Abbreviations
~X_1 = FIN(tls12_prf(tls12_prf(zero,master_secret,(~M_24700, a_24549)),server_finished,(((((CH(~M_24700,a_24552), SH(a_24549,nego(TLS12,RSA(a_24553),a_24554,a_24555, a_24556))),CRT(~M_24807)),CCS(change_cipher_spec)), CKE(rsa_enc(~M_24807,zero))),FIN(tls12_prf(tls12_prf(zero,master_secret,(~M_24700,a_24549)),client_finished, (~M_24700,a_24549)))))) = FIN(tls12_prf(tls12_prf(zero,master_secret,(cr_24558,a_24549)),server_finished, (((((CH(cr_24558,a_24552),SH(a_24549,nego(TLS12, RSA(a_24553),a_24554,a_24555,a_24556))),CRT(pk(k_24559))),CCS(change_cipher_spec)),CKE(rsa_enc(pk(k_24559),zero))),FIN(tls12_prf(tls12_prf(zero, master_secret,(cr_24558,a_24549)),client_finished, (cr_24558,a_24549))))))
~X_2 = b2ae(tls12_prf(tls12_prf(zero,master_secret,(~M_24700, a_24549)),client_key_expansion,(a_24549,~M_24700))) = b2ae(tls12_prf(tls12_prf(zero,master_secret, (cr_24558,a_24549)),client_key_expansion,(a_24549, cr_24558)))

A trace has been found.

Honest Process

Attacker

Beginning of process Client12

{2}new cr_24558

Beginning of process secrecySessionKey

Beginning of process longTermKeys

{75}event WeakOrCompromisedKey(NoPubKey)

a_24552

CH(~M_24700,~M_24701) = CH(cr_24558,a_24552)

SH(a_24549,nego(TLS12,RSA(a_24553),a_24554,a_24555, a_24556))

a_24550

{77}new k_24559

{78}insert longTermKeys_tbl(a_24550,k_24559,pk(k_24559))

~M_24807 = pk(k_24559)

CRT(~M_24807) = CRT(pk(k_24559))

{30}get longTermKeys_tbl(a_24550,k_24559,pk(k_24559))

CCS(~M_24858) = CCS(change_cipher_spec)

CKE(~M_24904) = CKE(rsa_enc(pk(k_24559),zero))

FIN(~M_24922) = FIN(tls12_prf(tls12_prf(zero,master_secret, (cr_24558,a_24549)),client_finished,(cr_24558, a_24549)))

~X_1

{25}insert clientSession(cr_24558,a_24549,NoPSK, pk(k_24559),a_24552,nego(TLS12,RSA(a_24553),a_24554, a_24555,a_24556),b2ae(tls12_prf(tls12_prf(zero, master_secret,(cr_24558,a_24549)),client_key_expansion, (a_24549,cr_24558))),b2ae(tls12_prf(tls12_prf(zero,master_secret,(cr_24558,a_24549)),server_key_expansion, (a_24549,cr_24558))),tls12_prf(tls12_prf(zero, master_secret,(cr_24558,a_24549)),client_finished, (cr_24558,a_24549)),tls12_prf(zero,master_secret, (cr_24558,a_24549)))

CCS(~M_24949) = CCS(change_cipher_spec)

{69}get clientSession(cr_24558,a_24549,NoPSK,pk(k_24559),a_24552,nego(TLS12,RSA(a_24553),a_24554, a_24555,a_24556),b2ae(tls12_prf(tls12_prf(zero, master_secret,(cr_24558,a_24549)),client_key_expansion, (a_24549,cr_24558))),b2ae(tls12_prf(tls12_prf(zero,master_secret,(cr_24558,a_24549)),server_key_expansion, (a_24549,cr_24558))),tls12_prf(tls12_prf(zero, master_secret,(cr_24558,a_24549)),client_finished, (cr_24558,a_24549)),tls12_prf(zero,master_secret, (cr_24558,a_24549)))

~X_2

{68}event ClientAEKeyLeaked(TLS12,cr_24558,a_24549, NoPSK,pk(k_24559))