A trace has been found.

Honest Process

Attacker

{1}new Alice_3

{2}new Bob_3

{3}let sidAlice_1: bitstring = session(Alice_3)

{5}insert tbl_locks_handle(session(Alice_3),lock_sidAlice_init)

a_11

{4}let sidBob_1: bitstring = session(Bob_3)

{7}insert tbl_locks_handle(session(Bob_3),lock_sidBob_init)

a_12

{9}new RootInit

{10}new EphemeralInit

{12}insert tbl_states_handle(session(Alice_3),stateChannelsidA)

a_13

{11}let CK_1: bitstring = pars1(hkdf(RootInit,EphemeralInit))

{15}insert tbl_states_handle(session(Bob_3),stateChannelsidB)

~M = pars1(hkdf(RootInit,EphemeralInit))

a_10

!

!

!

!

!

Beginning of process NewSession

Beginning of process NewSession

Beginning of process MsgNewSession

Beginning of process MsgNewSession

Beginning of process CompromiseSession(session(Alice_3), session(Bob_3))

Beginning of process SessionCipherEncrypt

Beginning of process SessionCipherEncrypt

Beginning of process SessionCipherDecrypt

Beginning of process SessionCipherDecrypt

Beginning of process NewSession

Beginning of process NewSession

Beginning of process NewSession

Beginning of process MsgNewSession

Beginning of process MsgNewSession

Beginning of process MsgNewSession

Beginning of process CompromiseSession(session(Alice_3), session(Bob_3))

Beginning of process CompromiseSession(session(Alice_3), session(Bob_3))

Beginning of process SessionCipherEncrypt

~M_1 + 1 = a_12 + 1

~M_2 + 1 = a_11 + 1

~M_3 = pars1(hkdf(RootInit,EphemeralInit))

{109}get tbl_locks_handle(session(Alice_3),lock_sidAlice_init)

a_14

{108}get tbl_locks_handle(session(Bob_3),lock_sidBob_init)

a_15

{107}get tbl_states_handle(session(Alice_3),stateChannelsidA)

a_16

~M_4 = a_16

{106}get tbl_states_handle(session(Bob_3),stateChannelsidB)

a_17

{94}let MKa_1: bitstring = hash2(a_16,s1)

~M_5 = a_16

~M_6 = a_17

{103}event eCompromise(session(Alice_3),session(Bob_3))

~M_7 + 1 = a_15 + 1

~M_8 + 1 = a_14 + 1

~M_9 = hash2(a_16,s1)

{95}let MKb_1: bitstring = hash2(a_17,s1)

~M_10 = hash2(a_17,s1)

{98}event eCompromise(session(Alice_3),session(Bob_3)): blocks

~M_11 = a_17

{279}get tbl_locks_handle(session(Alice_3),lock_sidAlice_init)

a_18

{278}get tbl_locks_handle(session(Bob_3),lock_sidBob_init)

a_7

{243}new Root_sy_8

{244}new Ephemeral_sy_8

{261}new ephemeral_secret_2

a_8

{246}let RKe: bitstring = pars2(hkdf(Root_sy_8,Ephemeral_sy_8))

{262}let CKeNew: bitstring = pars1(hkdf(pars2(hkdf(Root_sy_8,Ephemeral_sy_8)),ephemeral_secret_2))

~M_12 = pars1(hkdf(pars2(hkdf(Root_sy_8,Ephemeral_sy_8)),ephemeral_secret_2))

a_9

{268}event eHeal(session(Alice_3),session(Bob_3))

~M_13 = pars1(hkdf(pars2(hkdf(Root_sy_8,Ephemeral_sy_8)),ephemeral_secret_2))

{140}get tbl_locks_handle(session(Alice_3),lock_sidAlice_init)

a_19

{139}get tbl_states_handle(session(Alice_3),stateChannelsidA)

a_6

{116}new payload_2

{115}let MKs_1: bitstring = hash2(a_6,s1)

{117}let Enc_1: bitstring = enc(payload_2,hash2(a_6,s1))

~M_14 = enc(payload_2,hash2(a_6,s1))

{119}event eSend(session(Alice_3),session(Bob_3),hash2(a_6,s1))

The attacker has the message hash2(a_6,s1)