A trace has been found.

Abbreviations
~M_8135 = non_confirmable
~M_8136 = CoAP_POSTCode
~M_8137 = messageid_7998
~M_8138 = token_7999
~M_8141 = partial_iv_8000
~M_8142 = IDri_7994
~M_8143 = R1_8001
~M_8140 = aeadEncrypt(HKDF(msecret_7995,msalt_7996, (IDri_7994,R1_8001,AES_CCM,label_key),alg_key_length(AES_CCM,label_key)),aeadNonce(IDri_7994,partial_iv_8000, HKDF(msecret_7995,msalt_7996,(emptyId,R1_8001, AES_CCM,label_iv),alg_key_length(AES_CCM,label_iv))), CoAP_CONTEXTCode,(encrypt0,oscore_version_one, AES_CCM,IDri_7994,partial_iv_8000))
~X_1 = (a_7987,a_7988,a_7989,a_7990,(~M_8141,~M_8057, ~M_8143),~M_8140) = (a_7987,a_7988,a_7989,a_7990, (partial_iv_8000,IDri_7994,R1_8001),aeadEncrypt(HKDF(msecret_7995,msalt_7996,(IDri_7994,R1_8001, AES_CCM,label_key),alg_key_length(AES_CCM,label_key)), aeadNonce(IDri_7994,partial_iv_8000,HKDF(msecret_7995, msalt_7996,(emptyId,R1_8001,AES_CCM,label_iv), alg_key_length(AES_CCM,label_iv))),CoAP_CONTEXTCode, (encrypt0,oscore_version_one,AES_CCM,IDri_7994, partial_iv_8000)))
~M_8299 = non_confirmable
~M_8300 = CoAP_POSTCode
~M_8301 = responseID_8286
~M_8302 = a_7990
~M_8303 = aeadEncrypt(HKDF(msecret_7995,msalt_7996, (IDir_7993,R1_8001,AES_CCM,label_key),alg_key_length(AES_CCM,label_key)),aeadNonce(IDri_7994,partial_iv_8000, HKDF(msecret_7995,msalt_7996,(emptyId,R1_8001, AES_CCM,label_iv),alg_key_length(AES_CCM,label_iv))), CoAP_CONTEXTCode,(encrypt0,oscore_version_one, AES_CCM,IDri_7994,partial_iv_8000))

Honest Process

Attacker

!

{12}new initiator_7992
{13}new responder_7991

Beginning of process init_keys

~M_8042 = initiator_7992

~M_8044 = responder_7991

Beginning of process step_1(initiator_7992, responder_7991)
{16}new token_7999
{17}new messageid_7998
{18}new partial_iv_8000
{19}new R1_8001

Beginning of process step_2(responder_7991)

Beginning of process step_3(initiator_7992, responder_7991)

Beginning of process step_4(responder_7991)

Beginning of process step_5(initiator_7992, responder_7991)

~M_8044 = responder_7991

~M_8042 = initiator_7992

{4}new IDir_7993
{5}new IDri_7994
{6}new msecret_7995
{7}new msalt_7996
{8}new idcontext_7997

(~M_8056,~M_8057,~M_8058) = (IDir_7993,IDri_7994, idcontext_7997)

{10}insert security_context_lookup(responder_7991, initiator_7992,IDir_7993,IDri_7994,msecret_7995, msalt_7996,idcontext_7997)

{11}insert security_context_lookup(initiator_7992, responder_7991,IDri_7994,IDir_7993,msecret_7995, msalt_7996,idcontext_7997)

{34}get security_context_lookup(initiator_7992, responder_7991,IDri_7994,IDir_7993,msecret_7995, msalt_7996,idcontext_7997)

{30}insert token_to_message_lookup(initiator_7992, token_7999,(responder_7991,IDri_7994,IDir_7993, R1_8001,partial_iv_8000,aeadNonce(IDri_7994,partial_iv_8000, HKDF(msecret_7995,msalt_7996,(emptyId,R1_8001, AES_CCM,label_iv),alg_key_length(AES_CCM,label_iv)))))

{32}insert step_1_context(initiator_7992,responder_7991, R1_8001)

(~M_8135,~M_8136,~M_8137,~M_8138,(~M_8141,~M_8142, ~M_8143),~M_8140)

~X_1

{108}get security_context_lookup(responder_7991, initiator_7992,IDir_7993,IDri_7994,msecret_7995, msalt_7996,idcontext_7997)

{99}insert new_security_context_lookup(responder_7991, initiator_7992,IDir_7993,IDri_7994,msecret_7995, msalt_7996,R1_8001)

{100}new responseID_8286

(~M_8299,~M_8300,~M_8301,~M_8302,~M_8303)

{107}event here