Abbreviations \sim M_112298 = non_confirmable \sim M 112299 = CoAP POSTCode ~M 112300 = messageid 111160 \sim M 112301 = token 111161 \sim M 112304 = partial iv 111159 \sim M_112305 = IDir_111155 \sim M 112306 = idcontext 111158 ~M_112303 = aeadEncrypt(HKDF(msecret_111156,msalt_111157, (IDir_111155,idcontext_111158,AES_CCM,label_key, alg_key_length(AES_CCM,label_key))),aeadNonce(IDir_111155,partial_iv_111159,HKDF(msecret_111156, msalt_111157,(emptyId,idcontext_111158,AES_CCM, label_iv,alg_key_length(AES_CCM,label_iv))),((CoAP_GETCode,isLightBulbTurnedOn),msg1(a_111146, a_111147)),(encrypt0,oscore_version_one,AES_CCM, IDir_111155,partial_iv_111159)) $\sim X_1 = (a_1111149, a_1111150, a_1111151, a_1111152, (\sim M_112304, a_1111151, a_1111152, a_1111152, a_1111151, a_1111152, a_1111151, a_11111151, a_11111151, a_11111151, a_11111151, a_11111151, a_111111111151, a_111111111151, a_1111111151, a_11111111111111, a_1111$ ~M 112099,~M 112101),~M 112303) = (a 111149,a 111150, a_111151,a_111152,(partial_iv_111159,IDir_111155, idcontext 111158),aeadEncrypt(HKDF(msecret 111156, msalt_111157,(IDir_111155,idcontext 111158,AES CCM, label_key,alg_key_length(AES_CCM,label_key))), aeadNonce(IDir_111155,partial_iv_111159,HKDF(msecret_111156, msalt 111157, (emptyId, idcontext 111158, AES CCM, label iv,alg key length(AES_CCM,label_iv))),((CoAP GETCode, is Light Bulb Turned On), msg1(a 111146, a_111147)),(encrypt0,oscore_version_one,AES_CCM, IDir 111155,partial iv 111159))) \sim X 2 = (a 111149,a 111150,a 111151,a 111152,(\sim M 112304, ~M 112099,~M 112101),~M 112303) = (a 111149,a 111150, a_111151,a_111152,(partial_iv_111159,IDir_111155, idcontext_111158),aeadEncrypt(HKDF(msecret_111156, msalt_111157,(IDir_111155,idcontext_111158,AES_CCM, label key, alg key length(AES CCM, label key))), aeadNonce(IDir_111155,partial_iv_111159,HKDF(msecret_111156, msalt_111157,(emptyId,idcontext_111158,AES_CCM, label iv, alg key length(AES CCM, label iv)))),((CoAP GETCode, is LightBulbTurnedOn), msg1(a 111146, a_111147)),(encrypt0,oscore_version_one,AES_CCM, IDir 111155, partial iv 111159))) \sim M 113582 = non confirmable ~M 113583 = CoAP CHANGEDCode \sim M 113584 = responseId 113569 \sim M 113585 = a 111152 \sim M 113586 = empty \sim M_113587 = aeadEncrypt(HKDF(msecret_1111156,msalt_111157, (IDri_111154,idcontext_111158,AES_CCM,label_key, alg_key_length(AES_CCM,label_key))),aeadNonce(IDir_111155,partial_iv_111159,HKDF(msecret_111156, msalt_111157,(emptyId,idcontext_111158,AES_CCM, label_iv,alg_key_length(AES_CCM,label_iv))),((CoAP_CONTENTCode,bounded_by((CoAP_GETCode,isLightBulbTurnedOn))), msg2(a_111147,a_111146)),(encrypt0,oscore_version_one, AES CCM,IDir 111155,partial iv 111159)) Attacker a 111146 a 111147 a 111148

A trace has been found.

Honest Process {4}new IDir_111155 {5}new IDri 111154 {6}new msecret_111156 {7}new msalt 111157 {8} new idcontext_111158 $|(\sim M_112099, \sim M_112100, \sim M_112101) = (IDir_1111155, |$ IDri 111154,idcontext 111158) {10} insert security_context_lookup(a_1111146,a_1111147, IDir_111155,IDri_111154,msecret_1111156,msalt_111157, idcontext_111158) {11} insert security_context_lookup(a_111147,a_111146, IDri_111154, IDir_111155, msecret_111156, msalt_111157, idcontext 111158) Beginning of process oscore_initiator Beginning of process oscore responder Beginning of process oscore_responder a_111146 {20} new token_111161 {21} new messageid_111160 {22} new partial_iv_111159 a 111147 {39} get security_context_lookup(a_111146,a_111147, IDir_111155,IDri_111154,msecret_111156,msalt_111157, idcontext 111158) {34} insert token_to_message_lookup(a_111146,token_111161, (a_111147,IDir_111155,IDri_111154,idcontext_111158, partial_iv_111159,aeadNonce(IDir_111155,partial_iv_111159, HKDF(msecret_111156,msalt_111157,(emptyId,idcontext_111158, AES_CCM, label_iv, alg_key_length(AES_CCM, label_iv)))))) {35} event beginInitiator(a_111146,a_111147,(CoAP_GETCode, isLightBulbTurnedOn)) {37} event integrityReq(CoAP_GETCode,isLightBulbTurnedOn, msg1(a_111146,a_111147)) (~M_112298,~M_112299,~M_112300,~M_112301,(~M_112304, ~M_112305,~M_112306),~M_112303) a_111|147 $\sim X_{\perp}$ {64} get security_context_lookup(a_1111147,a_1111146, IDri_111154,IDir_111155,msecret_1111156,msalt_111157, idcontext 111158) {63} get replay_window(=a_111147,partial_112492: bitstring) suchthat (partial_112492 = partial_iv_111159): else branch taken {52} event integrityReq(CoAP_GETCode,isLightBulbTurnedOn, msg1(a_111146,a_111147)) a 111147 ~X_2 {64} get security_context_lookup(a_111147,a_111146, IDri_111154,IDir_111155,msecret_1111156,msalt_111157, idcontext 111158) {63} get replay_window(=a_111147,partial_113506: bitstring) suchthat (partial_11\overline{3}506 = partial_iv_111159): else branch taken {52} event integrityReq(CoAP GETCode,isLightBulbTurnedOn, msg1(a_111146,a_111147)) {53} insert replay_window(a_111147,partial_iv_111159) {54}new responseId 113569 {60} event endResponder(a 111146,a 111147,(CoAP GETCode, isLightBulbTurnedOn)) {61} event beginResponder(a_111146,a_111147,bounded_by((CoAP_GETCode,isLightBulbTurnedOn))) (~M_113582,~M_113583,~M_113584,~M_113585,~M_113586, ~M 113587) {53} insert replay_window(a_111147,partial_iv_111159) {54}new responseId_111824 {60} event endResponder(a_111146,a_111147,(CoAP_GETCode, isLightBulbTurnedOn))