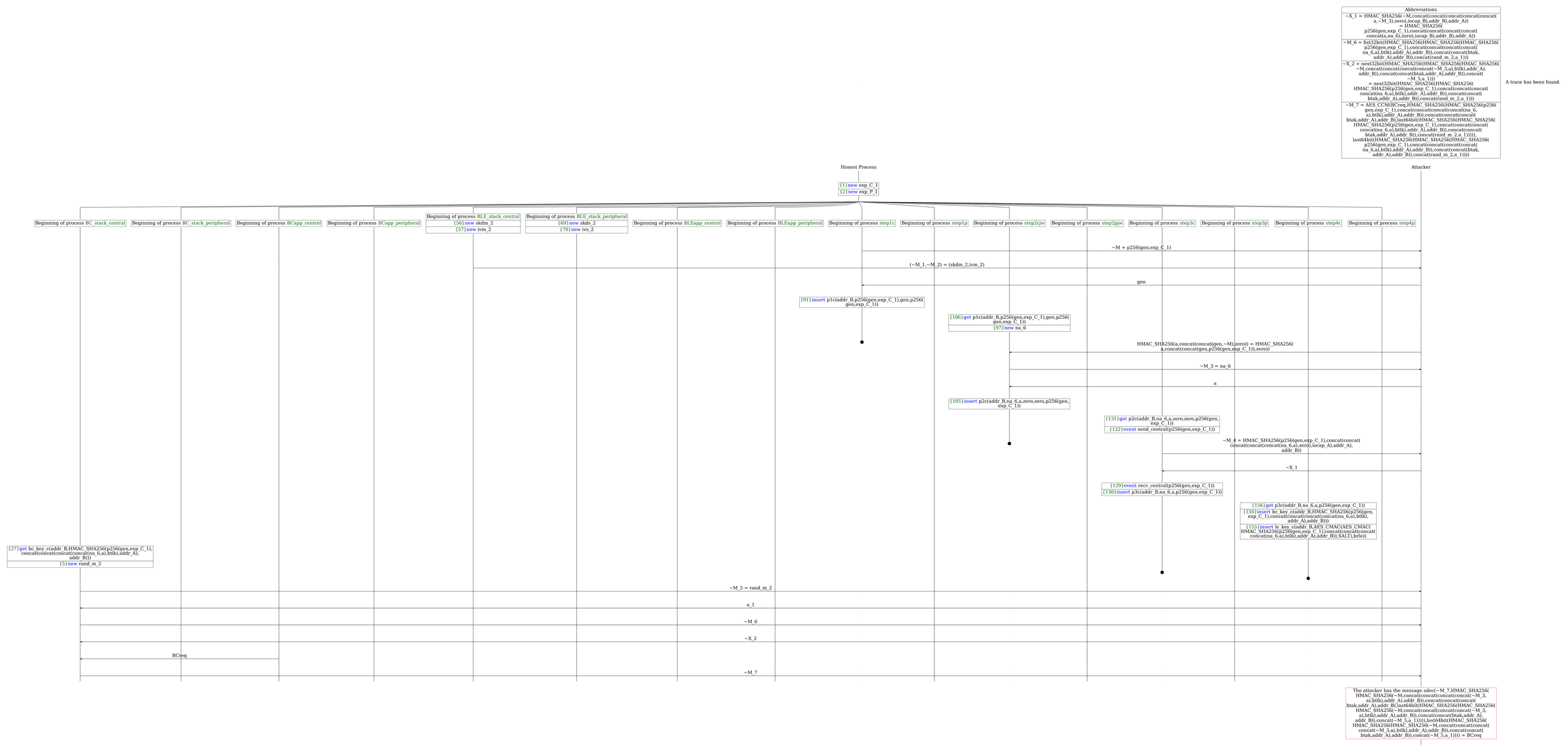
Abbreviations
~X_1 = HMAC_SHA256(~M,concat(concat(concat(concat(concat(a,~M_3),zero),iocap_B),addr_B),addr_A))
= HMAC_SHA256(gen,exp_C_1),concat(concat(concat(concat(concat(na_6,a),zero),iocap_A),addr_A),addr_B))
~M_6 = fst32bit(HMAC_SHA256(HMAC_SHA256(HMAC_SHA256(p256(gen,exp_C_1),concat(concat(concat(concat(na_6,a),btlk),addr_A),addr_B)),concat(concat(btak,addr_A),addr_B)),concat(rand_m_2,a_1)))
~X_2 = next32bit(HMAC_SHA256(HMAC_SHA256(HMAC_SHA256(~M,concat(concat(concat(concat(~M_3,a),btlk),addr_A),addr_B)),concat(concat(btak,addr_A),addr_B)),concat(~M_5,a_1)))
= next32bit(HMAC_SHA256(HMAC_SHA256(p256(gen,exp_C_1),concat(concat(concat(na_6,a),btlk),addr_A),addr_B)),concat(concat(btak,addr_A),addr_B)),concat(rand_m_2,a_1)))
~M_7 = AES_CCM(BCreq,HMAC_SHA256(HMAC_SHA256(p256(gen,exp_C_1),concat(concat(concat(concat(na_6,a),btlk),addr_A),addr_B)),concat(concat(concat(btak,addr_A),addr_B),last64bit(HMAC_SHA256(HMAC_SHA256(p256(gen,exp_C_1),concat(concat(concat(concat(na_6,a),btlk),addr_A),addr_B)),concat(concat(btak,addr_A),addr_B)),concat(rand_m_2,a_1)))),last64bit(HMAC_SHA256(HMAC_SHA256(p256(gen,exp_C_1),concat(concat(concat(concat(na_6,a),btlk),addr_A),addr_B)),concat(concat(btak,addr_A),addr_B)),concat(rand_m_2,a_1))))
A trace has been found.
Honest Process
{1}new exp_C_1
{2}new exp_P_1
Attacker
Beginning of process BC_stack_central
Beginning of process BC_stack_peripheral
Beginning of process BCapp_central
Beginning of process BCapp_peripheral
Beginning of process BLE_stack_central
{56}new skdm_2
{57}new ivm_2
Beginning of process BLE_stack_peripheral
{69}new skds_2
{70}new ivs_2
Beginning of process BLEapp_central
Beginning of process BLEapp_peripheral
Beginning of process step1c
Beginning of process step1p
Beginning of process step2cjw
Beginning of process step2pjw
Beginning of process step3c
Beginning of process step3p
Beginning of process step4c
Beginning of process step4p
~M = p256(gen,exp_C_1)
(~M_1,~M_2) = (skdm_2,ivm_2)
gen
{91}insert p1c(addr_B,p256(gen,exp_C_1),gen,p256(gen,exp_C_1))
{106}get p1c(addr_B,p256(gen,exp_C_1),gen,p256(gen,exp_C_1))
{97}new na_6
HMAC_SHA256(a,concat(concat(gen,~M),zero)) = HMAC_SHA256(a,concat(concat(gen,p256(gen,exp_C_1)),zero))
~M_3 = na_6
a
{105}insert p2c(addr_B,na_6,a,zero,zero,p256(gen,exp_C_1))
{131}get p2c(addr_B,na_6,a,zero,zero,p256(gen,exp_C_1))
{122}event send_central(p256(gen,exp_C_1))
~M_4 = HMAC_SHA256(p256(gen,exp_C_1),concat(concat(concat(concat(na_6,a),zero),iocap_A),addr_A),addr_B))
~X_1
{129}event recv_central(p256(gen,exp_C_1))
{130}insert p3c(addr_B,na_6,a,p256(gen,exp_C_1))
{156}get p3c(addr_B,na_6,a,p256(gen,exp_C_1))
{150}insert bc_key_c(addr_B,HMAC_SHA256(p256(gen,exp_C_1),concat(concat(concat(concat(na_6,a),btlk),addr_A),addr_B)))
{155}insert le_key_c(addr_B,AES_CMAC(AES_CMAC(HMAC_SHA256(p256(gen,exp_C_1),concat(concat(concat(concat(na_6,a),btlk),addr_A),addr_B)),SALT),brle))
{27}get bc_key_c(addr_B,HMAC_SHA256(p256(gen,exp_C_1),concat(concat(concat(concat(concat(na_6,a),btlk),addr_A),addr_B)))
{5}new rand_m_2
~M_5 = rand_m_2
a_1
~M_6
~X_2
BCreq
~M_7
The attacker has the message sdec(~M_7,HMAC_SHA256(HMAC_SHA256(~M,concat(concat(concat(concat(concat(~M_3,a),btlk),addr_A),addr_B)),concat(concat(concat(btak,addr_A),addr_B),last64bit(HMAC_SHA256(HMAC_SHA256(HMAC_SHA256(~M,concat(concat(concat(concat(concat(~M_3,a),btlk),addr_A),addr_B)),concat(concat(btak,addr_A),addr_B)),concat(~M_5,a_1)))),last64bit(HMAC_SHA256(HMAC_SHA256(HMAC_SHA256(~M,concat(concat(concat(concat(concat(~M_3,a),btlk),addr_A),addr_B)),concat(concat(btak,addr_A),addr_B)),concat(~M_5,a_1)))) = BCreq