\sim M_5362 = aeadEncrypt(HKDF(msecret_4931,msalt_4930, (IDir_4933,idcontext_4929,AES_CCM,label_key),alg_key_length(AES_CCM,label_key)),aeadNonce(IDir_4933,partial_iv_4935, HKDF(msecret_4931,msalt_4930,(emptyId,idcontext_4929, AES_CCM,label_iv),alg_key_length(AES_CCM,label_iv))), ((CoAP_GETCode,isLightBulbTurnedOn),msg_1id_4934), (encrypt0,oscore_version_one,AES_CCM,IDir_4933, partial_iv_4935)) \sim M_5488 = coap_version_one \sim M_5489 = non_confirmable \sim M 5490 = bounded by(token 5000) \sim M 5491 = CoAP POSTCode \sim M_5492 = messageid_5001 \sim M 5493 = token 5000 \sim M 5496 = partial iv 5002 \sim M 5497 = IDir 4933 \sim M 5498 = idcontext 4929 ~M 5495 = aeadEncrypt(HKDF(msecret 4931,msalt 4930, (IDir_4933,idcontext_4929,AES_CCM,label_key),alg_key_length(AES_CCM,label_key)),aeadNonce(IDir_4933,partial_iv_5002, HKDF(msecret 4931,msalt 4930,(emptyId,idcontext 4929, AES_CCM,label_iv),alg_key_length(AES_CCM,label_iv))), ((CoAP GETCode,isLightBulbTurnedOn),msg 1id 5003), (encrypt0,oscore_version_one,AES_CCM,IDir_4933, partial_iv_5002)) Honest Process Attacker {1}new IDir_4933 {2}new IDri 4932 {3}new msecret_4931 {4}new msalt 4930 {5}new idcontext 4929 {6} insert security_context_lookup(initiator,responder, IDir 4933,IDri 4932,msecret 4931,msalt 4930,idcontext 4929) {7} insert security_context_lookup(responder,initiator, IDri_4932,IDir_4933,msecret_4931,msalt_4930,idcontext_4929) Beginning of process oscore initiator(initiator) Beginning of process oscore initiator(initiator) Beginning of process oscore initiator(initiator) {9}new token 5000 {9}new token_4958 {9}new token_4936 {10} new messageid_4959 {10} new messageid_4937 {10} new messageid_5001 {11} new partial_iv_4960 {11} new partial_iv_4935 {11} new partial_iv_5002 responder {32} get security_context_lookup(initiator,responder, IDir_4933,IDri_4932,msecret_4931,msalt_4930,idcontext_4929) {21} new msg_1id_4961 {27} insert token_to_message_lookup(initiator,token_4958, (responder,IDir_4933,IDri_4932,idcontext_4929, partial_iv_4960,aeadNonce(IDir_4933,partial_iv_4960, HKDF(msecret 4931,msalt 4930, emptyld, idcontext 4929, AES_CCM,label_iv),alg_key_length(AES_CCM,label_iv))))) {28} event request_binding(token_4958,(responder, IDir_4933,IDri_4932,idcontext_4929,partial_iv_4960, aeadNonce(IDir_4933,partial_iv_4960,HKDF(msecret_4931, msalt_4930,(emptyId,idcontext_4929,AES_CCM,label_iv), alg_key_length(AES_CCM,label_iv)))) {29} event startInitiator(initiator, responder, ((CoAP GETCode, is Light Bulb Turned On), msg_1id_4961)) {30} event startInit(initiator,responder,(CoAP_GETCode, isLightBulbTurnedOn)) (~M_5222,~M_5223,~M_5224,~M_5225,~M_5226,~M_5227, (~M_5230,~M_5231,~M_5232),~M_5229) responder {32} get security_context_lookup(initiator,responder, IDir_4933,IDri_4932,msecret_4931,msalt_4930,idcontext_4929) {21} new msg_1id_4934 {27} insert token_to_message_lookup(initiator,token_4936, (responder,IDir_4933,IDri_4932,idcontext_4929, partial iv 4935, aeadNonce(IDir 4933, partial iv 4935, HKDF(msecret_4931,msalt_4930,(emptyld,idcontext_4929, AES CCM, label iv), alg key length (AES CCM, label iv))))) {28} event request_binding(token_4936,(responder, IDir_4933,IDri_4932,idcontext_4929,partial_iv_4935, aeadNonce(IDir_4933,partial_iv_4935,HKDF(msecret_4931, msalt_4930,(emptyId,idcontext_4929,AES_CCM,label_iv), alg_key_length(AES_CCM,label_iv)))) {29} event startInitiator(initiator,responder,((CoAP_GETCode,isLightBulbTurnedOn),msg_1id_4934)) {30} event startInit(initiator, responder, (CoAP GETCode, isLightBulbTurnedOn)) (~M_\$355,~M_5356,~M_5357,~M_5358,~M_5359,_M_5360, (~M 5363,~M 5364,~M 5365),~M 5362) responder {32} get security_context_lookup(initiator,responder, | IDir _4933, IDri _4932, msecret _4931, msalt _4930, idcontext _4929) {21}new msg_1id_5003 {27} insert token_to_message_lookup(initiator,token_5000, (responder, IDir_4933, IDri_4932, idcontext_4929, partial iv 5002, aeadNonce(IDir 4933, partial iv 5002, HKDF(msecret 4931,msalt 4930, emptyld, idcontext 4929, AES CCM, label iv), alg key length (AES CCM, label iv))))) {28} event request_binding(token_5000,(responder, IDir 4933, IDri 4932, idcontext 4929, partial iv 5002, aeadNonce(IDir_4933,partial_iv_5002,HKDF(msecret_4931, msalt_4930,(emptyId,idcontext_4929,AES_CCM,label_iv), alg_key_length(AES CCM,label iv)))) {29} event startInitiator(initiator, responder, ((CoAP_GETCode, is LightBulbTurnedOn), msg_1id_5003)) {30} event startInit(initiator,responder,(CoAP_GETCode, isLightBulbTurnedOn)) (~M_5488,~M_5489,~M_5490,~M_5491,~M_5492,~M_5493, (~M_5496,~M_5497,~M_5498),~M_5495) Phase $(\sim M 5501, \sim M 5502) = (msecret 4931, msalt 4930)$

Abbreviations

 \sim M_5222 = coap_version_one

 \sim M 5223 = non confirmable

 \sim M 5224 = bounded by(token 4958)

 \sim M 5225 = CoAP POSTCode

 \sim M 5226 = messageid 4959

 \sim M 5227 = token 4958

 \sim M_5230 = partial_iv_4960

 \sim M 5231 = IDir 4933

 \sim M_5232 = idcontext_4929

~M_5229 = aeadEncrypt(HKDF(msecret_4931,msalt_4930,

(IDir_4933,idcontext_4929,AES_CCM,label_key),alg_key_length(

AES CCM, label key), aeadNonce(IDir 4933, partial iv 4960,

HKDF(msecret_4931,msalt_4930,(emptyId,idcontext_4929,

AES_CCM,label_iv),alg_key_length(AES_CCM,label_iv))),

((CoAP_GETCode,isLightBulbTurnedOn),msg_1id_4961),

(encrypt0,oscore_version_one,AES_CCM,IDir_4933,

partial_iv_4960))

 \sim M_5355 = coap_version_one

 \sim M_5356 = non_confirmable

 \sim M_5357 = bounded_by(token_4936)

 \sim M_5358 = CoAP_POSTCode

 \sim M 5359 = messageid 4937

 \sim M 5360 = token 4936

 \sim M_5363 = partial_iv_4935

 \sim M 5364 = IDir 4933

 \sim M 5365 = idcontext 4929

The attacker has the message 2-proj-2-tuple(decrypt(

~M_5362,HKDF(~M_5501,~M_5502,(~M_5231,~M_5232,

AES_CCM,label_key),alg_key_length(AES_CCM,label_key)),

aeadNonce(~M 5231,~M 5363,HKDF(~M 5501,~M 5502,

(emptyId,~M_5232,AES_CCM,label_iv),alg_key_length(

AES CCM, label iv))))) = msg 1 id 4934 in phase 1

A trace has been found.