Abbreviations $\sim X_1 = (derive_encryption_key(exp(exp(g,derive_prikey_from_sn(g,derive_prik$ serial_number_const)),pri_c),rand_3),(exp(g,pri_c), (SendPubkey,pre_app1))) ~M_9 = AES_enc(smartthings_const,derive_key(derive_encryption_key(exp(exp(g,derive_prikey_from_sn(serial_number_const)), pri_c),rand_3),bleAuthentication_const),n2_2) \sim M 10 = open ch ~M_11 = AES_enc(smartthings_const,derive_key(derive_encryption_key(exp(exp(g,pri_c),derive_prikey_from_sn(serial_number_const)), rand 3),bleAuthentication const),n1 2) \sim M 12 = open ch \sim X_2 = (\sim M_11,open_ch) = (AES_enc(smartthings_const,derive_key(derive_encryption_key(exp(exp(g,derive_prikey_from_sn(serial_number_const), pri_c), rand_3), bleAuthentication_const), n1 2), open ch) ~X_3 = (AES_enc(smartthings_const,derive_key(derive_encryption_key(exp(~M_3,derive_prikey_from_sn(serial_number_const)), ~M 2),bleAuthentication_const),~M_7),open_ch) (AES_enc(smartthings_const,derive_key(derive_encryption_key(exp(exp(g,derive_prikey_from_sn(serial_number_const)), pri_c),rand_3),bleAuthentication_const),n2_2), open_ch) \sim M_13 = AES_enc(serial_number_const,derive_key(derive_encryption_key(exp(exp(g,pri_c),derive_prikey_from_sn(serial_number const)), rand_3),n2_2),n2_2) \sim M 14 = open_ch \sim X 4 = (\sim M 13,open ch) = (AES enc(serial number const, derive_key(derive_encryption_key(exp(exp(exp(g,derive_prikey_from_sn(serial_number_const)),pri_c),rand_3),n2_2),n2_2), open_ch) ~M_15 = AES_enc(secure_param_4,derive_key(derive_encryption_key(exp(exp(g,derive_prikey_from_sn(serial_number_const)), pri_c),rand_3),n2_2),n2_2) \sim M 16 = open ch $\sim X_5 = (\sim M_15, open_ch) = (AES_enc(secure_param_4, derive_key))$ derive_encryption_key(exp(exp(g,derive_prikey_from_sn(serial_number_const)),pri_c),rand_3),n2_2),n2_2), open ch) g,derive_prikey_from_sn(serial_number_const)), pri_c),rand_3),privacy_const),secure_param_4,secure_param_4, secure_param_4),(id_c,central_user_data_out)) g,derive_prikey_from_sn(serial_number_const)), pri_c),rand_3),privacy_const),secure_param_4,secure_param_4, secure_param_4),(id_p,peripheral_user_data_out)) \sim M 17 = tmp ~M_18 = AES_enc(sv,get_id(derive_key(derive_encryption_key(exp(exp(g,derive_prikey_from_sn(serial_number_const)), pri_c),rand_3),privacy_const),secure_param_4,secure_param_4, secure_param_4),tmp) \sim M 19 = open ch Attacker

A trace has been found.

Honest Process {1}new sec_ch {2}event SecureChannel(sec ch) {3}event Secret(sv) (serial_number_const,(derive_hashed_sn(serial_number_const), exp(g,derive_prikey_from_sn(serial_number_const)))) $(\sim M, \sim M_1) = (derive_hashed_sn(serial_number_const),$ open_ch) (derive hashed sn(serial number const), open ch) {21} new rand_3 (derive_hashed_sn(serial_number_const),(rand_3, pre_app1)) {7}new pri_c {9}event PubkeySources(exp(g,pri_c)) ~X 1 {24} event SendPubKey(exp(g,pri_c)) $(\sim M_2, (\sim M_3, \sim M_4)) = (rand_3, (exp(g, pri_c), open_ch))$ [{27} new n1_2 $(\sim M_5, \sim M_6) \models (n1_2, open_ch)$ $(\sim M_2, (\sim M_3, open_ch)) = (rand_3, (exp(g, pri_c), exp(g, pri_c))$ open ch)) [{61}new n2_2] $(\sim M \ 7, \sim M_8) = (n2_2, open_ch)$ $(\sim M 7, open ch) = (n2 2, open ch)$ $(\sim M \ 9, \sim M \ 10)$ $(\sim M_5, open_ch) = (n1_2, open_ch)$ $(\sim M 11, \sim M 12)$ $\sim X_2$ ~X 3 {71} event SendSn(serial_number_const,AES_enc(serial_number_const, derive_key(derive_encryption_key(exp(exp(g,pri_c), derive_prikey_from_sn(serial_number_const)),rand_3), n2_2),n2_2)) $(\sim M 13, \sim M 14)$ {38} event ReceiveSn(serial number const) (serial_number_const,(derive_encryption_key(exp({15} new secure param 4 {16} event SecureParamSources(secure_param_4) (secure param 4,(secure param,pre app1)) {42}event SendSecureParam(secure_param_4,AES_enc(secure_param_4,derive_key(derive_encryption_key(exp(exp(g,derive_prikey_from_sn(serial_number_const)), pri_c),rand_3),n2_2),n2_2)) $(\sim M 15, \sim M 16)$ ~X 5 ~X 6 ~X 7 (yes confirm const, central user ui)

|{48} new tmp|

 $(\sim M 17, (\sim M 18, \sim M 19))$

The attacker has the message AES_dec(~M_18,get_id(
derive_key(derive_encryption_key(exp(~M_3,derive_prikey_from_sn(
 serial_number_const)),~M_2),privacy_const),AES_dec(
 ~M_15,derive_key(derive_encryption_key(exp(~M_3,
 derive_prikey_from_sn(serial_number_const)),~M_2),
 ~M_7),~M_7),AES_dec(~M_15,derive_key(derive_encryption_key(
 exp(~M_3,derive_prikey_from_sn(serial_number_const)),
 ~M_2),~M_7),AES_dec(~M_15,derive_key(derive_encryption_key(
 exp(~M_3,derive_prikey_from_sn(serial_number_const)),
 ~M_2),~M_7),~M_7)),~M_17) = sv