Abbreviations
~M_22348 = coap_version_one
~M_22349 = non_confirmable
~M_22350 = bounded_by(token_21744)
~M_22351 = CoAP_POSTCode
~M_22352 = messageid_21745
~M_22353 = token_21744
~M_22356 = partial_iv_21735
~M_22357 = IDir_21731
~M_22358 = idcontext_21734
~M_22355 = aeadEncrypt(HKDF(msecret_21732,msalt_21733, (IDir_21731,idcontext_21734,AES_CCM,label_key), alg_key_length(AES_CCM,label_key)),aeadNonce(IDir_21731, partial_iv_21735,HKDF(msecret_21732,msalt_21733, (emptyId,idcontext_21734,AES_CCM,label_iv),alg_key_length(AES_CCM,label_iv))),((CoAP_GETCode,isLightBulbTurnedOn), msg_1id_21746),(encrypt0,oscore_version_one,AES_CCM, IDir_21731,partial_iv_21735))
~X_1 = (coap_version_one,non_confirmable,a_21725,a_21726, a_21727,a_21728,(~M_22356,~M_22357,~M_22358),~M_22355) = (coap_version_one,non_confirmable,a_21725,a_21726, a_21727,a_21728,(partial_iv_21735,IDir_21731,idcontext_21734), aeadEncrypt(HKDF(msecret_21732,msalt_21733,(IDir_21731, idcontext_21734,AES_CCM,label_key),alg_key_length(AES_CCM,label_key)),aeadNonce(IDir_21731,partial_iv_21735, HKDF(msecret_21732,msalt_21733,(emptyId,idcontext_21734, AES_CCM,label_iv),alg_key_length(AES_CCM,label_iv))), ((CoAP_GETCode,isLightBulbTurnedOn),msg_1id_21746), (encrypt0,oscore_version_one,AES_CCM,IDir_21731, partial_iv_21735)))
~X_2 = (coap_version_one,non_confirmable,a_21725,a_21726, a_21727,a_21728,(~M_22356,~M_22357,~M_22358),~M_22355) = (coap_version_one,non_confirmable,a_21725,a_21726, a_21727,a_21728,(partial_iv_21735,IDir_21731,idcontext_21734), aeadEncrypt(HKDF(msecret_21732,msalt_21733,(IDir_21731, idcontext_21734,AES_CCM,label_key),alg_key_length(AES_CCM,label_key)),aeadNonce(IDir_21731,partial_iv_21735, HKDF(msecret_21732,msalt_21733,(emptyId,idcontext_21734, AES_CCM,label_iv),alg_key_length(AES_CCM,label_iv))), ((CoAP_GETCode,isLightBulbTurnedOn),msg_1id_21746), (encrypt0,oscore_version_one,AES_CCM,IDir_21731, partial_iv_21735)))
~M_23166 = coap_version_one
~M_23167 = non_confirmable
~M_23168 = bounded_by(a_21728)
~M_23169 = CoAP_CHANGEDCode
~M_23170 = responseId_23153
~M_23171 = a_21728
~M_23172 = empty
~M_23173 = aeadEncrypt(HKDF(msecret_21732,msalt_21733, (IDri_21730,idcontext_21734,AES_CCM,label_key), alg_key_length(AES_CCM,label_key)),aeadNonce(IDir_21731, partial_iv_21735,HKDF(msecret_21732,msalt_21733, (emptyId,idcontext_21734,AES_CCM,label_iv),alg_key_length(AES_CCM,label_iv))),(((CoAP_GETCode,isLightBulbTurnedOn), CoAP_CONTENTCode),msg_2id_23152),(encrypt0,oscore_version_one, AES_CCM,IDir_21731,partial_iv_21735))

A trace has been found.

Honest Process

Attacker

{1}new IDir_21731

{2}new IDri_21730

{3}new msecret_21732

{4}new msalt_21733

{5}new idcontext_21734

{6}insert security_context_lookup(initiator,responder, IDir_21731,IDri_21730,msecret_21732,msalt_21733, idcontext_21734)

{7}insert security_context_lookup(responder,initiator, IDri_21730,IDir_21731,msecret_21732,msalt_21733, idcontext_21734)

!

!

!

!

Beginning of process oscore_initiator(initiator)

{9}new token_21744

{10}new messageid_21745

{11}new partial_iv_21735

Beginning of process oscore_responder(responder)

Beginning of process oscore_responder(responder)

responder

{32}get security_context_lookup(initiator,responder, IDir_21731,IDri_21730,msecret_21732,msalt_21733, idcontext_21734)

{21}new msg_1id_21746

{27}insert token_to_message_lookup(initiator,token_21744, (responder,IDir_21731,IDri_21730,idcontext_21734, partial_iv_21735,aeadNonce(IDir_21731,partial_iv_21735, HKDF(msecret_21732,msalt_21733,(emptyId,idcontext_21734, AES_CCM,label_iv),alg_key_length(AES_CCM,label_iv)))))

{28}event request_binding(token_21744,(responder, IDir_21731,IDri_21730,idcontext_21734,partial_iv_21735, aeadNonce(IDir_21731,partial_iv_21735,HKDF(msecret_21732, msalt_21733,(emptyId,idcontext_21734,AES_CCM,label_iv), alg_key_length(AES_CCM,label_iv)))))

{29}event startInitiator(initiator,responder,((CoAP_GETCode,isLightBulbTurnedOn),msg_1id_21746))

{30}event startInit(initiator,responder,(CoAP_GETCode, isLightBulbTurnedOn))

(~M_22348,~M_22349,~M_22350,~M_22351,~M_22352, ~M_22353,(~M_22356,~M_22357,~M_22358),~M_22355)

~X_1

{65}get security_context_lookup(responder,initiator, IDri_21730,IDir_21731,msecret_21732,msalt_21733, idcontext_21734)

{64}get unique_ivs(partial_22493: bitstring) suchthat (partial_22493 = partial_iv_21735): else branch taken

~X_2

{65}get security_context_lookup(responder,initiator, IDri_21730,IDir_21731,msecret_21732,msalt_21733, idcontext_21734)

{64}get unique_ivs(partial_23115: bitstring) suchthat (partial_23115 = partial_iv_21735): else branch taken

{53}insert unique_ivs(partial_iv_21735)

{54}new msg_2id_23152

{55}new responseId_23153

{61}event endResponder(initiator,responder,((CoAP_GETCode, isLightBulbTurnedOn),msg_1id_21746))

{62}event sendResponder(initiator,responder,bounded_by((CoAP_GETCode,isLightBulbTurnedOn)))

(~M_23166,~M_23167,~M_23168,~M_23169,~M_23170, ~M_23171,~M_23172,~M_23173)

{53}insert unique_ivs(partial_iv_21735)

{54}new msg_2id_22101

{55}new responseId_22102

{61}event endResponder(initiator,responder,((CoAP_GETCode, isLightBulbTurnedOn),msg_1id_21746))

{62}event sendResponder(initiator,responder,bounded_by((CoAP_GETCode,isLightBulbTurnedOn)))