Abbreviations
~M_6 = aenc(((groupkey_response,vid_7,gsk(vid_7,gmsk_5),gpk(gmsk_5)),sign((groupkey_response,vid_7,gsk(vid_7,gmsk_5),gpk(gmsk_5)),cask_3)),pk(vsk_4))
~M_7 = aenc(((pseudocert(pk(a_4),gsk(attvid_2,gmsk_5)),revoke_request),sign((pseudocert(pk(a_4),gsk(attvid_2,gmsk_5)),revoke_request),vsk_4),cert(vid_7,pk(vsk_4),cask_3)),pk(cask_3))

A trace has been found.

Honest Process

Attacker

{1}new gmsk_5

{2}new cask_3

~M = pk(cask_3)

!

!

!

!

Beginning of process CAGroupMasterSecretKeyReveal

{156}event CAGMSKReveal(gmsk_5)

{6}new vid_7

{7}new vsk_4

{92}new attvid_2

{93}new attsk_2

{96}event AttackerGetsEnrollmentCertificate(attvid_2, pk(attsk_2))

Beginning of process CARevoke

~M_1 = gmsk_5

Beginning of process CA

Beginning of process CA

(~M_2,~M_3,~M_4) = (attvid_2,attsk_2,cert(attvid_2, pk(attsk_2),cask_3))

Beginning of process Vehicle

{15}event ValidGroupKeyRequestSent(vid_7)

~M_5 = aenc((groupkey_request,sign(groupkey_request, vsk_4),cert(vid_7,pk(vsk_4),cask_3)),pk(cask_3))

~M_5 = aenc((groupkey_request,sign(groupkey_request, vsk_4),cert(vid_7,pk(vsk_4),cask_3)),pk(cask_3))

{116}get revokedcerts(=vid_7): else branch taken

{109}event ValidGroupKeyRequestReceived(cask_3, vid_7)

{114}event ValidGroupPrivateKeySent(vid_7,gsk(vid_7,gmsk_5),gpk(gmsk_5))

~M_6

~M_6

~M_6

{22}event ValidGroupPrivateKeyReceived(vid_7,gsk(vid_7,gmsk_5),gpk(gmsk_5))

!

!

!

Beginning of process VehicleReport(vid_7, vsk_4, cert(vid_7,pk(vsk_4),cask_3), pk(cask_3), gpk(gmsk_5))

(a_3,sign(a_3,a_4),pseudocert(pk(a_4),gsk(~M_2, ~M_1))) = (a_3,sign(a_3,a_4),pseudocert(pk(a_4), gsk(attvid_2,gmsk_5)))

{48}event RevocationAsked(vid_7,cert(vid_7,pk(vsk_4),cask_3),pseudocert(pk(a_4),gsk(attvid_2,gmsk_5)))

~M_7

aenc((groupkey_request,a_6,~M_4),~M) = aenc((groupkey_request, a_6,cert(attvid_2,pk(attsk_2),cask_3)),pk(cask_3))

~M_7

{154}get revokedcerts(=vid_7): else branch taken

{127}event ValidRevocationReportReceived(pseudocert(pk(a_4),gsk(attvid_2,gmsk_5)),cert(vid_7,pk(vsk_4),cask_3))

{153}get revokedcerts(=attvid_2): else branch taken

{130}event RevokedVid(attvid_2)

{131}insert revokedcerts(attvid_2)

{116}get revokedcerts(attvid_2)

{107}event RevokedCannotGetGroupKey(attvid_2)