\sim X_1 = Request(Header(\sim M_15486, \sim M_15487, \sim M_15488, \sim M_15489, ~M_15490),~M_15480,CoAP_Option_OSCORE_Option(~M_15484, ~M_15485),payload_from_ciphertext(~M_15483)) Request(Header(CoAP_versionOne,CoAP_nonConfirm, CoAP_tokenLength(token_14757),CoAP_GETCode,messageID_14758), token_14757,CoAP_Option_OSCORE_Option(partial_iv_14759, IDir_14760),payload_from_ciphertext(enc_COSE_ciphertext(derive_key(MasterSecret_14755,IDir_14760,default_aead_algorithm), aead nonce(IDir 14760, derive common iv(MasterSecret 14755, default_aead_algorithm),partial_iv_14759),(CoAP_POSTCode, payload_14761), AAD(oscore_version_one, default_aead_algorithm, IDir_14760,partial_iv_14759)))) \sim X_2 = Request(Header(a_14750,a_14751,a_14752,a_14753, a_14754),a_14749,CoAP_Option_OSCORE_Option(~M_15484, ~M_15023),payload_from_ciphertext(~M_15483)) Request(Header(a_14750,a_14751,a_14752,a_14753, a_14754),a_14749,CoAP_Option_OSCORE_Option(partial_iv_14759, IDir_14760),payload_from_ciphertext(enc_COSE_ciphertext(derive_key(MasterSecret_14755,IDir_14760,default_aead_algorithm), aead nonce(IDir 14760, derive common iv(MasterSecret 14755, default_aead_algorithm),partial_iv_14759),(CoAP_POSTCode, payload 14761), AAD (oscore version one, default aead algorithm, IDir_14760,partial_iv_14759)))) $\sim X_3 = \text{Request(Header(}\sim M_15818, \sim M_15819, \sim M_15820, \sim M_15821,$ ~M 15822),~M 15814,CoAP Option OSCORE Option empty, payload_from_ciphertext(~M_15817)) = Request(Header(CoAP_versionOne,CoAP_nonConfirm,CoAP_tokenLength(a_14749),CoAP_CHANGEDCode,responseMessageId_14809), a_14749,CoAP_Option_OSCORE_Option_empty,payload_from_ciphertext(enc_COSE_ciphertext(derive_key(MasterSecret_14755, IDri 14756, default aead algorithm), aead nonce(IDir 14760, derive common iv (Master Secret 14755, default_aead_algorithm),partial_iv_14759),(generateResponseCode(CoAP_POSTCode,payload_14761),generateResponsePayload(CoAP_POSTCode,payload_14761)),AAD(oscore_version_one, default aead algorithm, IDri 14756, partial iv 14759)))) $\sim X_4 = \text{Request(Header(a_14743,a_14744,a_14745,a_14746,$ a_14747),~M_15480,CoAP_Option_OSCORE_Option_empty, payload_from_ciphertext(~M_15817)) = Request(Header(a 14743,a 14744,a 14745,a 14746,a 14747),token 14757, CoAP_Option_OSCORE_Option_empty,payload_from_ciphertext(enc_COSE_ciphertext(derive_key(MasterSecret_14755, IDri_14756,default_aead_algorithm),aead_nonce(IDir 14760, derive common iv (Master Secret 14755, default_aead_algorithm),partial_iv_14759),(generateResponseCode(CoAP_POSTCode,payload_14761),generateResponsePayload(CoAP POSTCode, payload 14761), AAD (oscore version one, default_aead_algorithm,IDri_14756,partial_iv_14759))))

A trace has been found.

Abbreviations

Attacker **Honest Process** {1}new IDir_14760 {2}new IDri 14756 {3}new MasterSecret_14755 $(\sim M_15023, \sim M_15024) = (IDir_14760, IDri_14756)$ [8] insert security_context_lookup(IDir_14760,IDri_14756, MasterSecret_14755) [94] event IvReveal(derive_common_iv(MasterSecret_14755, default_aead_algorithm)) [90] event Reveal(derive_key(MasterSecret_14755, IDir_14760,default_aead_algorithm)] [92] event Reveal(derive_key(MasterSecret_14755, IDri_14756,default_aead_algorithm)] Beginning of process oscore_initiator(IDir_14760) Beginning of process oscore_responder(IDri_14756) ~M_15026 = derive_common_iv(MasterSecret_14755, default_aead_algorithm) ~M_15028 = derive_key(MasterSecret_14755,IDri_14756, default_aead_algorithm) \sim M_15030 = derive_key(MasterSecret_14755,IDir_14760, default_aead_algorithm) \sim M 15024 = IDri 14756 {11} event beginBparam(IDri_14756) {43} get security_context_lookup(IDir_14760,IDri_14756, MasterSecret_14755) {15} new token_14757 {16} new partial_iv_14759 {21}new messageID_14758 {22} new payload_14761 ~X 1 ~X_2 {48} event beginAparam(IDir_14760) {73} get security_context_lookup(IDir_14760,IDri_14756, MasterSecret_14755) {72} get unique_ivs(partial_15753: iv) suchthat (partial_15753 = partial_iv_14759): else branch taken {57} insert unique_ivs(partial_iv_14759) {66} new responseMessageId_14809 {69} event respondFinish(partial_iv_14759) [70] event endBparam(IDri_14756) $\sim X_3$ ~X_4 [41] event endAparam(IDir_14760)

{42} event here