
Abbreviations
~X_1 = (a_7,encxor((a_8,(id(a_1,a_2),(edhoc_kdf(hkdfextract(
edhoc_kdf(hkdfextract(hash((wrap(a_7),wrap(hash(
(wrap(method_three),(wrap(a_4),(wrap(~M_5),(wrap(
a_5),a_6)))))))),exp(a_7,~M_8)),stone,hash((wrap(
a_7),wrap(hash((wrap(method_three),(wrap(a_4),
(wrap(~M_5),(wrap(a_5),a_6)))))))),hash_length),
exp(a_2,~M_8)),stwo,(id(a_1,a_2),(hash((wrap(a_7),
wrap(hash((wrap(method_three),(wrap(a_4),(wrap(
~M_5),(wrap(a_5),a_6)))))))),(a_2,a_9))),hash_length),
a_9))),edhoc_kdf(hkdfextract(hash((wrap(a_7),wrap(
hash((wrap(method_three),(wrap(a_4),(wrap(~M_5),
(wrap(a_5),a_6)))))))),exp(a_7,~M_8)),stzero,hash(
(wrap(a_7),wrap(hash((wrap(method_three),(wrap(
a_4),(wrap(~M_5),(wrap(a_5),a_6)))))))),plaintext_length)))
=
(a_7,encxor((a_8,(id(a_1,a_2),(edhoc_kdf(hkdfextract(
edhoc_kdf(hkdfextract(hash((wrap(a_7),wrap(hash(
(wrap(method_three),(wrap(a_4),(wrap(exp(g,X_1)),
(wrap(a_5),a_6)))))))),exp(a_7,X_1)),stone,hash(
(wrap(a_7),wrap(hash((wrap(method_three),(wrap(
a_4),(wrap(exp(g,X_1)),(wrap(a_5),a_6)))))))),
hash_length),exp(a_2,X_1)),stwo,(id(a_1,a_2),(
hash((wrap(a_7),wrap(hash((wrap(method_three),
(wrap(a_4),(wrap(exp(g,X_1)),(wrap(a_5),a_6)))))))),
(a_2,a_9))),hash_length),a_9))),edhoc_kdf(hkdfextract(
hash((wrap(a_7),wrap(hash((wrap(method_three),
(wrap(a_4),(wrap(exp(g,X_1)),(wrap(a_5),a_6)))))))),
exp(a_7,X_1)),stzero,hash((wrap(a_7),wrap(hash(
(wrap(method_three),(wrap(a_4),(wrap(exp(g,X_1)),
(wrap(a_5),a_6)))))))),plaintext_length)))
A trace has been found.
Honest Process
Attacker
!
!
!
!
{26}new sk_3
{27}new ltdh_1
{28}new computerId_1
(~M,(~M_1,~M_2)) = (id(pk(sk_3),exp(g,ltdh_1)),
(pk(sk_3),exp(g,ltdh_1)))
{31}event eShareLT(ltdh_1)
{32}event eHonest(pk(sk_3))
{33}event eHonest(exp(g,ltdh_1))
Beginning of process compromiseDH
!
!
Beginning of process compromise
id(a_1,a_2)
Beginning of process I
(method_three,(a_4,(a_5,a_6)))
{40}event eMethodOk(method_three)
{41}new X_1
{42}new EAD_1
{43}event eShare(X_1)
Beginning of process CompromiseShare
{45}event eLeakShare(X_1)
{46}event eLeakShare(exp(g,X_1))
(~M_3,(~M_4,(~M_5,(~M_6,~M_7)))) = (method_three,
(a_4,(exp(g,X_1),(a_5,a_6))))
~M_8 = X_1
~X_1
{144}event eDerivedIShared(exp(g,ltdh_1),exp(a_7,
X_1))
{148}event eTHIShared(exp(g,ltdh_1),hash((wrap(
hash((wrap(a_7),wrap(hash((wrap(method_three),
(wrap(a_4),(wrap(exp(g,X_1)),(wrap(a_5),a_6))))))))),
((a_8,(id(a_1,a_2),(edhoc_kdf(hkdfextract(edhoc_kdf(
hkdfextract(hash((wrap(a_7),wrap(hash((wrap(method_three),
(wrap(a_4),(wrap(exp(g,X_1)),(wrap(a_5),a_6)))))))),
exp(a_7,X_1)),stone,hash((wrap(a_7),wrap(hash(
(wrap(method_three),(wrap(a_4),(wrap(exp(g,X_1)),
(wrap(a_5),a_6)))))))),hash_length),exp(a_2,X_1)),
stwo,(id(a_1,a_2),(hash((wrap(a_7),wrap(hash((
wrap(method_three),(wrap(a_4),(wrap(exp(g,X_1)),
(wrap(a_5),a_6)))))))),(a_2,a_9))),hash_length),
a_9))),a_2))))
{160}event eAcceptI(computerId_1,method_three,
exp(g,ltdh_1),a_2,hkdfextract(edhoc_kdf(hkdfextract(
hash((wrap(a_7),wrap(hash((wrap(method_three),
(wrap(a_4),(wrap(exp(g,X_1)),(wrap(a_5),a_6)))))))),
exp(a_7,X_1)),stone,hash((wrap(a_7),wrap(hash(
(wrap(method_three),(wrap(a_4),(wrap(exp(g,X_1)),
(wrap(a_5),a_6)))))))),hash_length),exp(a_2,X_1)),
hkdfextract(edhoc_kdf(hkdfextract(edhoc_kdf(hkdfextract(
hash((wrap(a_7),wrap(hash((wrap(method_three),
(wrap(a_4),(wrap(exp(g,X_1)),(wrap(a_5),a_6)))))))),
exp(a_7,X_1)),stone,hash((wrap(a_7),wrap(hash(
(wrap(method_three),(wrap(a_4),(wrap(exp(g,X_1)),
(wrap(a_5),a_6)))))))),hash_length),exp(a_2,X_1)),
sfive,hash((wrap(hash((wrap(a_7),wrap(hash((wrap(
method_three),(wrap(a_4),(wrap(exp(g,X_1)),(wrap(
a_5),a_6))))))))),((a_8,(id(a_1,a_2),(edhoc_kdf(
hkdfextract(edhoc_kdf(hkdfextract(hash((wrap(a_7),
wrap(hash((wrap(method_three),(wrap(a_4),(wrap(
exp(g,X_1)),(wrap(a_5),a_6)))))))),exp(a_7,X_1)),
stone,hash((wrap(a_7),wrap(hash((wrap(method_three),
(wrap(a_4),(wrap(exp(g,X_1)),(wrap(a_5),a_6)))))))),
hash_length),exp(a_2,X_1)),stwo,(id(a_1,a_2),(
hash((wrap(a_7),wrap(hash((wrap(method_three),
(wrap(a_4),(wrap(exp(g,X_1)),(wrap(a_5),a_6)))))))),
(a_2,a_9))),hash_length),a_9))),a_2))),hash_length),
exp(a_7,ltdh_1)),edhoc_kdf(hkdfextract(edhoc_kdf(
hkdfextract(edhoc_kdf(hkdfextract(hash((wrap(a_7),
wrap(hash((wrap(method_three),(wrap(a_4),(wrap(
exp(g,X_1)),(wrap(a_5),a_6)))))))),exp(a_7,X_1)),
stone,hash((wrap(a_7),wrap(hash((wrap(method_three),
(wrap(a_4),(wrap(exp(g,X_1)),(wrap(a_5),a_6)))))))),
hash_length),exp(a_2,X_1)),sfive,hash((wrap(hash(
(wrap(a_7),wrap(hash((wrap(method_three),(wrap(
a_4),(wrap(exp(g,X_1)),(wrap(a_5),a_6))))))))),
((a_8,(id(a_1,a_2),(edhoc_kdf(hkdfextract(edhoc_kdf(
hkdfextract(hash((wrap(a_7),wrap(hash((wrap(method_three),
(wrap(a_4),(wrap(exp(g,X_1)),(wrap(a_5),a_6)))))))),
exp(a_7,X_1)),stone,hash((wrap(a_7),wrap(hash(
(wrap(method_three),(wrap(a_4),(wrap(exp(g,X_1)),
(wrap(a_5),a_6)))))))),hash_length),exp(a_2,X_1)),
stwo,(id(a_1,a_2),(hash((wrap(a_7),wrap(hash((
wrap(method_three),(wrap(a_4),(wrap(exp(g,X_1)),
(wrap(a_5),a_6)))))))),(a_2,a_9))),hash_length),
a_9))),a_2))),hash_length),exp(a_7,ltdh_1)),sseven,
hash((wrap(hash((wrap(hash((wrap(a_7),wrap(hash(
(wrap(method_three),(wrap(a_4),(wrap(exp(g,X_1)),
(wrap(a_5),a_6))))))))),((a_8,(id(a_1,a_2),(edhoc_kdf(
hkdfextract(edhoc_kdf(hkdfextract(hash((wrap(a_7),
wrap(hash((wrap(method_three),(wrap(a_4),(wrap(
exp(g,X_1)),(wrap(a_5),a_6)))))))),exp(a_7,X_1)),
stone,hash((wrap(a_7),wrap(hash((wrap(method_three),
(wrap(a_4),(wrap(exp(g,X_1)),(wrap(a_5),a_6)))))))),
hash_length),exp(a_2,X_1)),stwo,(id(a_1,a_2),(
hash((wrap(a_7),wrap(hash((wrap(method_three),
(wrap(a_4),(wrap(exp(g,X_1)),(wrap(a_5),a_6)))))))),
(a_2,a_9))),hash_length),a_9))),a_2)))),((id(pk(
sk_3),exp(g,ltdh_1)),(edhoc_kdf(hkdfextract(edhoc_kdf(
hkdfextract(edhoc_kdf(hkdfextract(hash((wrap(a_7),
wrap(hash((wrap(method_three),(wrap(a_4),(wrap(
exp(g,X_1)),(wrap(a_5),a_6)))))))),exp(a_7,X_1)),
stone,hash((wrap(a_7),wrap(hash((wrap(method_three),
(wrap(a_4),(wrap(exp(g,X_1)),(wrap(a_5),a_6)))))))),
hash_length),exp(a_2,X_1)),sfive,hash((wrap(hash(
(wrap(a_7),wrap(hash((wrap(method_three),(wrap(
a_4),(wrap(exp(g,X_1)),(wrap(a_5),a_6))))))))),
((a_8,(id(a_1,a_2),(edhoc_kdf(hkdfextract(edhoc_kdf(
hkdfextract(hash((wrap(a_7),wrap(hash((wrap(method_three),
(wrap(a_4),(wrap(exp(g,X_1)),(wrap(a_5),a_6)))))))),
exp(a_7,X_1)),stone,hash((wrap(a_7),wrap(hash(
(wrap(method_three),(wrap(a_4),(wrap(exp(g,X_1)),
(wrap(a_5),a_6)))))))),hash_length),exp(a_2,X_1)),
stwo,(id(a_1,a_2),(hash((wrap(a_7),wrap(hash((
wrap(method_three),(wrap(a_4),(wrap(exp(g,X_1)),
(wrap(a_5),a_6)))))))),(a_2,a_9))),hash_length),
a_9))),a_2))),hash_length),exp(a_7,ltdh_1)),ssix,
(id(pk(sk_3),exp(g,ltdh_1)),(hash((wrap(hash((
wrap(a_7),wrap(hash((wrap(method_three),(wrap(
a_4),(wrap(exp(g,X_1)),(wrap(a_5),a_6))))))))),
((a_8,(id(a_1,a_2),(edhoc_kdf(hkdfextract(edhoc_kdf(
hkdfextract(hash((wrap(a_7),wrap(hash((wrap(method_three),
(wrap(a_4),(wrap(exp(g,X_1)),(wrap(a_5),a_6)))))))),
exp(a_7,X_1)),stone,hash((wrap(a_7),wrap(hash(
(wrap(method_three),(wrap(a_4),(wrap(exp(g,X_1)),
(wrap(a_5),a_6)))))))),hash_length),exp(a_2,X_1)),
stwo,(id(a_1,a_2),(hash((wrap(a_7),wrap(hash((
wrap(method_three),(wrap(a_4),(wrap(exp(g,X_1)),
(wrap(a_5),a_6)))))))),(a_2,a_9))),hash_length),
a_9))),a_2))),(exp(g,ltdh_1),EAD_1))),hash_length),
EAD_1)),exp(g,ltdh_1)))),hash_length),X_1,a_7)