Abbreviations
~X_1 = Request(Header(~M_19075,~M_19076,~M_19077,~M_19078, ~M_19079),~M_19068,CoAP_Option_OSCORE_Option_context(~M_19072,~M_19073,~M_19074),payload_from_ciphertext(~M_19071)) = Request(Header(CoAP_versionOne,CoAP_nonConfirm, CoAP_tokenLength(token_18529),CoAP_GETCode,messageID_18530), token_18529,CoAP_Option_OSCORE_Option_context(partial_iv_18531,IDir_18528,a_18521),payload_from_ciphertext(enc_COSE_ciphertext(derive_key_context(a_18520, IDir_18528,default_aead_algorithm,a_18521),aead_nonce(IDir_18528,derive_common_iv_context(a_18520,a_18521, default_aead_algorithm),partial_iv_18531),(CoAP_POSTCode, payload_18532),AAD(encrypt0_context,encrypt0(oscore_version_one, default_aead_algorithm,IDir_18528,partial_iv_18531)))))
~X_2 = Request(Header(a_18515,a_18516,a_18517,a_18518, a_18519),~M_19068,CoAP_Option_OSCORE_Option_empty, payload_from_ciphertext(~M_19071)) = Request(Header(a_18515,a_18516,a_18517,a_18518,a_18519),token_18529, CoAP_Option_OSCORE_Option_empty,payload_from_ciphertext(enc_COSE_ciphertext(derive_key_context(a_18520, IDir_18528,default_aead_algorithm,a_18521),aead_nonce(IDir_18528,derive_common_iv_context(a_18520,a_18521, default_aead_algorithm),partial_iv_18531),(CoAP_POSTCode, payload_18532),AAD(encrypt0_context,encrypt0(oscore_version_one, default_aead_algorithm,IDir_18528,partial_iv_18531)))))

A trace has been found.

Honest Process

Attacker

{1}new IDir_18528

{2}new IDri_18563

{3}new MasterSecret_18569

{4}new idcontext_18564

(~M_18572,~M_18573,~M_18574) = (IDir_18528,IDri_18563, idcontext_18564)

{6}insert security_context_lookup(IDir_18528,IDri_18563, MasterSecret_18569,idcontext_18564)

!

!

!

Beginning of process oscore_initiator(IDir_18528)

Beginning of process init(IDir_18528, IDri_18563)

Beginning of process init(IDir_18528, IDri_18563)

(~M_18572,a_18521) = (IDir_18528,a_18521)

{9}event beginBparam(IDir_18528)

(a_18522,~M_18572,a_18523,~M_18572,a_18520,a_18521) = (a_18522,IDir_18528,a_18523,IDir_18528,a_18520, a_18521)

{78}insert security_context_lookup(IDir_18528, IDir_18528,a_18520,a_18521)

{42}get security_context_lookup(IDir_18528,IDir_18528, a_18520,a_18521)

{13}new token_18529

{14}new partial_iv_18531

{19}new messageID_18530

{20}new payload_18532

~X_1

{31}event here

~X_2

{40}event endAparam(IDir_18528)