Abbreviations  $\sim$ M\_61225 = coap\_version\_one  $\sim$ M\_61226 = non\_confirmable  $\sim$ M 61228 = CoAP POSTCode  $\sim$ M 61229 = messageid 60558  $\sim$ M 61230 = token 60557  $\sim$ M\_61233 = partial\_iv\_60548  $\sim$ M 61234 = IDir 60544  $\sim$ M 61235 = idcontext 60547 IDir\_60544,partial\_iv\_60548)) AES CCM, label iv), alg key length(AES CCM, label iv))), ((CoAP\_GETCode, is LightBulbTurnedOn), msg1id 60559), (encrypt0,oscore\_version\_one,AES\_CCM,IDir 60544, partial iv 60548))) (coap\_version\_one,confirmable,a 60536,a 60537, partial\_iv\_60548)))  $\sim$ M 62436 = coap version one  $\sim$ M 62437 = non confirmable  $\sim$ M 62439 = CoAP CHANGEDCode  $\sim$ M 62440 = responseId 62423  $\sim$ M 62441 = a 60539  $\sim$ M 62442 = empty partial iv 60548)) Attacker Beginning of process oscore\_responder (responder a 60542)  $(\sim M_61323, \sim M_61324, \sim M_61325, \sim M_61326) = (coap_version_one,$ acknowledgement, CoAP | EMPTYCode, a 60538) (responder,a\_60542) ~X 2  $(\sim M_62157, \sim M_62158, \sim M_62159, \sim M_62160) = (coap_version_one, coap_version_one, coap_version_one$ acknowledgement, CoAP EMPTYCode, a 60\$38) {70} get security\_context\_lookup(responder,initiator, IDri 60543, IDir 60544, msecret 60545, msalt 60546, idcontext  $605\overline{47}$ ) {69} get replay\_window(=responder,partial\_62381: bitstring) suchthat (partial\_62381 = partial\_iv\_60548): else branch taken (59) insert replay\_window(responder,partial\_iv\_60548) {60} new msg2id\_62422 {61}new responseId\_62423 {67} event endResponder(initiator, responder, (CoAP\_GETCode, isLightBulbTurnedOn)) (~M\_62436,~M\_62437,~M\_62438,~M\_62439,~M\_62440, ~M\_62441,~M\_62442,~M\_62443)

 $\sim$ M 61227 = bounded by(token 60557) ~M\_61232 = aeadEncrypt(HKDF(msecret\_60545,msalt\_60546, (IDir\_60544,idcontext\_60547,AES\_CCM,label\_key), alg\_key\_length(AES\_CCM,label\_key)),aeadNonce(IDir\_60544, partial iv 60548,HKDF(msecret 60545,msalt 60546, (emptyId,idcontext\_60547,AES\_CCM,label\_iv),alg\_key\_length( AES\_CCM,label\_iv))),((CoAP\_GETCode,isLightBulbTurnedOn), msg1id\_60559),(encrypt0,oscore\_version\_one,AES\_CCM,  $\sim$ X\_1 = (coap\_version\_one,confirmable,a\_60536,a\_60537, a\_60538,a\_60539,(~M\_61233,~M\_61234,~M\_61235),~M\_61232) (coap\_version\_one,confirmable,a\_60536,a\_60537, a\_60538,a\_60539,(partial\_iv\_60548,IDir\_60544,idcontext\_60547), aeadEncrypt(HKDF(msecret\_60545,msalt\_60546,(IDir\_60544, idcontext 60547,AES CCM,label key),alg key length( AES CCM, label key)), aeadNonce(IDir 60544, partial iv 60548, HKDF(msecret 60545,msalt 60546,(emptyId,idcontext 60547,

A trace has been found.

 $\sim$ X 2 = (coap version one, confirmable, a 60536, a 60537, a 60538,a 60539,(~M\_61233,~M\_61234,~M\_61235),~M\_61232)

a 60538,a 60539,(partial iv 60548,IDir 60544,idcontext 60547), aeadEncrypt(HKDF(msecret 60545,msalt 60546,(IDir 60544, idcontext 60547,AES\_CCM,label\_key),alg\_key\_length( AES\_CCM,label\_key)),aeadNonce(IDir\_60544,partial iv 60548, HKDF(msecret 60545,msalt 60546,(emptyId,idcontext 60547, AES\_CCM,label\_iv),alg\_key\_length(AES\_CCM,label\_iv))), ((CoAP\_GETCode,isLightBulbTurnedOn),msg1id 60559), (encrypt0,oscore\_version one,AES CCM,IDir 60544,

 $\sim$ M 62438 = bounded by(a 60539)

 $\sim$ M\_62443 = aeadEncrypt(HKDF(msecret\_60545,msalt\_60546, (IDri 60543,idcontext 60547,AES CCM,label key), alg\_key\_length(AES\_CCM,label\_key)),aeadNonce(IDir\_60544, partial iv 60548,HKDF(msecret 60545,msalt 60546, (emptyId,idcontext 60547,AES CCM,label iv),alg key length( AES CCM, label iv))),((CoAP CONTENTCode, bounded by( (CoAP GETCode, is LightBulbTurnedOn))), msg2id 62422), (encrypt0,oscore version one,AES CCM,IDir 60544,

{59} insert replay\_window(responder,partial\_iv\_60548) {60} new msg2id 60970 {61} new responseId\_ 60971 {67} event endResponder(initiator,responder,(CoAP\_GETCode, isLightBulbTurnedOn))

**Honest Process** 

{1}new IDir 60544

{2}new IDri\_60543

{3}new msecret 60545

{4}new msalt 60546

{5} new idcontext\_60547

{6} insert security\_context\_lookup(initiator,responder,

IDir\_60544,IDri\_60543,msecret\_60545,msalt\_60546,

idcontext\_ $605\overline{4}7$ )

{7} insert security\_context\_lookup(responder,initiator,

IDri\_60543,IDir\_60544,msecret\_60545,msalt\_60546, idcontext\_60547)

(initiator, a 60540)

responder

(~M\_61225,~M\_61226,~M\_61227,~M\_61228,~M\_61229,

~M 61230,(~M 61233,~M 61234,~M 61235),~M 61232)

{70} get security\_context\_lookup(responder,initiator,

IDri 60543, IDir 60544, msecret 60545, msalt 60546,

idcontext  $605\overline{47}$ )

{69} get replay\_window(=responder,partial\_61418:

bitstring) suchthat (partial\_61418 = partial\_iv\_60548):

else branch taken

 $\sim X \mid 1$ 

Beginning of process oscore\_responder

Beginning of process oscore\_initiator

{11}new token\_60557

{12}new messageid\_60558

{13}new partial\_iv\_60548

{30} get security\_context\_lookup(initiator,responder, IDir\_60544,IDri\_60543,msecret\_60545,msalt\_60546,

idcontext  $605\overline{47}$ )

{21}new msg1id\_60559

{27} insert token\_to\_message\_lookup(initiator,token\_60557,

(responder,IDir\_60544,IDri\_60543,idcontext\_60547,

partial\_iv\_60548,aeadNonce(IDir\_60544,partial\_iv\_60548,

HKDF(msecret\_60545,msalt\_60546,(emptyId,idcontext\_60547, AES\_CCM,label\_iv),alg\_key\_length(AES\_CCM,label\_iv)))))

{28} event startInitiator(initiator,responder,(

CoAP\_GETCode, is LightBulbTurnedOn))