Abbreviations
~M_5 = AES_CMAC(AES_CMAC(AES_CMAC(AES_CMAC(ZERO, concat(concat(concat(concat(PI,PCap),PS),p256(gen,exp_P_1)),gen)),p256(gen,exp_P_1)),prck),concat(rand_prov_2,auth_val_3))
~M_7 = AES_CCM((ivindex,keys),AES_CMAC(AES_CMAC(AES_CMAC(ZERO,concat(concat(AES_CMAC(ZERO,concat(concat(concat(PI,PCap),PS),p256(gen,exp_P_1)), gen)),rand_prov_2),rand_prov_2)),p256(gen,exp_P_1)), prsk),AES_CMAC(AES_CMAC(AES_CMAC(ZERO,concat(concat(concat(AES_CMAC(ZERO,concat(concat(concat(PI,PCap), PS),p256(gen,exp_P_1)),gen)),rand_prov_2),rand_prov_2)), p256(gen,exp_P_1)),prsn))

A trace has been found.

Honest Process

{1}new exp_P_1
{2}new exp_D_1

Attacker

Beginning of process invite_prov

{7}insert pi_table_prov(addr_dev,PI)
{8}insert pcap_table_prov(addr_dev,a)

Beginning of process invite_dev

{11}insert pi_table_dev(addr_prov,a_1)
{12}insert pcap_table_dev(addr_prov,PCap)

Beginning of process pubkey_exchange_noob_prov

{21}get pcap_table_prov(addr_dev,a)

{18}insert pubkey_table_prov(addr_prov,p256(gen, exp_P_1))
{19}insert pubkey_table_prov(addr_dev,gen)
{20}insert dhkey_table_prov(addr_prov,p256(gen, exp_P_1))

Beginning of process pubkey_exchange_noob_dev

{30}get pi_table_dev(addr_prov,a_1)

{27}insert pubkey_table_dev(addr_prov,a_3)
{28}insert pubkey_table_dev(addr_dev,p256(gen, exp_D_1))
{29}insert dhkey_table_dev(addr_dev,p256(a_3,exp_D_1))

Beginning of process auth_outputoob_prov

{57}get pubkey_table_prov(addr_prov,p256(gen,exp_P_1))
{56}get pubkey_table_prov(addr_dev,gen)
{55}get dhkey_table_prov(addr_prov,p256(gen,exp_P_1))
{31}new rand_prov_2

Beginning of process auth_outputoob_dev

{87}get pubkey_table_dev(addr_prov,a_3)
{86}get pubkey_table_dev(addr_dev,p256(gen,exp_D_1))
{85}get dhkey_table_dev(addr_dev,p256(a_3,exp_D_1))
{58}new rand_dev_2
{59}new auth_val_3

Beginning of process send_data_prov

{42}event send_prov(p256(gen,exp_P_1))

Beginning of process recv_data_dev

{46}event recv_prov(p256(gen,exp_P_1))
{51}insert key_table_prov(addr_dev,AES_CMAC(AES_CMAC(AES_CMAC(ZERO,concat(concat(AES_CMAC(ZERO,concat(concat(concat(concat(PI,PCap),PS),p256(gen,exp_P_1)),gen)),rand_prov_2),rand_prov_2)),p256(gen,exp_P_1)),prsk))
{54}insert nonce_table_prov(addr_dev,AES_CMAC(AES_CMAC(AES_CMAC(ZERO,concat(concat(AES_CMAC(ZERO,concat(concat(concat(concat(PI,PCap),PS),p256(gen,exp_P_1)),gen)),rand_prov_2),rand_prov_2)),p256(gen,exp_P_1)),prsn))

{95}get key_table_prov(addr_dev,AES_CMAC(AES_CMAC(AES_CMAC(ZERO,concat(concat(AES_CMAC(ZERO,concat(concat(concat(concat(PI,PCap),PS),p256(gen,exp_P_1)),gen)),rand_prov_2),rand_prov_2)),p256(gen,exp_P_1)),prsk))
{94}get nonce_table_prov(addr_dev,AES_CMAC(AES_CMAC(AES_CMAC(ZERO,concat(concat(AES_CMAC(ZERO,concat(concat(concat(concat(PI,PCap),PS),p256(gen,exp_P_1)),gen)),rand_prov_2),rand_prov_2)),p256(gen,exp_P_1)),prsn))

Beginning of process outputoob_user

Beginning of process Mesh_stack_central

Beginning of process Mesh_stack_peripheral

Beginning of process Meshapp_central
{176}new seq1_4
{177}insert mesh_seq_c(addr_prov,seq1_4)

Beginning of process Meshapp_peripheral

~M = PI
a
a_1
~M_1 = PCap
~M_2 = PS
~M_3 = p256(gen,exp_P_1)
gen
a_2
a_3
~M_4 = p256(gen,exp_D_1)
auth_val_3
auth_val_3
~M_5
~M_5
~M_6 = rand_prov_2
~M_6 = rand_prov_2
~M_7

The attacker has the message 2-proj-2-tuple(sdec(~M_7,AES_CMAC(AES_CMAC(ZERO,concat(concat(AES_CMAC(ZERO,concat(concat(concat(concat(~M,~M_1),~M_2),~M_3),gen)),~M_6),~M_3),prsk),AES_CMAC(AES_CMAC(AES_CMAC(ZERO,concat(concat(AES_CMAC(ZERO,concat(concat(concat(concat(~M,~M_1),~M_2),~M_3),gen)),~M_6),~M_3),prsn))) = keys