

Authenticated key agreement

Tanja Lange

Eindhoven University of Technology

2WF80: Introduction to Cryptology

Practical problems

- ▶ Eve can set up a *man-in-the-middle* attack:

$$A \xleftrightarrow{g^{ae}} E \xleftrightarrow{g^{bf}} B$$

E decrypts everything from A and reencrypts it to B and vice versa.

- ▶ This attack cannot be detected unless A and B have some long-term keys that are known to each other or compare their keys out of band.

Practical problems

- ▶ Eve can set up a *man-in-the-middle* attack:

$$A \xleftrightarrow{g^{ae}} E \xleftrightarrow{g^{bf}} B$$

E decrypts everything from A and reencrypts it to B and vice versa.

- ▶ This attack cannot be detected unless A and B have some long-term keys that are known to each other or compare their keys out of band.
- ▶ How to do this in practice?

Needham-Schroeder identification protocol

Convince Alice she is talking to Bob and vice versa.

Alice knows Bob's h_B , Bob knows Alice's h_A .

Alice

sample ℓ -bit nonce

$n_A \leftarrow_{\$} \{0, 1\}^\ell$

encrypt n_A, h_A to h_B

$\text{Enc}_{h_B}(n_A, h_A)$

decrypt, check n_A

obtain n_B

$\text{Enc}_{h_B}(n_B)$

Use $H(n_A, n_B)$ as key for symmetric crypto.

Bob

decrypt to obtain n_A, h_A

sample ℓ -bit nonce

$n_B \leftarrow_{\$} \{0, 1\}^\ell$

decrypt, check n_B

Needham-Schroeder identification protocol

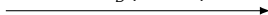
Convince Alice she is talking to Bob and vice versa.

Alice knows Bob's h_B , Bob knows Alice's h_A .

Alice

$n_A \leftarrow \{0, 1\}^\ell$

$\text{Enc}_{h_B}(n_A, h_A)$



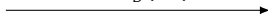
Bob

$n_B \leftarrow \{0, 1\}^\ell$

$\text{Enc}_{h_A}(n_A, n_B)$



$\text{Enc}_{h_B}(n_B)$



Use $H(n_A, n_B)$ as key for symmetric crypto.

Needham-Schroeder identification protocol

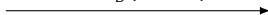
Convince Alice she is talking to Bob and vice versa.

Alice knows Bob's h_B , Bob knows Alice's h_A .

Alice

$n_A \leftarrow \{0, 1\}^\ell$

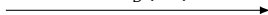
$\text{Enc}_{h_B}(n_A, h_A)$



$\text{Enc}_{h_A}(n_A, n_B)$



$\text{Enc}_{h_B}(n_B)$



Bob

$n_B \leftarrow \{0, 1\}^\ell$

Use $H(n_A, n_B)$ as key for symmetric crypto.

Does this achieve the purpose?

Can Eve get in the middle, and if so where?

Needham-Schroeder identification protocol

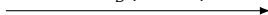
Convince Alice she is talking to Bob and vice versa.

Alice knows Bob's h_B , Bob knows Alice's h_A .

Alice

$n_A \leftarrow \{0, 1\}^\ell$

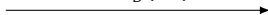
$\text{Enc}_{h_B}(n_A, h_A)$



$\text{Enc}_{h_A}(n_A, n_B)$



$\text{Enc}_{h_B}(n_B)$



Bob

$n_B \leftarrow \{0, 1\}^\ell$

Use $H(n_A, n_B)$ as key for symmetric crypto.

Does this achieve the purpose?

Can Eve get in the middle, and if so where?

Is Alice sure she is talking to Bob?

Needham-Schroeder identification protocol

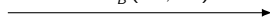
Convince Alice she is talking to Bob and vice versa.

Alice knows Bob's h_B , Bob knows Alice's h_A .

Alice

$n_A \leftarrow \{0, 1\}^\ell$

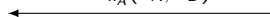
$\text{Enc}_{h_B}(n_A, h_A)$



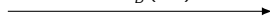
Bob

$n_B \leftarrow \{0, 1\}^\ell$

$\text{Enc}_{h_A}(n_A, n_B)$



$\text{Enc}_{h_B}(n_B)$



Use $H(n_A, n_B)$ as key for symmetric crypto.

Does this achieve the purpose?

Can Eve get in the middle, and if so where?

Is Alice sure she is talking to Bob?

Is Bob sure he is talking to Alice?

Eve in the middle in Needham-Schroeder

Eve in the middle in Needham-Schroeder

Assume that Eve can convince Alice to talk to her (as Eve).


Alice

$n_A \leftarrow \{0, 1\}^\ell$

Eve

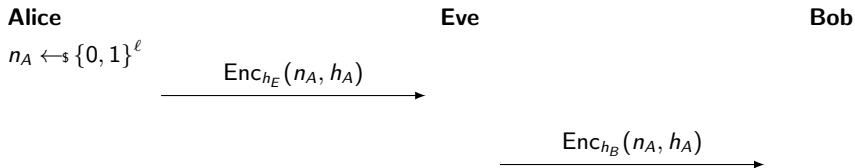
Bob

$\text{Enc}_{h_E}(n_A, h_A)$



Eve in the middle in Needham-Schroeder

Assume that Eve can convince Alice to talk to her (as Eve).



Eve in the middle in Needham-Schroeder

Assume that Eve can convince Alice to talk to her (as Eve).

Alice

$$n_A \leftarrow \{0, 1\}^\ell$$

$$\text{Enc}_{h_E}(n_A, h_A)$$

Eve

$$\text{Enc}_{h_B}(n_A, h_A)$$

$$\text{Enc}_{h_A}(n_A, n_B)$$

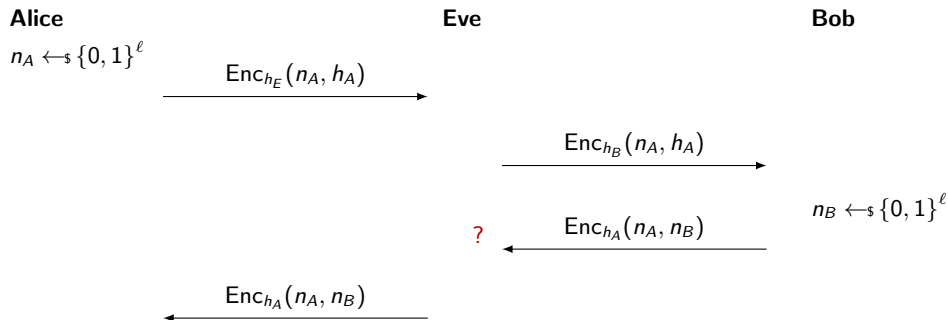
?

Bob

$$n_B \leftarrow \{0, 1\}^\ell$$

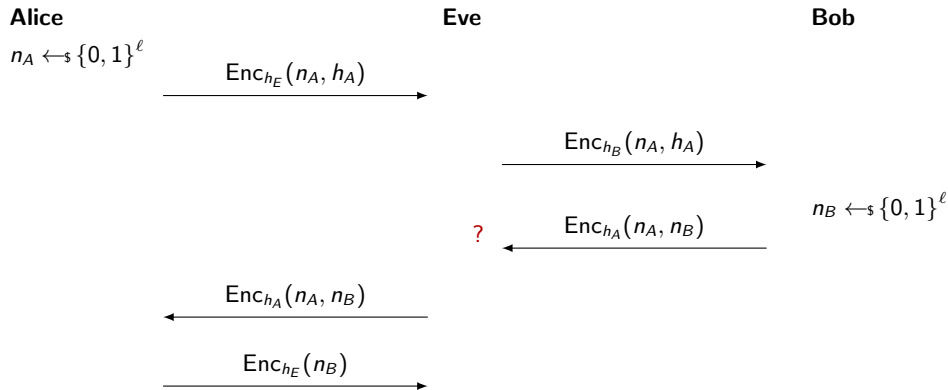
Eve in the middle in Needham-Schroeder

Assume that Eve can convince Alice to talk to her (as Eve).



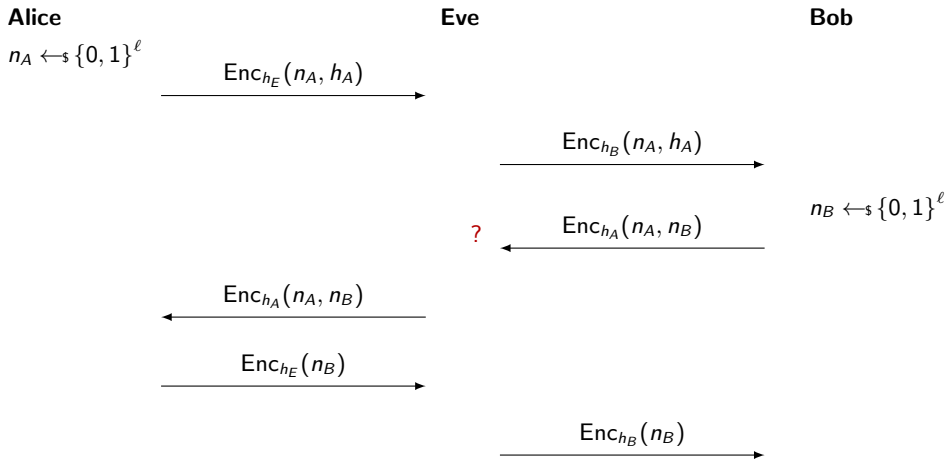
Eve in the middle in Needham-Schroeder

Assume that Eve can convince Alice to talk to her (as Eve).



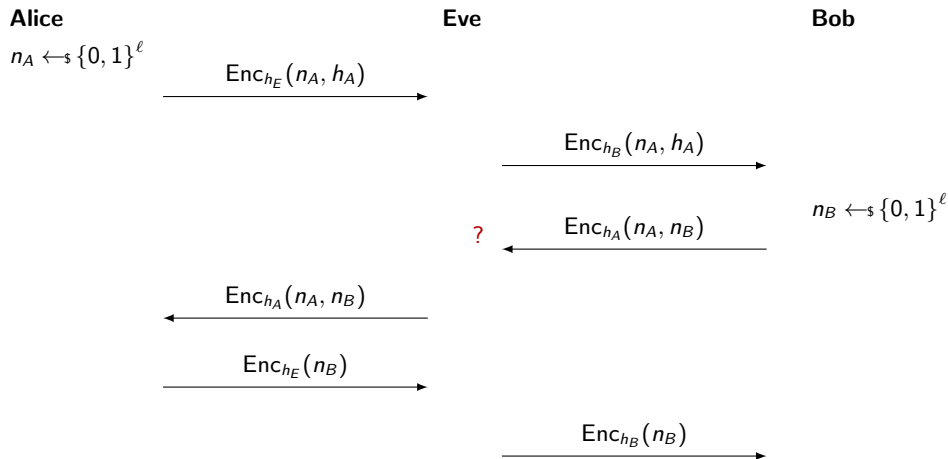
Eve in the middle in Needham-Schroeder

Assume that Eve can convince Alice to talk to her (as Eve).



Eve in the middle in Needham-Schroeder

Assume that Eve can convince Alice to talk to her (as Eve).



Alice is convinced that she has a connection with Eve.

Bob is convinced that he has a connection with Alice.

Diffie-Hellman with signatures

Alice has long-term signing key (a, A) , knows Bob's public signing key B .

Bob has long-term signing key (b, B) , knows Alice's public signing key A .

Alice

$$r \leftarrow_{\$} [1, |G| - 1]$$

$$\xrightarrow{g^r, \text{Sig}(g^r)}$$

verify

$$k = H((g^s)^r)$$

Bob

verify

$$s \leftarrow_{\$} [1, |G| - 1]$$

$$\xleftarrow{g^s, \text{Sig}(g^s)}$$

$$k = H((g^r)^s)$$

This works but requires signatures in addition to Diffie-Hellman.

Triple DH

Alice has long-term DH key $(a, h_A = g^a)$, knows Bob's public DH key h_B .

Bob has long-term DH key $(b, h_B = g^b)$, knows Alice's public DH key h_A .

Alice

$$r \leftarrow_s [1, |G| - 1]$$

$$\xrightarrow{g^r}$$

$$\xleftarrow{g^s}$$

$$k = H((g^s)^a, h_B^r, (g^s)^r)$$

Bob

$$s \leftarrow_s [1, |G| - 1]$$

$$k = H(h_A^s, (g^r)^b, (g^r)^s)$$

Triple DH

Alice has long-term DH key $(a, h_A = g^a)$, knows Bob's public DH key h_B .

Bob has long-term DH key $(b, h_B = g^b)$, knows Alice's public DH key h_A .

Alice

$$r \leftarrow_s [1, |G| - 1]$$

$$\xrightarrow{g^r}$$

Bob

$$s \leftarrow_s [1, |G| - 1]$$

$$\xleftarrow{g^s}$$

$$k = H((g^s)^a, h_B^r, (g^s)^r)$$

$$k = H(h_A^s, (g^r)^b, (g^r)^s)$$

Computing k requires knowledge of (a, r) , or (b, s) ,

Triple DH

Alice has long-term DH key $(a, h_A = g^a)$, knows Bob's public DH key h_B .

Bob has long-term DH key $(b, h_B = g^b)$, knows Alice's public DH key h_A .

Alice

$$r \leftarrow_s [1, |G| - 1]$$

$$\xrightarrow{g^r}$$

Bob

$$s \leftarrow_s [1, |G| - 1]$$

$$\xleftarrow{g^s}$$

$$k = H((g^s)^a, h_B^r, (g^s)^r)$$

$$k = H(h_A^s, (g^r)^b, (g^r)^s)$$

Computing k requires knowledge of (a, r) , or (b, s) , or (r, s) .

If Bob's random-number generator is broken, so that Eve knows s , then Eve can impersonate Alice to Bob.

Triple DH

Alice has long-term DH key $(a, h_A = g^a)$, knows Bob's public DH key h_B .

Bob has long-term DH key $(b, h_B = g^b)$, knows Alice's public DH key h_A .

Alice

$$r \leftarrow_s [1, |G| - 1]$$

$$\xrightarrow{g^r}$$

Bob

$$s \leftarrow_s [1, |G| - 1]$$

$$\xleftarrow{g^s}$$

$$k = H((g^s)^a, h_B^r, (g^s)^r)$$

$$k = H(h_A^s, (g^r)^b, (g^r)^s)$$

Computing k requires knowledge of (a, r) , or (b, s) , or (r, s) .

If Bob's random-number generator is broken, so that Eve knows s , then Eve can impersonate Alice to Bob.

Could include g^{ab} to deal with the latter concern.

Triple DH

Alice has long-term DH key $(a, h_A = g^a)$, knows Bob's public DH key h_B .

Bob has long-term DH key $(b, h_B = g^b)$, knows Alice's public DH key h_A .

Alice

$$r \leftarrow_s [1, |G| - 1]$$

$$\xrightarrow{g^r}$$

Bob

$$s \leftarrow_s [1, |G| - 1]$$

$$\xleftarrow{g^s}$$

$$k = H((g^s)^a, h_B^r, (g^s)^r)$$

$$k = H(h_A^s, (g^r)^b, (g^r)^s)$$

Computing k requires knowledge of (a, r) , or (b, s) , or (r, s) .

If Bob's random-number generator is broken, so that Eve knows s , then Eve can impersonate Alice to Bob.

Could include g^{ab} to deal with the latter concern.

Signal used to use 3DH as above but has changed to Extended Triple Diffie-Hellman (X3DH) (including signatures).