| 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,auth_val_3)) |
| ~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_inputoob_prov

{60}get pubkey_table_prov(addr_prov,p256(gen,exp_P_1))
{59}get pubkey_table_prov(addr_dev,gen)
{58}get dhkey_table_prov(addr_prov,p256(gen,exp_P_1))
{31}new rand_prov_2
{32}new auth_val_3

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

{49}event recv_prov(p256(gen,exp_P_1))
{54}insert key_table_prov(addr_dev,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))
{57}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_inputoob_dev

{92}get key_table_prov(addr_dev,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))
{91}get nonce_table_prov(addr_dev,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)),prsn))

Beginning of process send_data_prov

Beginning of process recv_data_dev

Beginning of process inputoob_user

Attacker

~M = PI
a
a_1
~M_1 = PCap
~M_2 = PS
~M_3 = p256(gen,exp_P_1)
gen
auth_val_3
~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