A trace has been found.

Honest Process   Attacker

{1}new rpid_4

{2}new clientid_1

{3}new pinAuth_3

{4}new wk_2

{5}new aaguid_4

{6}new username_4

{7}new skA_2

{9}insert rp_record(username_4,aaguid_4,senc(Auth1(
username_4,rpid_4,skA_2),wk_2),spk(skA_2))

{10}insert auth_record(senc(Auth1(username_4,rpid_4,
skA_2),wk_2))

Beginning of process RP_Auth | Beginning of process Client_Auth | Beginning of process Auth_Auth

~M = username_4

~M = username_4

{22}get rp_record(username_4,aaguid_4,senc(Auth1(
username_4,rpid_4,skA_2),wk_2),spk(skA_2))

{13}new challenge_3

(~M_1,~M_2,~M_3) = (rpid_4,challenge_3,senc(Auth1(
username_4,rpid_4,skA_2),wk_2))

~X_1

{20}event Server_Finish_Auth(username_4,rpid_4,
a_1,a_2,spk(a_3))