol Analyzer. In *Proceedings of the 1999 IEEE Symposium on Security and Privacy*. IEEE Computer Society Press, 1999.