A trace has been found.

Abbreviations

~M_5 = AES_CMAC(AES_CMAC(AES_CMAC(AES_CMAC(ZERO, concat(concat(concat(concat(PI,PCap),PS),p256(gen,exp_P_1)),prck),concat(rand_prov_2,auth_val_3))

~M_7 = AES_CCM(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(AES_CMAC(ZERO,concat(concat(Concat(Concat(Concat(Concat(Concat(PI,PCap), PS),p256(gen,exp_P_1)), gen)),rand_prov_2),rand_prov_2)), p256(gen,exp_P_1)),gen)),rand_prov_2),rand_prov_2)), p256(gen,exp_P_1)),prsn))

Attacker

	$\begin{array}{c} \{1\} \underset{\text{new exp_P_1}}{\text{new exp_P_1}} \\ \{2\} \underset{\text{new exp_D_1}}{\text{new exp_D_1}} \end{array}$	
principal of process invite provide Deginning of process invite day. Deginning of process publical evaluations and process invites day.	Paginning of process publicut evaluation pack day. Deginning of process outh outputs of process outh outputs of day. Deginning of process	as sand data provide Deginning of process restricted data day. Deginning of process systems as a second
eginning of process invite_prov Beginning of process invite_dev Beginning of process pubkey_exchange_noob_	Prov Beginning of process pubkey_exchange_noob_dev Beginning of process auth_outputoob_prov Beginning of process auth_outputoob_prov Beginning of process auth_outputoob_dev Beginning of process auth_outputoob_dev Beginning of process auth_outputoob_not beginning of process auth_outputoob_dev Beginning of process auth_outputoob_not beginning of process auth_outputoob_dev Beginning of process auth_outputoob_dev Beginning of process auth_outputoob_not beginning of process auth_outputoob_dev Beginning of process auth_outputo	Beginning of process recv_data_dev Beginning of process outputoob_user
	\sim M = PI	
nsert pi_table_prov(addr_dev,PI) nsert pcap_table_prov(addr_dev,a)		
	a_1	
	\sim 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)		
	\sim M_2 = PS	
	$\sim M_3 = p256(gen, exp_P_1)$	
	gen	
{18}insert pubkey_table_prov(addr_prov,p256((gen,	
{19}insert pubkey_table_prov(addr_dev,ger {20}insert dhkey_table_prov(addr_prov,p256(gen))	gen,	
$\frac{\exp_P_1)}{ }$	{30}get pi_table_dev(addr_prov,a_1)	
	a_2	
	$\frac{a_3}{MA - n^2 E G(mon, orm, D, 1)}$	
	$\sim M_4 = p256(gen, exp_D_1)$	
	{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))	
	\[\frac{57}{\text{get pubkey_table_prov(addr_prov,p256(gen,exp_P_1))}}{\frac{56}{\text{get pubkey_table_prov(addr_dev,gen)}}{\frac{55}{\text{get dhkey_table_prov(addr_prov,p256(gen,exp_P_1))}}{\frac{31}{\text{new rand_prov_2}}} \]	
	{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	
		auth_val_3
	auth_val_	3
		~M_5
		~M_5
	[42] event send_prov(p256(gen,exp_P_1))	
		6 = rand prov 2
	~M	6 = rand prov 2
	{46} event recy 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(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))	
	Pron()	
	{54} insert 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))	
		dev,AES_CMAC(AES_CMAC(Cat(AES_CMAC(ZERO,concat(Cat(AES_CMAC(ZERO,CONCAT(Cat(AES_CMAC(Cat(AES_CMAC(ZERO,CONCAT(Cat(AES_CMAC(ZERO,CONCAT(Cat(AES_CMAC(ZERO,CONCAT(Cat(AES_CMAC(ZERO,CONCAT(Cat(AES_CMAC(ZERO,CONCAT(Cat(AES_CMAC(ZERO,CONCAT(Cat(AES_CMAC(ZERO,CONCAT(Cat(AES_CMAC(
	{92}get key table_prov(addr_AES_CMAC(ZERO,concat(concat(concat(concat(concat(concat(concat(concat(concat(prov_2),rand_prov_2),rand_prov_2),rand_prov_2),rand_prov_s	r dev.AES CMAC(AES CMAC(
	AES_CMAC(ZERO,concat(concat(PI,PCa concat(concat(concat(PI,PCa gen)),rand_prov_2),rand_pr	r_dev,AES_CMAC(AES_CMAC(cat(AES_CMAC(ZERO,concat(ap),PS),p256(gen,exp_P_1)),cov_2)),p256(gen,exp_P_1)),
	prs	11 <i>)</i>
		~M_7

Honest Process