A trace has been found.

Honest Process

Attacker

{1}new rpid_5

{2}new clientid_1

{3}new pinAuth_3

{4}new wk_2

{5}new aaguid_4

{6}new username_5

{7}new skA_2

{9}insert rp_record(username_5,aaguid_4,senc(Auth1(username_5,rpid_5,skA_2),wk_2),spk(skA_2))

{10}insert auth_record(senc(Auth1(username_5,rpid_5,skA_2),wk_2))

!

!

!

!

Beginning of process Client_Auth

Beginning of process LoadBalancer

username_5

~M = sanity1

The attacker has the message ~M = sanity1