Abbreviations
~M_4 = AES_CCM(BCreq,HMAC_SHA256(lk_1,concat(concat(concat(btak,addr_A),addr_B),last64bit(HMAC_SHA256(HMAC_SHA256(lk_1,concat(concat(btak,addr_A),addr_B)),concat(rand_m_2,rand_s_2))))),last64bit(HMAC_SHA256(HMAC_SHA256(lk_1,concat(concat(btak,addr_A),addr_B)),concat(rand_m_2,rand_s_2))))

A trace has been found.

Honest Process

Attacker

Beginning of process BC_secure_pairing

{2}new lk_1

{3}insert bc_key_c(addr_B,lk_1)

{4}insert bc_key_p(addr_A,lk_1)

{9}insert le_key_c(addr_B,AES_CMAC(AES_CMAC(lk_1, SALT),brle))

{14}insert le_key_p(addr_A,AES_CMAC(AES_CMAC(lk_1, SALT),brle))

Beginning of process BC_stack_central

{38}get bc_key_c(addr_B,lk_1)

{16}new rand_m_2

Beginning of process BC_stack_peripheral_compromised

Beginning of process BCapp_central

~M = rand_m_2

{79}get bc_key_p(addr_A,lk_1)

{54}new rand_s_2

~M = rand_m_2

~M_1 = rand_s_2

~M_1 = rand_s_2

~M_2 = fist32bit(HMAC_SHA256(HMAC_SHA256(lk_1, concat(concat(btak,addr_A),addr_B)),concat(rand_m_2, rand_s_2)))

~M_2 = fist32bit(HMAC_SHA256(HMAC_SHA256(lk_1, concat(concat(btak,addr_A),addr_B)),concat(rand_m_2, rand_s_2)))

~M_3 = next32bit(HMAC_SHA256(HMAC_SHA256(lk_1, concat(concat(btak,addr_A),addr_B)),concat(rand_m_2, rand_s_2)))

~M_3 = next32bit(HMAC_SHA256(HMAC_SHA256(lk_1, concat(concat(btak,addr_A),addr_B)),concat(rand_m_2, rand_s_2)))

BCreq

~M_4

~M_4

~M_5 = BCreq

The attacker has the message ~M_5 = BCreq