Abbreviations

-M_16834 = sr_16485

-M_16836 = TLS12

-M_16841 = StrongRSADecryption

-M_16838 = a_16467

-M_16839 = a_16468

-M_16840 = a_16469

-X_1 = SH(~M_16834,nego(TLS12,RSA(a_16479),a_16480,a_16481, a_16482))

= SH(sr_16485,nego(TLS12,RSA(a_16479), a_16480,a_16481, a_16480,a_16481,a_16482))

-X_2 = FIN(tls12_prf(tls12_prf(zero,master_secret,(~M_16693, ~M_16834)),client_finished,(~M_16693, ~M_16834)))

= SH(ST_16485, SH(ST) = SH(ST) =

FIN(tls12_prf(tls12_prf(zero,master_secret,(

cr_16484,sr_16485)),client_finished,(cr_16484,

sr_16485)))

A trace has been found.

~X_3 = FIN(tls12_prf(tls12_prf(zero,master_secret,(~M_16693, ~M_16834)),server_finished,((((CH(~M_16693,a_16478), SH(~M_16834,nego(TLS12,RSA(a_16479),a_16480,a_16481, a_16482))),CRT(~M_17151)),CCS(change_cipher_spec)), CKE(rsa_enc(~M_17151,zero))),FIN(tls12_prf(tls12_prf(zero,master_secret,(~M_16693,~M_16834)),client_finished, (~M_16693,~M_16834)))))) = FIN(tls12_prf(tls12_prf(zero,master_secret,(cr_16484,sr_16485)),server_finished, ((((CH(cr_16484,a_16478),SH(sr_16485,nego(TLS12, RSA(a_16479),a_16480,a_16481,a_16482))),CRT(pk(k_16486))),CCS(change_cipher_spec)),CKE(rsa_enc(pk(k_16486),zero))),FIN(tls12_prf(tls12_prf(zero,master_secret,(cr_16484,sr_16485)),client_finished,

(cr_16484,sr_16485))))))

Attacker

Beginning of process Client12 Beginning of process longTermKeys Beginning of process longTermKeys Beginning of process sameSessionAuth {2}new cr_16484 Beginning of process Server12 [75] event WeakOrCompromisedKey(NoPubKey) [75] event WeakOrCompromisedKey(NoPubKey) a_16478 $CH(\sim M_16693,\sim M_16694) \models CH(cr_16484,a_16478)$ $CH(\sim M_16693, a_16471) = CH(cr_16484, a_16471)$ SH(a_1647),nego(TLS12,RSA(StrongRSADecryption), a_16467,a_16468,a_16469)) {36}new sr_16485 SH(~M_16834,nego(~M_16836,RSA(~M_16841),~M_16838, ~M_16839,~M_16840)) a_16475 {77}new k_16487 [78] insert longTermKeys_tbl(a_16475,k_16487,pk(\sim M_169 $56 = pk(k_16487)$ {64}get longTermKeys_tbl(a_16475,k_16487,pk(k_16487)) $CRT(\sim M_16980) = CRT(pk(k_16487))$ CCS(a_16477) $CKE(rsa_enc(\sim M_16956, zero)) = CKE(rsa_enc(pk(k_16487),$ \sim M_17083 = zero ~X_2 $FIN(\sim M_17132) = FIN(tls12_prf(tls12_prf(zero,master_secret,$ (cr_16484,sr_16485)),server_finished,(cr_16484, sr_16485))) $FIN(\sim M_17144) = FIN(tls12_prf(tls12_prf(zero,master_secret,$ (cr_16484,sr_16485)),server_finished,(cr_16484, sr_16485))) {57}insert serverSession(cr_16484,sr_16485,NoPSK, pk(k_16487),a_16471,nego(TLS12,RSA(StrongRSADecryption), a_16467,a_16468,a_16469),b2ae(tls12_prf(tls12_prf(zero,master_secret,(cr_16484,sr_16485)),client_key_expansion, (sr_16485,cr_16484))),b2ae(tls12_prf(tls12_prf(zero,master_secret,(cr_16484,sr_16485)),server_key_expansion, (sr_16485,cr_16484))),tls12_prf(tls12_prf(zero,master_secret,(cr_16484,sr_16485)),client_finished, (cr_16484,sr_16485)),tls12_prf(zero,master_secret, (cr_16484,sr_16485))) {77}new k_16486 {78}insert longTermKeys_tbl(a_16473,k_16486,pk(k_16486)) \sim M_17151 \(\delta\) pk(k_16486) $CRT(\sim M_17151) = CRT(pk(k_16486))$ {30}get longTermKeys_tbl(a_16473,k_16486,pk(k_16486)) $CCS(\sim M_17202) = CCS(change_cipher_spec)$ $CKE(\sim M_17248) = CKE(rsa_enc(pk(k_16486), zero))$ $FIN(\sim M_17266) = FIN(tls12_prf(tls12_prf(zero,master_secret,$ (cr_16484,sr_16485)),client_finished,(cr_16484, sr_16485))) $\sim X_3$ {25}insert clientSession(cr_16484,sr_16485,NoPSK, pk(k_16486),a_16478,nego(TLS12,RSA(a_16479),a_16480, a_16481,a_16482),b2ae(tls12_prf(tls12_prf(zero, master_secret,(cr_16484,sr_16485)),client_key_expansion, (sr_16485,cr_16484))),b2ae(tls12_prf(tls12_prf(zero, master_secret,(cr_16484,sr_16485)),server_key_expansion, (sr_16485,cr_16484))),tls12_prf(tls12_prf(zero, master_secret,(cr_16484,sr_16485)),client_finished, (cr_16484,sr_16485)),tls12_prf(zero,master_secret, (cr_16484,sr_16485))) $CCS(\sim M_17293) = CCS(change_cipher_spec)$

Honest Process

{92}get clientSession(cr_16484,sr_16485,NoPSK, pk(k_16486),a_16478,nego(TLS12,RSA(a_16479),a_16480, a_16481,a_16482),b2ae(tls12_prf(tls12_prf(zero, master_secret,(cr_16484,sr_16485)),client_key_expansion, (sr_16485,cr_16484))),b2ae(tls12_prf(tls12_prf(zero,master_secret,(cr_16484,sr_16485)),server_key_expansion, (sr_16485,cr_16484))),tls12_prf(tls12_prf(zero, master_secret,(cr_16484,sr_16485)),client_finished, (cr_16484,sr_16485)),tls12_prf(zero,master_secret, (cr_16484,sr_16485)))

{91} get serverSession(cr_16484,sr_16485,NoPSK, pk(k_16487),a_16471,nego(TLS12,RSA(StrongRSADecryption), a_16467,a_16468,a_16469),b2ae(tls12_prf(tls12_prf(zero,master_secret,(cr_16484,sr_16485)),client_key_expansion, (sr_16485,cr_16484))),b2ae(tls12_prf(tls12_prf(zero,master_secret,(cr_16484,sr_16485)),server_key_expansion, (sr_16485,cr_16484))),tls12_prf(tls12_prf(zero,master_secret,(cr_16484,sr_16485)),client_finished, (cr_16484,sr_16485)),tls12_prf(zero,master_secret, (cr_16484,sr_16485)))