Abbreviations \sim M_59197 = coap_version_one \sim M 59198 = non confirmable \sim M 59199 = bounded by(token 58527) \sim M 59200 = CoAP POSTCode ~M 59201 = messageid 58528 \sim M 59202 = token 58527 \sim M_59205 = partial_iv_58518 \sim M 59206 = IDri 58514 \sim M 59207 = idcontext 58517 IDri_58514,partial_iv_58518)) partial iv 58518))) partial_iv_58518))) \sim M 60400 = coap version one \sim M 60401 = non confirmable \sim M 60402 = bounded by(a 58509) \sim M 60403 = CoAP CHANGEDCode \sim M 60404 = responseId 60387 \sim M 60405 = a 58509 \sim M 60406 = empty partial_iv_58518)) Attacker Beginning of process oscore_responder (initiator, a_58512) $(\sim M_59293, \sim M_59294, \sim M_59295, \sim M_59296) = (coap_version_one,$ acknowledgement, CoAP | EMPTYCode, a 58508) (initiator, a 58512) ~X 2 $(\sim M_60121, \sim M_60122, \sim M_60123, \sim M_60124) = (coap_version_one, coap_version_one, coap_version_one$ acknowledgement, CoAP EMPTYCode, a 58\$08) {70} get security_context_lookup(initiator,responder, IDir 58513, IDri 58514, msecret 58515, msalt 58516, idcontext 58517) {69} get replay_window(=initiator,partial_60345: bitstring) suchthat (partial_60345 = partial_iv_58518): else branch taken {59} insert replay_window(initiator,partial_iv_58518) {60}new msg2id_60386 {61}new responseId_60387 {67} event endResponder(responder,initiator,(CoAP_GETCode, isLightBulbTurnedOn)) $(\sim M_60400, \sim M_60401, \sim M_60402, \sim M_60403, \sim M_60404,$ ~M 60405,~M 60406,~M 60407)

~M_59204 = aeadEncrypt(HKDF(msecret_58515,msalt_58516, (IDri_58514,idcontext_58517,AES_CCM,label_key), alg_key_length(AES_CCM,label_key)),aeadNonce(IDri_58514, partial iv 58518,HKDF(msecret 58515,msalt_58516, (emptyId,idcontext_58517,AES_CCM,label_iv),alg_key_length(AES_CCM,label_iv))),((CoAP_GETCode,isLightBulbTurnedOn), msg1id_58529),(encrypt0,oscore_version_one,AES_CCM, \sim X_1 = (coap_version_one,confirmable,a_58506,a_58507, a_58508,a_58509,(~M_59205,~M_59206,~M_59207),~M_59204) (coap version one, confirmable, a 58506, a 58507, a_58508,a_58509,(partial_iv_58518,IDri_58514,idcontext_58517), aeadEncrypt(HKDF(msecret_58515,msalt_58516,(IDri_58514, idcontext 58517,AES CCM,label key),alg key length(AES CCM, label key), aeadNonce(IDri 58514, partial iv 58518, HKDF(msecret 58515,msalt 58516,(emptyId,idcontext 58517, AES CCM, label iv), alg key length(AES CCM, label iv))), ((CoAP_GETCode,isLightBulbTurnedOn),msg1id 58529), (encrypt0,oscore version one,AES CCM,IDri 58514, \sim X 2 = (coap version one, confirmable, a 58506, a 58507, a 58508,a 58509,(~M 59205,~M 59206,~M_59207),~M_59204) (coap version one, confirmable, a 58506, a 58507, a 58508,a 58509,(partial iv 58518,IDri 58514,idcontext 58517), aeadEncrypt(HKDF(msecret 58515,msalt 58516,(IDri 58514, idcontext 58517,AES_CCM,label_key),alg_key_length(AES CCM, label key)), aeadNonce(IDri 58514, partial iv 58518, HKDF(msecret 58515,msalt 58516,(emptyId,idcontext_58517, AES_CCM,label_iv),alg_key_length(AES_CCM,label_iv))),

A trace has been found.

((CoAP_GETCode,isLightBulbTurnedOn),msg1id 58529), (encrypt0,oscore_version one,AES CCM,IDri 58514,

 \sim M_60407 = aeadEncrypt(HKDF(msecret_58515,msalt_58516, (IDir 58513,idcontext 58517,AES CCM,label key), alg key length(AES CCM,label key)),aeadNonce(IDri 58514, partial iv 58518,HKDF(msecret 58515,msalt 58516, (emptyId,idcontext 58517,AES CCM,label iv),alg key length(AES CCM, label iv))),((CoAP CONTENTCode, bounded by((CoAP GETCode, is LightBulbTurnedOn))), msg2id 60386), (encrypt0,oscore_version_one,AES_CCM,IDri_58514,

{67} event endResponder(responder,initiator,(CoAP_GETCode, isLightBulbTurnedOn))

{59} insert replay_window(initiator,partial_iv_58518)

{60}new msg2id 58940

{61}new responseId_58941

Honest Process

{1}new IDir 58513

{2}new IDri_58514

{3}new msecret 58515

{4}new msalt 58516

{5} new idcontext_58517

{6} insert security_context_lookup(initiator,responder,

IDir_58513,IDri_58514,msecret_58515,msalt_58516,

idcontext $585\overline{17}$)

{7} insert security_context_lookup(responder,initiator,

IDri_58514,IDir_58513,msecret_58515,msalt_58516, idcontext_58517)

(responder,a_58510)

initiator

(~M_59197,~M_59198,~M_59199,~M_59200,~M_59201,

~M 59202,(~M |59205,~M 59206,~M 59207),~M 59204)

{70} get security_context_lookup(initiator,responder,

IDir_58513,IDri_58514,msecret_58515,msalt_58516,

idcontext $585\overline{17}$)

{69} get replay_window(=initiator,partial_59388:

bitstring) suchthat (partial_59388 = partial_iv_58518):

else branch taken

 $\sim X \mid 1$

Beginning of process oscore_responder

Beginning of process oscore_initiator

{11} new token_58527

{12}new messageid_58528

{13}new partial_iv_58518

{30} get security_context_lookup(responder,initiator,

IDri_58514,IDir_58513,msecret_58515,msalt_58516,

idcontext $585\overline{17}$)

{21}new msg1id_58529

{27} insert token_to_message_lookup(responder,token_58527, (initiator,IDri_58514,IDir_58513,idcontext_58517,

partial iv 58518, aeadNonce(IDri 58514, partial iv 58518,

HKDF(msecret_58515,msalt_58516,(emptyld,idcontext_58517, AES_CCM,label_iv),alg_key_length(AES_CCM,label_iv)))))

{28} event startInitiator(responder,initiator,(

CoAP_GETCode, is LightBulbTurnedOn))