Abbreviations
~X_1 = AES_CMAC(AES_CMAC(AES_CMAC(AES_CMAC(ZERO,concat(concat(concat(concat(~M,~M_1),~M_2),gen),~M_4)),~M_4),prck),concat(a_3,zero)) = AES_CMAC(AES_CMAC(AES_CMAC(AES_CMAC(ZERO,concat(concat(concat(concat(PI,PCap),PS),gen),p256(gen,exp_D_1))),p256(gen,exp_D_1)),prck),concat(a_3,zero))
~M_5 = AES_CMAC(AES_CMAC(AES_CMAC(AES_CMAC(ZERO,concat(concat(concat(concat(PI,PCap),PS),gen),p256(gen,exp_D_1))),p256(gen,exp_D_1)),prck),concat(rand_dev_2,zero))
~X_2 = AES_CMM((a_4,a_5),AES_CMAC(AES_CMAC(AES_CMAC(ZERO,concat(concat(AES_CMAC(ZERO,concat(concat(concat(concat(~M,~M_1),~M_2),gen),~M_4)),a_3),~M_6)),~M_4),prsk),AES_CMAC(AES_CMAC(AES_CMAC(ZERO,concat(concat(AES_CMAC(ZERO,concat(concat(concat(concat(~M,~M_1),~M_2),gen),~M_4)),a_3),~M_6)),~M_4),prsn)) = AES_CCM((a_4,a_5),AES_CMAC(AES_CMAC(AES_CMAC(ZERO,concat(concat(AES_CMAC(ZERO,concat(concat(concat(PI,PCap),PS),gen),p256(gen,exp_D_1))),a_3),rand_dev_2)),p256(gen,exp_D_1)),prsk),AES_CMAC(AES_CMAC(AES_CMAC(ZERO,concat(concat(AES_CMAC(ZERO,concat(concat(concat(concat(PI,PCap),PS),gen),p256(gen,exp_D_1))),a_3),rand_dev_2)),p256(gen,exp_D_1)),prsn))
~M_7 = AES_CCM(p_complete,AES_CMAC(AES_CMAC(AES_CMAC(ZERO,concat(concat(AES_CMAC(ZERO,concat(concat(concat(concat(PI,PCap),PS),gen),p256(gen,exp_D_1))),a_3),rand_dev_2)),p256(gen,exp_D_1)),prsk),AES_CMAC(AES_CMAC(AES_CMAC(ZERO,concat(concat(AES_CMAC(ZERO,concat(concat(concat(concat(PI,PCap),PS),gen),p256(gen,exp_D_1))),a_3),rand_dev_2)),p256(gen,exp_D_1)),prsn))

A trace has been found.

Honest Process

{1}new exp_P_1
{2}new exp_D_1

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)

Beginning of process pubkey_exchange_noob_dev

{30}get pi_table_dev(addr_prov,a_1)

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

Beginning of process auth_staticoob_prov

Beginning of process auth_staticoob_dev

{84}get pubkey_table_dev(addr_prov,gen)
{83}get pubkey_table_dev(addr_dev,p256(gen,exp_D_1))
{82}get dhkey_table_dev(addr_dev,p256(gen,exp_D_1))
{59}new rand_dev_2

{71}event recv_dev(p256(gen,exp_D_1))
{72}event send_dev(p256(gen,exp_D_1))

{78}insert key_table_dev(addr_prov,AES_CMAC(AES_CMAC(AES_CMAC(ZERO,concat(concat(AES_CMAC(ZERO,concat(concat(concat(concat(PI,PCap),PS),gen),p256(gen,exp_D_1))),a_3),rand_dev_2)),p256(gen,exp_D_1)),prsk))
{81}insert nonce_table_dev(addr_prov,AES_CMAC(AES_CMAC(AES_CMAC(ZERO,concat(concat(AES_CMAC(ZERO,concat(concat(concat(concat(PI,PCap),PS),gen),p256(gen,exp_D_1))),a_3),rand_dev_2)),p256(gen,exp_D_1)),prsn))

Beginning of process send_data_prov

Beginning of process recv_data_dev

{100}get key_table_dev(addr_prov,AES_CMAC(AES_CMAC(AES_CMAC(ZERO,concat(concat(AES_CMAC(ZERO,concat(concat(concat(concat(PI,PCap),PS),gen),p256(gen,exp_D_1))),a_3),rand_dev_2)),p256(gen,exp_D_1)),prsk))
{99}get nonce_table_dev(addr_prov,AES_CMAC(AES_CMAC(AES_CMAC(ZERO,concat(concat(AES_CMAC(ZERO,concat(concat(concat(concat(PI,PCap),PS),gen),p256(gen,exp_D_1))),a_3),rand_dev_2)),p256(gen,exp_D_1)),prsn))

{95}insert mesh_net_key_p(addr_dev,get_net_key(a_5))
{96}insert mesh_app_key_p(addr_dev,get_app_key(a_5))
{97}insert mesh_iv_p(addr_dev,a_4)

Beginning of process Mesh_stack_central

Beginning of process Mesh_stack_peripheral

Beginning of process Meshapp_central

{171}new seq1_4
{172}insert mesh_seq_c(addr_prov,seq1_4)

Beginning of process Meshapp_peripheral

Attacker

~M = PI
a
a_1
~M_1 = PCap
~M_2 = PS
~M_3 = p256(gen,exp_P_1)
a_2
gen
~M_4 = p256(gen,exp_D_1)
~X_1
~M_5
a_3
~M_6 = rand_dev_2
~X_2
~M_7

The attacker has the message sdec(~M_7,AES_CMAC(AES_CMAC(AES_CMAC(ZERO,concat(concat(AES_CMAC(ZERO,concat(concat(concat(concat(~M,~M_1),~M_2),gen),~M_4)),a_3),~M_6)),~M_4),prsk),AES_CMAC(AES_CMAC(AES_CMAC(ZERO,concat(concat(AES_CMAC(ZERO,concat(concat(concat(concat(~M,~M_1),~M_2),gen),~M_4)),a_3),~M_6)),~M_4),prsn)) = p_complete