Abbreviations
~M_4 = AES_CMAC(AES_CMAC(AES_CMAC(AES_CMAC(ZERO, concat(concat(concat(concat(PI,PCap),PS),p256(gen,exp_P_1)),p256(gen,exp_D_1))),p256(p256(gen,exp_P_1),exp_D_1)),prck),concat(rand_prov_2,static_oobdata))

A trace has been found.

Honest Process

Attacker

{1}new exp_P_1
{2}new exp_D_1

Beginning of process invite_prov
Beginning of process invite_dev
Beginning of process pubkey_exchange_oob_prov
Beginning of process pubkey_exchange_oob_dev
Beginning of process auth_staticoob_prov
Beginning of process auth_staticoob_dev
Beginning of process send_data_prov
Beginning of process recv_data_dev

~M = PI

a

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

a_1

~M_1 = PCap

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

{21}get pcap_table_prov(addr_dev,a)

~M_2 = PS

{30}get pi_table_dev(addr_prov,a_1)

a_2

p256(gen,exp_D_1)

~M_3 = p256(gen,exp_P_1)

{18}insert pubkey_table_prov(addr_prov,p256(gen,exp_P_1))
{19}insert pubkey_table_prov(addr_dev,p256(gen,exp_D_1))
{20}insert dhkey_table_prov(addr_prov,p256(p256(gen,exp_D_1),exp_P_1))

{57}get pubkey_table_prov(addr_prov,p256(gen,exp_P_1))
{56}get pubkey_table_prov(addr_dev,p256(gen,exp_D_1))
{55}get dhkey_table_prov(addr_prov,p256(p256(gen,exp_P_1),exp_D_1))
{32}new rand_prov_2

~M_4

~M_4

{42}event send_prov(p256(p256(gen,exp_P_1),exp_D_1))

~M_5 = rand_prov_2

~M_5 = rand_prov_2

{46}event recv_prov(p256(p256(gen,exp_P_1),exp_D_1))