Abbreviations
\sim M_21946 = coap_version_one
\sim M_21947 = non_confirmable
~M_21948 = bounded_by(token_21744)
\sim M_21949 = CoAP_POSTCode
~M_21950 = messageid_21745
$\sim M_21951 = token_21744$
$\sim M_21954 = partial_iv_21735$
~M_21955 = IDir_21731
$\sim M_21956 = idcontext_21734$
-M_21953 = aeadEncrypt(HKDF(msecret_21732,msalt_21733,

(IDir 21731,idcontext 21734,AES_CCM,label_key), alg_key_length(AES_CCM,label_key)),aeadNonce(IDir_21731, partial iv 21735,HKDF(msecret 21732,msalt 21733, (emptyId,idcontext_21734,AES_CCM,label_iv),alg_key_length(AES_CCM,label_iv))),((CoAP_GETCode,isLightBulbTurnedOn), msg_1id_21746),(encrypt0,oscore_version_one,AES_CCM, IDir_21731,partial_iv_21735)) \sim X 1 = (coap version one,non confirmable,a 21725,a 21726, a_21727,a_21728,(~M_21954,~M_21955,~M_21956),~M_21953) (coap version one,non confirmable,a 21725,a 21726, a_21727,a_21728,(partial_iv_21735,IDir_21731,idcontext_21734), aeadEncrypt(HKDF(msecret 21732,msalt 21733,(IDir 21731, idcontext 21734,AES CCM,label key),alg key length(AES CCM, label key), aeadNonce(IDir 21731, partial iv 21735, HKDF(msecret 21732,msalt 21733,(emptyId,idcontext 21734, AES CCM, label iv), alg key length (AES CCM, label iv))), ((CoAP GETCode, is LightBulbTurnedOn), msg 1id 21746), (encrypt0,oscore_version one,AES CCM,IDir 21731, partial iv 21735))) Attacker

Honest Process {1}new IDir 21731 {2}new IDri 21730 {3}new msecret 21732 {4}new msalt 21733 {5}new idcontext 21734 {6} insert security context lookup(initiator, responder, | IDir_21731, IDri_21730, msecret_21732, msalt 21733, idcontext 21734) {7} insert security_context_lookup(responder,initiator, | IDri_21730, IDir_21731, msecret_21732, msalt 21733, | idcontext $217\overline{3}4$) Beginning of process oscore_initiator(initiator) {9}new token_21744 Beginning of process oscore responder(responder) {10}new messageid 21745 {11}new partial iv 21735 responder {32} get security_context_lookup(initiator,responder, IDir_21731,IDri_21730,msecret_21732,msalt_21733, idcontext $217\overline{3}4$) {21} new msg_1id_21746 {27} insert token_to_message_lookup(initiator,token_21744, (responder,IDir_21731,IDri_21730,idcontext_21734, partial_iv_21735,aeadNonce(IDir_21731,partial_iv_21735, HKDF(msecret_21732,msalt_21733,(emptyld,idcontext_21734, AES_CCM,label_iv),alg_key_length(AES_CCM,label_iv))))) {28} event request_binding(token_21744,(responder, IDir 21731,IDri 21730,idcontext_21734,partial_iv_21735, aeadNonce(IDir 21731, partial iv 21735, HKDF (msecret 21732, msalt_21733,(emptyId,idcontext_21734,AES_CCM,label_iv), alg key length(AES CCM, label iv))))) {29} event startInitiator(initiator, responder, ((CoAP GETCode, is Light Bulb Turned On), msg 1 id 21746)) {30} event startInit(initiator, responder, (CoAP GETCode, isLightBulbTurnedOn)) (~M_21946,~M_21947,~M_21948,~M_21949,~M_21950, ~M 21951,(~M 21954,~M 21955,~M 21956),~M 21953) $\sim X_1$ {65} get security_context_lookup(responder,initiator, IDri_21730,IDir_21731,msecret_21732,msalt_21733, idcontext 21734) {64} get unique_ivs(partial_22091: bitstring) suchthat (partial_22091 = partial_iv_21735): else branch taken {53} insert unique_ivs(partial_iv_21735) {54} new msg 2id 22101 {55}new responseId 22102 {61} event endResponder(initiator, responder, ((CoAP_GETCode, isLightBulbTurnedOn),msg 1id 21746)) {62} event sendResponder(initiator, responder, bounded by((CoAP GETCode, is LightBulbTurnedOn)))

A trace has been found.