Abbreviations  $\sim$ M\_114865 = non\_confirmable  $\sim$ M 114866 = CoAP POSTCode  $\sim$ M 114867 = messageid 113727  $\sim$ M 114868 = token 113728  $\sim$ M\_114871 = partial iv 113726  $\sim$ M\_114872 = IDri\_113722  $\sim$ M 114873 = idcontext 113725 ~M\_114870 = aeadEncrypt(HKDF(msecret\_113723,msalt\_113724, (IDri\_113722,idcontext\_113725,AES\_CCM,label\_key, alg\_key\_length(AES\_CCM,label\_key))),aeadNonce( IDri\_113722,partial\_iv\_113726,HKDF(msecret\_113723, msalt\_113724,(emptyId,idcontext\_113725,AES\_CCM, label\_iv,alg\_key\_length(AES\_CCM,label\_iv))),( (CoAP\_GETCode,isLightBulbTurnedOn),msg1(a\_113713, a\_113714)),(encrypt0,oscore\_version\_one,AES\_CCM, IDri\_113722,partial\_iv\_113726))  $\sim X_1 = (a_{113716}, a_{113717}, a_{113718}, a_{113719}, (\sim M_{114871}, a_{113718}, a_{113719}, a_{1$ ~M 114667,~M 114668),~M 114870) = (a 113716,a 113717, a 113718,a 113719,(partial iv 113726,IDri 113722, idcontext 113725),aeadEncrypt(HKDF(msecret 113723, msalt 113724,(IDri 113722,idcontext 113725,AES CCM, label\_key,alg\_key\_length(AES\_CCM,label\_key))), aeadNonce(IDri\_113722,partial\_iv\_113726,HKDF(msecret\_113723, msalt 113724,(emptyId,idcontext 113725,AES CCM, label iv, alg key length(AES CCM, label iv)))),( (CoAP GETCode, is Light Bulb Turned On), msg1(a 113713, a\_113714)),(encrypt0,oscore\_version\_one,AES\_CCM, IDri 113722, partial iv 113726)))  $\sim$ X 2 = (a 113716,a 113717,a 113718,a 113719,( $\sim$ M 114871, ~M 114667,~M 114668),~M 114870) = (a 113716,a 113717, a\_113718,a\_113719,(partial\_iv\_113726,IDri\_113722, idcontext\_113725),aeadEncrypt(HKDF(msecret\_113723, msalt\_113724,(IDri\_113722,idcontext\_113725,AES\_CCM, label key, alg key length(AES CCM, label key))), aeadNonce(IDri 113722, partial iv 113726, HKDF (msecret 113723, msalt\_113724,(emptyId,idcontext\_113725,AES\_CCM, label\_iv,alg\_key\_length(AES\_CCM,label\_iv))),( (CoAP\_GETCode,isLightBulbTurnedOn),msg1(a\_113713, a\_113714)),(encrypt0,oscore\_version\_one,AES\_CCM, IDri 113722, partial iv 113726)))  $\sim$ M 116149 = non confirmable  $\sim$ M 116150 = CoAP CHANGEDCode  $\sim$ M 116151 = responseId 116136  $\sim$ M 116152 = a 113719  $\sim$ M 116153 = empty  $\sim$ M\_116154 = aeadEncrypt(HKDF(msecret\_113723,msalt\_113724, (IDir\_113721,idcontext\_113725,AES\_CCM,label\_key, alg key length(AES CCM,label key))),aeadNonce( IDri\_113722,partial\_iv\_113726,HKDF(msecret\_113723, msalt\_113724,(emptyId,idcontext\_113725,AES\_CCM, label\_iv,alg\_key\_length(AES\_CCM,label\_iv))),( (CoAP\_CONTENTCode,bounded\_by((CoAP\_GETCode,isLightBulbTurnedOn))), msg2(a\_113714,a\_113713)),(encrypt0,oscore\_version\_one, AES CCM,IDri 113722,partial iv 113726)) Attacker

**Honest Process** a 113714 a 113713 a 113715 {4}new IDir\_113721 {5}new IDri 113722 {6}new msecret\_113723 {7}new msalt 113724 {8}new idcontext\_113725  $|(\sim M_114666, \sim M_114667, \sim M_114668) = (IDir_113721, |$ IDri 113722,idcontext 113725) {10} insert security\_context\_lookup(a\_113714,a\_113713, IDir\_113721,IDri\_113722,msecret\_113723,msalt\_113724, idcontext\_113725) {11} insert security\_context\_lookup(a\_113713,a\_113714, IDri\_113722,IDir\_113721,msecret\_113723,msalt\_113724, idcontext  $113\overline{7}25$ ) Beginning of process oscore\_initiator Beginning of process oscore\_responder Beginning of process oscore\_responder a 113713 {20} new token\_113728 {21} new messageid\_113727 {22} new partial\_iv\_113726 a 113714 {39} get security\_context\_lookup(a\_113713,a\_113714, IDri\_113722,IDir\_113721,msecret\_113723,msalt\_113724, idcontext  $113\overline{7}25$ ) {34} insert token\_to\_message\_lookup(a\_113713,token\_113728, (a\_113714,IDri\_113722,IDir\_113721,idcontext\_113725, partial\_iv\_113726,aeadNonce(IDri\_113722,partial\_iv\_113726, HKDF(msecret\_113723,msalt\_113724,(emptyId,idcontext\_113725, AES\_CCM, label\_iv, alg\_key\_length(AES\_CCM, label\_iv)))))) {35} event beginInitiator(a 113713,a 113714,(CoAP GETCode, isLightBulbTurnedOn)) {37} event integrityReq(CoAP GETCode,isLightBulbTurnedOn, msg1(a\_113713,a 113714)) (~M\_114865,~M\_114866,~M\_114867,~M\_114868,(~M\_114871, ~M\_114872,~M\_114873),~M\_114870) a\_113|714  $\sim X_{\perp}$ {64} get security\_context\_lookup(a\_113714,a\_113713, IDir\_113721,IDri\_113722,msecret\_113723,msalt\_113724, idcontext 113725) {63} get replay\_window(=a\_113714,partial\_115059: bitstring) suchthat (partial\_115059 = partial\_iv\_113726): else branch taken {52} event integrityReq(CoAP\_GETCode,isLightBulbTurnedOn, msg1(a\_113713,a\_113714)) a 113714 ~X\_2 {64} get security\_context\_lookup(a\_113714,a\_113713, IDir\_113721,IDri\_113722,msecret\_113723,msalt\_113724, idcontext  $113\overline{7}25$ ) {63} get replay\_window(=a\_113714,partial\_116073: bitstring) suchthat (partial\_11\overline{6}073 = partial\_iv\_113726): else branch taken {52} event integrityReq(CoAP GETCode,isLightBulbTurnedOn, msg1(a\_113713,a\_113714)) {53} insert replay\_window(a\_113714,partial\_iv\_113726) {54}new responseId 116136 {60} event endResponder(a 113713,a 113714,(CoAP GETCode, isLightBulbTurnedOn)) {61} event beginResponder(a 113713,a 113714,bounded by( (CoAP\_GETCode,isLightBulbTurnedOn))) (~M\_116149,~M\_116150,~M\_116151,~M\_116152,~M\_116153, ~M 116154) {53} insert replay\_window(a\_113714,partial iv 113726) {54} new responseId\_114391 {60} event endResponder(a\_113713,a\_113714,(CoAP\_GETCode, isLightBulbTurnedOn))

A trace has been found.