Abbreviations
~M_4 = aenc(((groupkey_response,vid_11,gsk(vid_11, gmsk_6),gpk(gmsk_6)),sign((groupkey_response,vid_11, gsk(vid_11,gmsk_6),gpk(gmsk_6)),cask_3)),pk(vsk_7))
~M_11 = aenc((groupkey_response,vid_10,gsk(vid_10, gmsk_6),gpk(gmsk_6)),sign((groupkey_response,vid_10, gsk(vid_10,gmsk_6),gpk(gmsk_6)),cask_3)),pk(vsk_6))
~M_12 = aenc(((pseudocert(pk(vpseudosk_4),gsk(vid_11,gmsk_6)),revoke_request),sign((pseudocert(pk(vpseudosk_4),gsk(vid_11,gmsk_6)),revoke_request), vsk_6),cert(vid_10,pk(vsk_6),cask_3)),pk(cask_3))
~M_16 = aenc(((groupkey_response,vid_12,gsk(vid_12, updatedgmsk_2),gpk(updatedgmsk_2)),sign((groupkey_response, vid_12,gsk(vid_12,updatedgmsk_2),gpk(updatedgmsk_2)), cask_3)),pk(vsk_8))

A trace has been found.

Honest Process

Attacker

{1}new gmsk_6

{2}new cask_3

~M = pk(cask_3)

!

{6}new vid_12

{7}new vsk_8

{6}new vid_11

{7}new vsk_7

{6}new vid_10

{7}new vsk_6

Beginning of process CARevoke

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_1 = aenc((groupkey_request,sign(groupkey_request, vsk_6),cert(vid_10,pk(vsk_6),cask_3)),pk(cask_3))

Beginning of process Vehicle

{15}event ValidGroupKeyRequestSent(vid_12)

~M_2 = aenc((groupkey_request,sign(groupkey_request, vsk_7),cert(vid_11,pk(vsk_7),cask_3)),pk(cask_3))

~M_3 = aenc((groupkey_request,sign(groupkey_request, vsk_8),cert(vid_12,pk(vsk_8),cask_3)),pk(cask_3))

~M_2 = aenc((groupkey_request,sign(groupkey_request, vsk_7),cert(vid_11,pk(vsk_7),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_6),gpk(gmsk_6))

~M_4

~M_4

{22}event ValidGroupPrivateKeyReceived(vid_11, gsk(vid_11,gmsk_6),gpk(gmsk_6))

!

Beginning of process VehicleSend(vid_11, gsk(vid_11, gmsk_6))

{24}new vpseudosk_4

{27}event PseudoCertCreated(vid_11,vpseudosk_4)

!

{29}new m_10

{31}event ValidMessageSent(vid_11,pseudocert(pk(vpseudosk_4),gsk(vid_11,gmsk_6)),m_10)

{29}new m_9

{31}event ValidMessageSent(vid_11,pseudocert(pk(vpseudosk_4),gsk(vid_11,gmsk_6)),m_9)

(~M_5,~M_6,~M_7) = (m_9,sign(m_9,vpseudosk_4), pseudocert(pk(vpseudosk_4),gsk(vid_11,gmsk_6)))

(~M_8,~M_9,~M_10) = (m_10,sign(m_10,vpseudosk_4), pseudocert(pk(vpseudosk_4),gsk(vid_11,gmsk_6)))

~M_1 = aenc((groupkey_request,sign(groupkey_request, vsk_6),cert(vid_10,pk(vsk_6),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_6),gpk(gmsk_6))

~M_11

~M_11

{22}event ValidGroupPrivateKeyReceived(vid_10, gsk(vid_10,gmsk_6),gpk(gmsk_6))

Beginning of process VehicleReport(vid_10, vsk_6, cert(vid_10,pk(vsk_6),cask_3), pk(cask_3), gpk(gmsk_6))

(~M_8,~M_9,~M_7) = (m_10,sign(m_10,vpseudosk_4), pseudocert(pk(vpseudosk_4),gsk(vid_11,gmsk_6)))

{48}event RevocationAsked(vid_10,cert(vid_10,pk(vsk_6),cask_3),pseudocert(pk(vpseudosk_4),gsk(vid_11,gmsk_6)))

~M_12

~M_12

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

{127}event ValidRevocationReportReceived(pseudocert(pk(vpseudosk_4),gsk(vid_11,gmsk_6)),cert(vid_10, pk(vsk_6),cask_3))

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

{130}event RevokedVid(vid_11)

{131}insert revokedcerts(vid_11)

Phase 1

{133}new updatedgmsk_2

Phase 2

Beginning of process Vehicle

{56}event ValidGroupKeyRequestSent(vid_12)

Beginning of process Vehicle

{56}event ValidGroupKeyRequestSent(vid_11)

Beginning of process Vehicle

{56}event ValidGroupKeyRequestSent(vid_10)

Beginning of process CA

~M_13 = aenc((groupkey_request,sign(groupkey_request, vsk_6),cert(vid_10,pk(vsk_6),cask_3)),pk(cask_3))

~M_14 = aenc((groupkey_request,sign(groupkey_request, vsk_7),cert(vid_11,pk(vsk_7),cask_3)),pk(cask_3))

~M_15 = aenc((groupkey_request,sign(groupkey_request, vsk_8),cert(vid_12,pk(vsk_8),cask_3)),pk(cask_3))

~M_3 = aenc((groupkey_request,sign(groupkey_request, vsk_8),cert(vid_12,pk(vsk_8),cask_3)),pk(cask_3))

{152}get revokedcerts(=vid_12): else branch taken

{145}event ValidGroupKeyRequestReceived(cask_3, vid_12)

{150}event ValidGroupPrivateKeySent(vid_12,gsk(vid_12,updatedgmsk_2),gpk(updatedgmsk_2))

~M_16

~M_16

{63}event ValidGroupPrivateKeyReceived(vid_12, gsk(vid_12,updatedgmsk_2),gpk(updatedgmsk_2))

Beginning of process VehicleSend(vid_12, gsk(vid_12, updatedgmsk_2))

{65}new vpseudosk_5

{68}event PseudoCertCreated(vid_12,vpseudosk_5)

{70}new m_11

{72}event ValidMessageSent(vid_12,pseudocert(pk(vpseudosk_5),gsk(vid_12,updatedgmsk_2)),m_11)

(~M_17,~M_18,~M_19) = (m_11,sign(m_11,vpseudosk_5), pseudocert(pk(vpseudosk_5),gsk(vid_12,updatedgmsk_2)))

Phase 5

Beginning of process CAGroupMasterSecretKeyReveal

{155}event CAGMSKReveal(updatedgmsk_2)

~M_20 = updatedgmsk_2

The attacker has the message gopen(~M_19,~M_20) = vid_12 in phase 5