Abbreviations
~M_1 = nonce_4
~M_2 = rpid_5
~M_3 = senc(Auth1(username_4,rpid_5,skA_2),wk_2)
~M_4 = dhexp(g,dh_spairRP_2)
~M_5 = sign(RP1(nonce_4,rpid_5,senc(Auth1(username_4, rpid_5,skA_2),wk_2),dhexp(g,dh_spairRP_2)),sskey_RP_3)
~X_1 = (hash(Client1(rpid_5,nonce_4)),HMAC(pinAuth_3, hash(Client1(rpid_5,nonce_4))),RP1(nonce_4,rpid_5, senc(Auth1(username_4,rpid_5,skA_2),wk_2),dhexp(g,dh_spairRP_2)),sign(RP1(nonce_4,rpid_5,senc(Auth1(username_4,rpid_5,skA_2),wk_2),dhexp(g,dh_spairRP_2)), sskey_RP_3))

A trace has been found.

Honest Process

{1}new rpid_5

{2}new clientid_1

{3}new pinAuth_3

{4}new wk_2

{5}new aaguid_4

{6}new username_4

{7}new skA_2

{8}new sskey_RP_3

{10}insert rp_record(username_4,aaguid_4,senc(Auth1(username_4,rpid_5,skA_2),wk_2),spk(skA_2))

{11}insert auth_record(senc(Auth1(username_4,rpid_5, skA_2),wk_2))

Beginning of process RP_Auth

Beginning of process Client_Auth

Beginning of process Auth_Auth

Attacker

~M = username_4

~M = username_4

{34}get rp_record(username_4,aaguid_4,senc(Auth1(username_4,rpid_5,skA_2),wk_2),spk(skA_2))

{15}new nonce_4

{16}new dh_spairRP_2

(RP1(~M_1,~M_2,~M_3,~M_4),~M_5)

(RP1(~M_1,~M_2,~M_3,~M_4),~M_5)

{43}event Client_Init_Auth(username_4,rpid_5)

~X_1

{71}get auth_record(senc(Auth1(username_4,rpid_5, skA_2),wk_2))

{61}new dh_spairA_1

{65}event Authnr_Finish_Auth(username_4,aaguid_4, senc(Auth1(username_4,rpid_5,skA_2),wk_2),spk(skA_2))