Abbreviations \sim M_45235 = coap_version_one \sim M_45236 = non_confirmable \sim M_45237 = bounded_by(token_44938) \sim M_45238 = CoAP_POSTCode \sim M_45239 = messageid_44939 \sim M_45240 = token_44938 \sim M_45243 = partial_iv_44940 \sim M_45244 = IDir_44902 \sim M_45245 = idcontext_44904 ~M_45242 = aeadEncrypt(HKDF(msecret_44906,msalt_44907, (IDir_44902,idcontext_44904,AES_CCM,label_key), alg_key_length(AES_CCM,label_key)),aeadNonce(IDir_44902, partial_iv_44940,HKDF(msecret_44906,msalt_44907, (emptyId,idcontext_44904,AES_CCM,label_iv),alg_key_length(AES_CCM,label_iv))),((CoAP_GETCode,isLightBulbTurnedOn), msg1id_44941),(encrypt0,oscore_version_one,AES_CCM, IDir_44902,partial_iv_44940)) \sim M_45370 = coap_version_one \sim M_45371 = non_confirmable \sim M_45372 = bounded_by(token_44958) \sim M_45373 = CoAP_POSTCode \sim M_45374 = messageid_44959 \sim M_45375 = token_44958 \sim M_45378 = partial_iv_44960 \sim M 45379 = IDir 44902 \sim M_45380 = idcontext_44904 \sim M_45377 = aeadEncrypt(HKDF(msecret_44906,msalt_44907, [IDir_44902,idcontext_44904,AES_CCM,label_key), alg_key_length(AES_CCM,label_key)),aeadNonce(IDir_44902, partial_iv_44960,HKDF(msecret_44906,msalt_44907, (emptyId,idcontext_44904,AES_CCM,label_iv),alg_key_length(AES_CCM,label_iv))),((CoAP_GETCode,isLightBulbTurnedOn), msg1id_44961),(encrypt0,oscore_version_one,AES_CCM, IDir_44902,partial_iv_44960)) \sim M_45505 = coap_version_one \sim M_45506 = non_confirmable \sim M_45507 = bounded_by(token_44901) \sim M_45508 = CoAP_POSTCode \sim M_45509 = messageid_44908 \sim M_45510 = token_44901 \sim M_45513 = partial_iv_44905 \sim M 45514 = IDir 44902 \sim M_45515 = idcontext_44904 ~M_45512 = aeadEncrypt(HKDF(msecret_44906,msalt_44907, [IDir_44902,idcontext_44904,AES_CCM,label_key), alg_key_length(AES_CCM,label_key)),aeadNonce(IDir_44902, partial_iv_44905,HKDF(msecret_44906,msalt_44907, (emptyId,idcontext_44904,AES_CCM,label_iv),alg_key_length(AES CCM, label iv))),((CoAP GETCode, is LightBulbTurnedOn), msg1id_44909),(encrypt0,oscore_version_one,AES_CCM, IDir_44902,partial_iv_44905)) \sim X_1 = (coap_version_one,confirmable,a_44893,a_44892, a_44891,a_44890,(~M_45513,~M_45244,~M_45245),~M_45512) (coap_version_one,confirmable,a_44893,a_44892, a_44891,a_44890,(partial_iv_44905,IDir_44902,idcontext_44904), aeadEncrypt(HKDF(msecret 44906,msalt 44907,(IDir 44902, idcontext_44904,AES_CCM,label_key),alg_key_length(AES_CCM,label_key)),aeadNonce(IDir_44902,partial_iv_44905, HKDF(msecret_44906,msalt_44907,(emptyId,idcontext_44904, AES_CCM,label_iv),alg_key_length(AES_CCM,label_iv))), ((CoAP_GETCode,isLightBulbTurnedOn),msg1id_44909), (encrypt0,oscore_version_one,AES_CCM,IDir_44902, partial_iv_44905))) \sim M_45765 = coap_version_one \sim M_45766 = non confirmable \sim M_45767 = bounded_by(a_44890) \sim M 45768 = CoAP CHANGEDCode \sim M_45769 = responseId 44990 \sim M 45770 = a 44890 \sim M 45771 = empty \sim M_45772 = aeadEncrypt(HKDF(msecret_44906,msalt_44907, (IDri_44903,idcontext_44904,AES_CCM,label_key), alg_key_length(AES_CCM,label_key)),aeadNonce(IDir_44902, partial_iv_44905,HKDF(msecret_44906,msalt_44907, (emptyId,idcontext_44904,AES_CCM,label_iv),alg_key_length(AES_CCM,label_iv))),((CoAP_CONTENTCode,bounded_by((CoAP_GETCode,isLightBulbTurnedOn))),msg2id_44991), (encrypt0,oscore_version_one,AES_CCM,IDir_44902, partial_iv_44905)) \sim X_2 = (coap_version_one,non_confirmable,a_44887,a_44888, a_44889,~M_45510,empty,~M_45772) = (coap_version_one, non_confirmable,a_44887,a_44888,a_44889,token_44901, empty,aeadEncrypt(HKDF(msecret_44906,msalt_44907, (IDri_44903,idcontext_44904,AES_CCM,label_key), alg_key_length(AES_CCM,label_key)),aeadNonce(IDir_44902, partial_iv_44905,HKDF(msecret_44906,msalt_44907, (emptyId,idcontext_44904,AES_CCM,label_iv),alg_key_length(AES_CCM,label_iv))),((CoAP_CONTENTCode,bounded_by((CoAP_GETCode,isLightBulbTurnedOn))),msg2id_44991), (encrypt0,oscore_version_one,AES_CCM,IDir_44902, partial_iv_44905))) Attacker

A trace has been found.

Honest Process {1}new IDir_44902 {2}new IDri_44903 {3}new msecret_44906 {4}new msalt_44907 {5}new idcontext_44904 {6} insert security_context_lookup(initiator,responder, IDir_44902,IDri_44903,msecret_44906,msalt_44907, idcontext_44904) {7} insert security_context_lookup(responder,initiator, IDri_44903,IDir_44902,msecret_44906,msalt_44907, idcontext_44904) Beginning of process oscore_initiator Beginning of process oscore_initiator Beginning of process oscore_initiator Beginning of process oscore_initiator_response_receiver Beginning of process oscore_responder (initiator,a_44896) {11} new token_44938 {12}new messageid_44939 {13}new partial_iv_44940 responder {30} get security_context_lookup(initiator,responder, IDir_44902,IDri_44903,msecret_44906,msalt_44907, idcontext_44904) {21} new msg1id 44941 {27} insert token_to_message_lookup(initiator,token_44938, (responder,IDir_44902,IDri_44903,idcontext_44904, partial_iv_44940,aeadNonce(IDir_44902,partial_iv_44940, HKDF(msecret_44906,msalt_44907,(emptyId,idcontext_44904, AES_CCM,label_iv),alg_key_length(AES_CCM,label_iv))))) {28} event startInitiator(initiator,responder,(CoAP_GETCode, is LightBulbTurnedOn)) (~M_45235,~M_45236,~M_45237,~M_45238,~M_45239, ~M_45240,(~M_45243,~M_45244,~M_45245),~M_45242) (initiator, a 44898) {11} new token_44958 {12}new messageid_44959 {13}new partial_iv_44960 responder {30} get security_context_lookup(initiator,responder, IDir_44902,IDri_44903,msecret_44906,msalt_44907, idcontext_44904) {21}new msg1id_44961 {27} insert token_to_message_lookup(initiator,token_44958, (responder,IDir_44902,IDri_44903,idcontext_44904, partial_iv_44960,aeadNonce(IDir_44902,partial_iv_44960, HKDF(msecret_44906,msalt_44907,(emptyId,idcontext_44904, AES_CCM,label_iv),alg_key_length(AES_CCM,label_iv))))) {28} event startInitiator(initiator, responder, (CoAP_GETCode, is LightBulbTurnedOn)) (~M_45370,~M_45371,~M_45372,~M_45373,~M_45374, ~M 45375,(~M 45378,~M \\delta5379,~M 45380),~M 45377) (initiator,a 44885) {11} new token_44901 {12}new messageid_44908 {13}new partial_iv_44905 responder {30} get security_context_lookup(initiator,responder, IDir_44902,IDri_44903,msecret_44906,msalt_44907, _idcontext_44904) {21}new msg1id_44909 {27} insert token_to_message_lookup(initiator,token_44901, (responder,IDir_44902,IDri_44903,idcontext_44904, partial_iv_44905,aeadNonce(IDir_44902,partial_iv_44905, HKDF(msecret_44906,msalt_44907,(emptyId,idcontext_44904, AES_CCM,label_iv),alg_key_length(AES_CCM,label_iv))))) {28} event startInitiator(initiator,responder,(CoAP GETCode, is LightBulbTurnedOn)) (~M_45\$05,~M_45506,~M_45507,~M_45508,~M_45509, ~M 45510,(~M 45513,~M 45514,~M 45515),~M 45512) initiator (responder,a_44894) $\sim X_1$ $(\sim M_45641, \sim M_45642, \sim M_45643, \sim M_45644) = (coap_version_one,$ acknowledgement, CoAP EMPTYCode, a | 44891) {70} get security_context_lookup(responder,initiator, IDri_44903,IDir_44902,msecret_44906,msalt_44907, idcontext_44904) {69} get replay_window(=responder,partial_45736: bitstring) suchthat (partial_45736 = partial_iv_44905): else branch taken {59} insert replay_window(responder,partial_iv_44905) {60} new msg2id_44991 {61} new responseId_44990 {67} event endResponder(initiator,responder,(CoAP_GETCode, isLightBulbTurnedOn)) (~M_45765,~M_45766,~M_45767,~M_45768,~M_45769, ~M 45770,~M 45771,~M 45772) ~X_2 {44} get token_to_message_lookup(initiator,token_44901, (responder,IDir_44902,IDri_44903,idcontext_44904, partial iv 44905, aeadNonce(IDir 44902, partial iv 44905, HKDF(msecret_44906,msalt_44907,(emptyId,idcontext_44904, AES_CCM,label_iv),alg_key_length(AES_CCM,label_iv))))) {35} event response_binding(token_44901,(responder, IDir_44902,IDri_44903,idcontext_44904,partial_iv_44905, aeadNonce(IDir_44902,partial_iv_44905,HKDF(msecret_44906, msalt_44907,(emptyId,idcontext_44904,AES_CCM,label_iv), alg_key_length(AES_CCM,label_iv))))) {43} get security_context_lookup(initiator,responder,

IDir_44902,IDri_44903,msecret_44906,msalt_44907, idcontext_44904)

{41} event here