Abbreviations \sim M_168722 = non_confirmable \sim M_168723 = CoAP_POSTCode \sim M 168724 = messageid 168248 \sim M 168725 = token 168241 \sim M 168728 = partial iv 168245 \sim M 168729 = IDir 168242 \sim M 168730 = idcontext 168244 ~M_168727 = aeadEncrypt(HKDF(msecret_168246,msalt_168247, (IDir_168242,idcontext_168244,AES_CCM,label_key, alg key length(AES CCM,label key))),aeadNonce(IDir 168242, partial iv 168245, HKDF (msecret 168246, msalt_168247,(emptyId,idcontext_168244,AES_CCM, label_iv,alg_key_length(AES_CCM,label_iv))),((CoAP_GETCode,isLightBulbTurnedOn),msg1(a_168230, a_168230)),(encrypt0,oscore_version_one,AES_CCM, IDir 168242, partial iv 168245)) $\sim X_1 = (a_168239, a_168238, a_168237, a_168236, (\sim M_168728, a_168236, a_16826, a_16826, a_16826, a_16826, a_16826, a_16826, a_16826, a_16826, a_16826, a$ ~M 168529,~M 168531),~M 168727) = (a 168239,a 168238, a_168237,a_168236,(partial_iv_168245,IDir_168242, idcontext_168244),aeadEncrypt(HKDF(msecret_168246, msalt_168247,(IDir_168242,idcontext_168244,AES_CCM, label_key,alg_key_length(AES_CCM,label_key))), aeadNonce(IDir_168242,partial_iv_168245,HKDF(msecret 168246, msalt_168247,(emptyId,idcontext_168244,AES_CCM, label iv, alg key length(AES CCM, label iv)))),((CoAP GETCode, is LightBulbTurnedOn), msg1(a_168230, A trace has been found. a_168230)),(encrypt0,oscore_version_one,AES_CCM, IDir 168242, partial iv 168245))) \sim M 168965 = non confirmable ~M 168966 = CoAP CHANGEDCode \sim M_168967 = responseId 168291 \sim M 168968 = a 168236 \sim M 168969 = empty \sim M_168970 = aeadEncrypt(HKDF(msecret_168246,msalt_168247, (IDri 168243,idcontext 168244,AES CCM,label key, alg key length(AES CCM,label key))),aeadNonce(IDir 168242, partial iv 168245, HKDF (msecret 168246, msalt_168247,(emptyId,idcontext_168244,AES CCM, label_iv,alg_key_length(AES_CCM,label iv)))),((CoAP CONTENTCode, bounded by ((CoAP GETCode, is LightBulbTurnedOn))), msg2(a_168230,a_168230)),(encrypt0,oscore_version_one, AES_CCM,IDir_168242,partial_iv_168245)) \sim X_2 = (\sim M_168725,a_168233,a_168234,a_168235,empty, \sim M_168970) (token_168241,a_168233,a_168234,a_168235,empty, aeadEncrypt(HKDF(msecret_168246,msalt_168247,(IDri_168243,idcontext_168244,AES_CCM,label_key, alg_key_length(AES_CCM,label_key))),aeadNonce(IDir_168242,partial_iv_168245,HKDF(msecret_168246, msalt_168247,(emptyId,idcontext_168244,AES_CCM, label iv, alg key length(AES CCM, label iv)))),((CoAP_CONTENTCode,bounded_by((CoAP_GETCode,isLightBulbTurnedOn))),

msg2(a_168230,a_168230)),(encrypt0,oscore_version_one, AES_CCM,IDir_168242,partial_iv_168245))) **Honest Process** Attacker a 168230 a 168230 a 168231 {4}new IDir_168242 {5}new IDri 168243 {6} new msecret_168246 {7}new msalt_168247 {8}new idcontext 168244 $(\sim M_168529, \sim M_168530, \sim M_168531) = (IDir_168242,$ IDri 168243,idcontext 168244) {10} insert security_context_lookup(a_168230,a_168230, IDir_168242,IDri_168243,msecret_168246,msalt_168247, idcontext 168244) {11} insert security_context_lookup(a_168230,a_168230, IDri_168243,IDir_168242,msecret_168246,msalt_168247, idcontext_168244) Beginning of process oscore_initiator Beginning of process oscore responder Beginning of process oscore_initiator_response_receiver a 168230 {20} new token_168241 {21} new messageid_168248 {22} new partial_iv_168245 a 168230 {39} get security_context_lookup(a_168230,a_168230, IDir_168242,IDri_168243,msecret_168246,msalt_168247, idcontext 168244) {34} insert token_to_message_lookup(a_168230,token_168241, (a_168230,IDir_168242,IDri_168243,idcontext_168244, partial_iv_168245,aeadNonce(IDir_168242,partial_iv_168245, HKDF(msecret_168246,msalt_168247,(emptyId,idcontext_168244, AES_CCM,label_iv,alg_key_length(AES_CCM,label_iv)))))) {35} event beginInitiator(a_168230,a_168230,(CoAP_GETCode, isLightBulbTurnedOn)) {37} event integrityReq(CoAP_GETCode,isLightBulbTurnedOn, $msg1(a 168\overline{2}30, a 168230))$ (~M_1687|22,~M_168723,~M_168724,~M_168725,(~M_16\$728, ~M 168729,~M 168730),~M 168727) a 168230 $\sim X_1$ {64} get security_context_lookup(a_168230,a_168230, IDri_168243, IDir_168242, msecret_168246, msalt_168247, idcontext $168\overline{244}$) {63} get replay_window(=a_168230,partial_168916: bitstring) suchthat (partial_168916 = partial_iv_168245): else branch taken {52} event integrityReq(CoAP_GETCode,isLightBulbTurnedOn, msg1(a_168230,a_168230)) {53} insert replay_window(a_168230,partial_iv_168245) {54}new responseId_168291 (60) event endResponder(a_168230,a_168230,(CoAP_GETCode, isLightBulbTurnedOn)) {61} event beginResponder(a_168230,a_168230,bounded_by((CoAP GETCode, is LightBulb TurnedOn))) (~M_168965,~M_168966,~M_168967,_M_168968,~M_168969, ~M_168970) a 168230 ~X_2 [81] get token_to_message_lookup(a_168230,token_168241, a_168230,IDir_168242,IDri_168243,idcontext_168244, partial_iv_168245,aeadNonce(IDir_168242,partial_iv_168245, HKDF(msecret_168246,msalt_168247,(emptyId,idcontext_168244, AES_CCM, label_iv, alg_key_length(AES_CCM, label_iv)))))) {80} get security_context_lookup(a_168230,a_168230, IDir_168242,IDri_168243,msecret_168246,msalt_168247,

{77} event endInitiator(a_168230,a_168230,bounded_by(CoAP_GETCode,isLightBulbTurnedOn)))

idcontext $168\overline{2}44$)

{79} get used tokens(=a 168230,acceptedT 169111:

bitstring) suchthat (acceptedT_169111 = token_168241):

else branch taken

{75} insert used_tokens(a_168230,token_168241)

{76} event match(a_168235,(CoAP_CONTENTCode,bounded by(

(CoAP GETCode, is Light Bulb Turned On))))