Abbreviations
~M_15675 = coap_version_one
~M_15676 = non_confirmable
~M_15677 = bounded_by(token_15072)
~M_15678 = CoAP_POSTCode
~M_15679 = messageid_15073
~M_15680 = token_15072
~M_15683 = partial_iv_15063
~M_15684 = IDir_15061
~M_15685 = idcontext_15057
~M_15682 = aeadEncrypt(HKDF(msecret_15059,msalt_15058, (IDir_15061,idcontext_15057,AES_CCM,label_key), alg_key_length(AES_CCM,label_key)),aeadNonce(IDir_15061, partial_iv_15063,HKDF(msecret_15059,msalt_15058, (emptyId,idcontext_15057,AES_CCM,label_iv),alg_key_length(AES_CCM,label_iv))),((CoAP_GETCode,isLightBulbTurnedOn), msg_1id_15062),(encrypt0,oscore_version_one,AES_CCM, IDir_15061,partial_iv_15063))
~X_1 = (coap_version_one,non_confirmable,a_15053,a_15054, a_15055,a_15056,(~M_15683,~M_15684,~M_15685),~M_15682) = (coap_version_one,non_confirmable,a_15053,a_15054, a_15055,a_15056,(partial_iv_15063,IDir_15061,idcontext_15057), aeadEncrypt(HKDF(msecret_15059,msalt_15058,(IDir_15061, idcontext_15057,AES_CCM,label_key),alg_key_length(AES_CCM,label_key)),aeadNonce(IDir_15061,partial_iv_15063, HKDF(msecret_15059,msalt_15058,(emptyId,idcontext_15057, AES_CCM,label_iv),alg_key_length(AES_CCM,label_iv))), ((CoAP_GETCode,isLightBulbTurnedOn),msg_1id_15062), (encrypt0,oscore_version_one,AES_CCM,IDir_15061, partial_iv_15063)))
~X_2 = (coap_version_one,non_confirmable,a_15053,a_15054, a_15055,a_15056,(~M_15683,~M_15684,~M_15685),~M_15682) = (coap_version_one,non_confirmable,a_15053,a_15054, a_15055,a_15056,(partial_iv_15063,IDir_15061,idcontext_15057), aeadEncrypt(HKDF(msecret_15059,msalt_15058,(IDir_15061, idcontext_15057,AES_CCM,label_key),alg_key_length(AES_CCM,label_key)),aeadNonce(IDir_15061,partial_iv_15063, HKDF(msecret_15059,msalt_15058,(emptyId,idcontext_15057, AES_CCM,label_iv),alg_key_length(AES_CCM,label_iv))), ((CoAP_GETCode,isLightBulbTurnedOn),msg_1id_15062), (encrypt0,oscore_version_one,AES_CCM,IDir_15061, partial_iv_15063)))
~M_16493 = coap_version_one
~M_16494 = non_confirmable
~M_16495 = bounded_by(a_15056)
~M_16496 = CoAP_CHANGEDCode
~M_16497 = responseId_16480
~M_16498 = a_15056
~M_16499 = empty
~M_16500 = aeadEncrypt(HKDF(msecret_15059,msalt_15058, (IDri_15060,idcontext_15057,AES_CCM,label_key), alg_key_length(AES_CCM,label_key)),aeadNonce(IDir_15061, partial_iv_15063,HKDF(msecret_15059,msalt_15058, (emptyId,idcontext_15057,AES_CCM,label_iv),alg_key_length(AES_CCM,label_iv))),(((CoAP_GETCode,isLightBulbTurnedOn), CoAP_CONTENTCode),msg_2id_16479),(encrypt0,oscore_version_one, AES_CCM,IDir_15061,partial_iv_15063))

A trace has been found.

Honest Process

Attacker

{1}new IDir_15061

{2}new IDri_15060

{3}new msecret_15059

{4}new msalt_15058

{5}new idcontext_15057

{6}insert security_context_lookup(initiator,responder, IDir_15061,IDri_15060,msecret_15059,msalt_15058, idcontext_15057)

{7}insert security_context_lookup(responder,initiator, IDri_15060,IDir_15061,msecret_15059,msalt_15058, idcontext_15057)

!

!

!

!

Beginning of process oscore_initiator(initiator)

{9}new token_15072

{10}new messageid_15073

{11}new partial_iv_15063

Beginning of process oscore_responder(responder)

Beginning of process oscore_responder(responder)

responder

{32}get security_context_lookup(initiator,responder, IDir_15061,IDri_15060,msecret_15059,msalt_15058, idcontext_15057)

{21}new msg_1id_15062

{27}insert token_to_message_lookup(initiator,token_15072, (responder,IDir_15061,IDri_15060,idcontext_15057, partial_iv_15063,aeadNonce(IDir_15061,partial_iv_15063, HKDF(msecret_15059,msalt_15058,(emptyId,idcontext_15057, AES_CCM,label_iv),alg_key_length(AES_CCM,label_iv)))))

{28}event request_binding(token_15072,(responder, IDir_15061,IDri_15060,idcontext_15057,partial_iv_15063, aeadNonce(IDir_15061,partial_iv_15063,HKDF(msecret_15059, msalt_15058,(emptyId,idcontext_15057,AES_CCM,label_iv), alg_key_length(AES_CCM,label_iv)))))

{29}event startInitiator(initiator,responder,((CoAP_GETCode,isLightBulbTurnedOn),msg_1id_15062))

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

(~M_15675,~M_15676,~M_15677,~M_15678,~M_15679, ~M_15680,(~M_15683,~M_15684,~M_15685),~M_15682)

~X_1

{65}get security_context_lookup(responder,initiator, IDri_15060,IDir_15061,msecret_15059,msalt_15058, idcontext_15057)

{64}get unique_ivs(partial_15820: bitstring) suchthat (partial_15820 = partial_iv_15063): else branch taken

~X_2

{65}get security_context_lookup(responder,initiator, IDri_15060,IDir_15061,msecret_15059,msalt_15058, idcontext_15057)

{64}get unique_ivs(partial_16442: bitstring) suchthat (partial_16442 = partial_iv_15063): else branch taken

{53}insert unique_ivs(partial_iv_15063)

{54}new msg_2id_16479

{55}new responseId_16480

{61}event endResponder(initiator,responder,((CoAP_GETCode, isLightBulbTurnedOn),msg_1id_15062))

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

(~M_16493,~M_16494,~M_16495,~M_16496,~M_16497, ~M_16498,~M_16499,~M_16500)

{53}insert unique_ivs(partial_iv_15063)

{54}new msg_2id_15428

{55}new responseId_15429

{61}event endResponder(initiator,responder,((CoAP_GETCode, isLightBulbTurnedOn),msg_1id_15062))