Abbreviations
~M_4 = 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,static_oobdata))
~M_6 = AES_CCM(keys,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),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))

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)

{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

Beginning of process auth_staticoob_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))
{32}new rand_prov_2

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

{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))

Beginning of process auth_staticoob_dev

Beginning of process send_data_prov

{89}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))
{88}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 recv_data_dev

Attacker

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

The attacker has the message sdec(~M_6,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_5),~M_5)),~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_5),~M_5)),~M_3),prsn)) = keys