Abbreviations \sim M_27096 = coap_version_one \sim M_27097 = non_confirmable \sim M_27098 = bounded_by(token_26750) \sim M_27099 = CoAP_POSTCode \sim M_27100 = messageid_26751 \sim M_27101 = token_26750 \sim M_27104 = partial_iv_26752 \sim M 27105 = IDir 26720 \sim M_27106 = idcontext_26722 ~M_27103 = aeadEncrypt(HKDF(msecret_26719,msalt_26718, (IDir_26720,idcontext_26722,AES_CCM,label_key), alg_key_length(AES_CCM,label_key)),aeadNonce(IDir_26720, partial_iv_26752,HKDF(msecret_26719,msalt_26718, (emptyId,idcontext_26722,AES_CCM,label_iv),alg_key_length(AES_CCM,label_iv))),((CoAP_GETCode,isLightBulbTurnedOn), msg1id_26753),(encrypt0,oscore_version_one,AES_CCM, IDir_26720,partial_iv_26752)) \sim M_27233 = coap_version_one \sim M_27234 = non_confirmable \sim M_27235 = bounded_by(token_26780) \sim M_27236 = CoAP_POSTCode $\sim M_27237 = messageid_26781$ \sim M_27238 = token_26780 \sim M_27241 = partial_iv_26782 \sim M 27242 = IDri 26721 \sim M_27243 = idcontext_26722 ~M_27240 = aeadEncrypt(HKDF(msecret_26719,msalt_26718, (IDri_26721,idcontext_26722,AES_CCM,label_key), alg_key_length(AES_CCM,label_key)),aeadNonce(IDri_26721, partial_iv_26782,HKDF(msecret_26719,msalt_26718, (emptyId,idcontext_26722,AES_CCM,label_iv),alg_key_length(AES_CCM,label_iv))),((CoAP_GETCode,isLightBulbTurnedOn), msglid_26783),(encrypt0,oscore_version_one,AES_CCM, IDri_26721,partial_iv_26782)) \sim M_27370 = coap_version_one \sim M_27371 = non_confirmable \sim M_27372 = bounded_by(token_26726) \sim M_27373 = CoAP_POSTCode \sim M_27374 = messageid_26727 \sim M_27375 = token_26726 \sim M_27378 = partial_iv_26723 \sim M_27379 = IDri_26721 \sim M_27380 = idcontext_26722 \sim M_27377 = aeadEncrypt(HKDF(msecret_26719,msalt_26718, (IDri 26721,idcontext 26722,AES CCM,label key), alg_key_length(AES_CCM,label_key)),aeadNonce(IDri_26721, partial iv 26723,HKDF(msecret 26719,msalt 26718, (emptyId,idcontext 26722,AES CCM,label iv),alg key length(AES CCM, label iv))),((CoAP GETCode, is LightBulbTurnedOn), msg1id_26724),(encrypt0,oscore_version_one,AES_CCM, IDri_26721,partial_iv_26723)) \sim M_27505 = coap_version_one \sim M_27506 = non_confirmable \sim M_27507 = bounded_by(token_26822) \sim M_27508 = CoAP_POSTCode \sim M 27509 = messageid 26823 \sim M 27510 = token 26822 \sim M_27513 = partial_iv_26824 \sim M 27514 = IDir 26720 \sim M_27515 = idcontext_26722 \sim M_27512 = aeadEncrypt(HKDF(msecret_26719,msalt_26718, (IDir_26720,idcontext_26722,AES_CCM,label_key), alg_key_length(AES_CCM,label_key)),aeadNonce(IDir_26720, partial_iv_26824,HKDF(msecret_26719,msalt_26718, (emptyId,idcontext_26722,AES_CCM,label_iv),alg_key_length(AES CCM, label iv))),((CoAP GETCode, is LightBulbTurnedOn), msg1id_26825),(encrypt0,oscore_version_one,AES_CCM, IDir_26720,partial_iv_26824)) $\sim X_1 = (coap_version_one, confirmable, a_26709, a_26708,$ a_26707,a_26706,(~M_27378,~M_27242,~M_27106),~M_27377) (coap_version_one,confirmable,a_26709,a_26708, a_26707,a_26706,(partial_iv_26723,IDri_26721,idcontext_26722), aeadEncrypt(HKDF(msecret 26719,msalt 26718,(IDri 26721, idcontext_26722,AES_CCM,label_key),alg_key_length(AES_CCM,label_key)),aeadNonce(IDri_26721,partial_iv_26723, HKDF(msecret_26719,msalt_26718,(emptyId,idcontext_26722, AES_CCM,label_iv),alg_key_length(AES_CCM,label_iv))), ((CoAP_GETCode,isLightBulbTurnedOn),msg1id_26724), (encrypt0,oscore_version_one,AES_CCM,IDri_26721, __partial_iv_26723))) \sim M_27727 = coap_version_one \sim M_27728 = non_confirmable \sim M_27729 = bounded_by(a_26706) \sim M_27730 = CoAP_CHANGEDCode \sim M_27731 = responseId_26740 \sim M_27732 = a_26706 \sim M_27733 = empty \sim M_27734 = aeadEncrypt(HKDF(msecret_26719,msalt_26718, [IDir_26720,idcontext_26722,AES_CCM,label_key), alg_key_length(AES_CCM,label_key)),aeadNonce(IDri_26721, partial iv 26723, HKDF (msecret 26719, msalt 26718, (emptyId,idcontext_26722,AES_CCM,label_iv),alg_key_length(AES_CCM,label_iv))),((CoAP_CONTENTCode,bounded_by(

(CoAP_GETCode,isLightBulbTurnedOn))),msg2id_26725),

(encrypt0,oscore_version_one,AES_CCM,IDri_26721, partial_iv_26723))

Attacker

A trace has been found.

Honest Process

{1}new IDir_26720 {2}new IDri_26721 {3}new msecret_26719 {4}new msalt_26718 {5}new idcontext_26722 {6} insert security_context_lookup(initiator,responder, IDir_26720,IDri_26721,msecret_26719,msalt_26718, idcontext_26722) {7} insert security_context_lookup(responder,initiator, IDri_26721,IDir_26720,msecret_26719,msalt_26718, idcontext_26722) Beginning of process oscore_initiator Beginning of process oscore_initiator Beginning of process oscore_initiator Beginning of process oscore_initiator Beginning of process oscore_responder (initiator,a 26712) {11}new token_26750 {12} new messageid_26751 {13} new partial_iv_26752 responder {30} get security_context_lookup(initiator,responder, IDir_26720,IDri_26721,msecret_26719,msalt_26718, idcontext_26722) {21} new msg1id_26753 {27} insert token_to_message_lookup(initiator,token_26750, (responder,IDir_26720,IDri_26721,idcontext_26722, partial_iv_26752,aeadNonce(IDir_26720,partial_iv_26752, HKDF(msecret_26719,msalt_26718,(emptyId,idcontext_26722, AES_CCM,label_iv),alg_key_length(AES_CCM,label_iv))))) {28} event startInitiator(initiator,responder,(CoAP_GETCode,isLightBulbTurnedOn)) (~M_27096,_M_27097,~M_27098,~M_27099,~M_27100, ~M_27101,(\dagger/M_27104,~M_27105,~M_27106),~M_27103) (responder,a_26714) {11}new token_26780 {12} new messageid_26781 {13}new partial_iv_26782 initiator {30} get security_context_lookup(responder,initiator, IDri_26721,IDir_26720,msecret_26719,msalt_26718, idcontext_26722) {21} new msg1id_26783 {27} insert token_to_message_lookup(responder,token_26780, (initiator,IDri_26721,IDir_26720,idcontext_26722, partial_iv_26782,aeadNonce(IDri_26721,partial_iv_26782, HKDF(msecret_26719,msalt_26718,(emptyId,idcontext_26722, AES_CCM,label_iv),alg_key_length(AES_CCM,label_iv))))) {28} event startInitiator(responder,initiator,(CoAP_GETCode,isLightBulbTurnedOn)) (~M_27233,~M_27234,~M_27235,~M_27236,~M_27237, ~M_27238,(~M_27241,~M_27242,~M_27243),~M_27240) (responder, a_26704) {11}new token_26726 {12} new messageid_26727 {13}new partial_iv_26723 {30} get security_context_lookup(responder,initiator, IDri_26721,IDir_26720,msecret_26719,msalt_26718, idcontext_26722) {21}new msg1id_26724 {27} insert token_to_message_lookup(responder,token_26726, (initiator,IDri_26721,IDir_26720,idcontext_26722, partial_iv_26723,aeadNonce(IDri_26721,partial_iv_26723, HKDF(msecret_26719,msalt_26718,(emptyId,idcontext_26722, AES_CCM,label_iv),alg_key_length(AES_CCM,label_iv))))) {28} event startInitiator(responder,initiator,(CoAP_GETCode, is Light Bulb Turned On) (~M_27370,~M_27371,~M_27372,~M_27373,~M_27374, ~M_27375,(~M_27378,~M_27379,~M_27380),~M_27377) (initiator,a_26716) {11} new token_26822 {12}new messageid_26823 {13}new partial_iv_26824 responder {30} get security_context_lookup(initiator,responder, IDir_26720,IDri_26721,msecret_26719,msalt_26718, idcontext_26722) {21}new msg1id_26825 {27} insert token_to_message_lookup(initiator,token_26822, (responder,IDir_26720,IDri_26721,idcontext_26722, partial_iv_26824,aeadNonce(IDir_26720,partial_iv_26824, HKDF(msecret_26719,msalt_26718,(emptyId,idcontext_26722, AES_CCM,label_iv),alg_key_length(AES_CCM,label_iv))))) {28} event startInitiator(initiator,responder,(CoAP_GETCode,isLightBulbTurnedOn)) (~M_275\$\$5,~M_27506,~M_27507,~M_27508,↓M_27509, ~M_27510,(~M_27513,~M_27514,~M_27515),~M_27512) (initiator,a 26710) ~X_1 $(\sim M_27601, \sim M_27602, \sim M_27603, \sim M_27604) = (coap_version_one,$ acknowledgement, CoAP_EMPTYCode, a_26707) {70} get security_context_lookup(initiator,responder, IDir_26720,IDri_26721,msecret_26719,msalt_26718, idcontext_26722) {69} get replay_window(=initiator,partial_27696: bitstring) suchthat (partial_27696 = partial_iv_26723): else branch taken {59} insert replay_window(initiator,partial_iv_26723) {60} new msg2id_26725 {61}new responseId_26740 {67} event endResponder(responder,initiator,(CoAP_GETCode, isLightBulbTurnedOn)) (~M_27727,~M_27728,~M_27729,~M_27730,~M_27731, ~M_27|732,~M_27733,~M_27734) Phase 1

The attacker has the message 2-proj-2-tuple(decrypt(~M_27734,HKDF(~M_27737,~M_27738,(~M_27105,~M_27106, AES_CCM,label_key),alg_key_length(AES_CCM,label_key)), aeadNonce(~M_27242,~M_27378,HKDF(~M_27737,~M_27738, (emptyId,~M_27106,AES_CCM,label_iv),alg_key_length(AES_CCM,label_iv))))) = msg2id_26725 in phase 1

 $(\sim M_27737, \sim M_27738) = (msecret_26719, msalt_26718)$