Abbreviations
~M_4 = aenc(((groupkey_response,vid_11,gsk(vid_11, gmsk_7),gpk(gmsk_7)),sign((groupkey_response,vid_11, gsk(vid_11,gmsk_7),gpk(gmsk_7)),cask_3)),pk(vsk_6))
~M_5 = aenc(((groupkey_response,vid_10,gsk(vid_10, gmsk_7),gpk(gmsk_7)),sign((groupkey_response,vid_10, gsk(vid_10,gmsk_7),gpk(gmsk_7)),cask_3)),pk(vsk_5))
~M_6 = aenc(((pseudocert(pk(a_5),gsk(a_6,gmsk_7)), revoke_request),sign((pseudocert(pk(a_5),gsk(a_6, gmsk_7)),revoke_request),vsk_5),cert(vid_10,pk(vsk_5),cask_3)),pk(cask_3))

A trace has been found.

Honest Process

Attacker

{1}new gmsk_7

{2}new cask_3

~M = pk(cask_3)

!

!

!

!

Beginning of process CAGroupMasterSecretKeyReveal

{156}event CAGMSKReveal(gmsk_7)

{6}new vid_11

{7}new vsk_6

{6}new vid_10

{7}new vsk_5

Beginning of process CARevoke

~M_1 = gmsk_7

Beginning of process Vehicle

{15}event ValidGroupKeyRequestSent(vid_10)

Beginning of process CA

Beginning of process CA

Beginning of process Vehicle

{15}event ValidGroupKeyRequestSent(vid_11)

~M_2 = aenc((groupkey_request,sign(groupkey_request, vsk_5),cert(vid_10,pk(vsk_5),cask_3)),pk(cask_3))

~M_3 = aenc((groupkey_request,sign(groupkey_request, vsk_6),cert(vid_11,pk(vsk_6),cask_3)),pk(cask_3))

~M_3 = aenc((groupkey_request,sign(groupkey_request, vsk_6),cert(vid_11,pk(vsk_6),cask_3)),pk(cask_3))

{116}get revokedcerts(=vid_11): else branch taken

{109}event ValidGroupKeyRequestReceived(cask_3, vid_11)

{114}event ValidGroupPrivateKeySent(vid_11,gsk(vid_11,gmsk_7),gpk(gmsk_7))

~M_4

~M_2 = aenc((groupkey_request,sign(groupkey_request, vsk_5),cert(vid_10,pk(vsk_5),cask_3)),pk(cask_3))

{116}get revokedcerts(=vid_10): else branch taken

{109}event ValidGroupKeyRequestReceived(cask_3, vid_10)

{114}event ValidGroupPrivateKeySent(vid_10,gsk(vid_10,gmsk_7),gpk(gmsk_7))

~M_5

~M_5

{22}event ValidGroupPrivateKeyReceived(vid_10, gsk(vid_10,gmsk_7),gpk(gmsk_7))

! ! !

Beginning of process VehicleReport(vid_10, vsk_5, cert(vid_10,pk(vsk_5),cask_3), pk(cask_3), gpk(gmsk_7))

(a_4,sign(a_4,a_5),pseudocert(pk(a_5),gsk(a_6, ~M_1))) = (a_4,sign(a_4,a_5),pseudocert(pk(a_5), gsk(a_6,gmsk_7)))

{48}event RevocationAsked(vid_10,cert(vid_10,pk(vsk_5),cask_3),pseudocert(pk(a_5),gsk(a_6,gmsk_7)))

~M_6

~M_6

{154}get revokedcerts(=vid_10): else branch taken

{127}event ValidRevocationReportReceived(pseudocert(pk(a_5),gsk(a_6,gmsk_7)),cert(vid_10,pk(vsk_5), cask_3))

{153}get revokedcerts(=a_6): else branch taken

{130}event RevokedVid(a_6)

{131}insert revokedcerts(a_6)

Phase 1

{133}new updatedgmsk_1

Phase 2

!

Beginning of process Vehicle

{56}event ValidGroupKeyRequestSent(vid_11)

Beginning of process Vehicle

{56}event ValidGroupKeyRequestSent(vid_10)

~M_7 = aenc((groupkey_request,sign(groupkey_request, vsk_5),cert(vid_10,pk(vsk_5),cask_3)),pk(cask_3))

~M_8 = aenc((groupkey_request,sign(groupkey_request, vsk_6),cert(vid_11,pk(vsk_6),cask_3)),pk(cask_3))

~M_4

{63}event ValidGroupPrivateKeyReceived(vid_11, gsk(vid_11,gmsk_7),gpk(gmsk_7))

! ! !

Beginning of process VehicleReceive(vid_11, gpk(gmsk_7))

(a_9,sign(a_9,a_10),pseudocert(pk(a_10),gsk(a_6, ~M_1))) = (a_9,sign(a_9,a_10),pseudocert(pk(a_10), gsk(a_6,gmsk_7)))

{79}event ValidMessageReceived(vid_11,a_9)

{80}event ValidMessageReceivedSenderVid(a_6)