Extended Master Secret

Internet-Draft by:
K. Bhargavan, A. Delignat-Lavaud, A. Pironti, Inria Paris-Rocquencourt
A. Langley, Google Inc.
M. Ray, Microsoft Corp.
Triple Handshake Attack

• The TLS master secret is not cryptographically bound to the client and server identities.
• Consequently, it is possible for an active attacker to set up two sessions, one with a client and another with a server, such that the master secrets on the two sessions are the same.
• Thereafter, any mechanism that relies on the master secret for authentication, including TLS channel bindings [RFC5929], becomes vulnerable to a man-in-the-middle attack.
• Extended Master Secret I-D defines a TLS extension that binds the master secret to the log of the full handshake that computes it, preventing such attacks.
Changes in the Master Secret Computation

• Existing TLS master secret computation allows MITM to synchronize master secrets when RSA or DHE key exchange is used:

  \[
  \text{master\_secret} = \text{PRF(} \text{pre\_master\_secret, "master secret"}, \\
  \text{ClientHello.random + ServerHello.random)} [0..47];
  \]

• Proposed master secret computation:

  \[
  \text{master\_secret} = \text{PRF(} \text{pre\_master\_secret, "extended master secret"}, \\
  \text{session\_hash)} [0..47];
  \]

• The "session\_hash" depends upon a handshake log that includes "ClientHello.random" and "ServerHello.random", in addition to cipher suites, client and server certificates.
Negotiating the Use of Extended Master Secret

- This I-D defines a new TLS extension, "extended_master_secret", which is used to signal both client and server to use the extended master secret computation. The "extension_data" field of this extension is empty.

- To maximize backward compatibility, the I-D also defines a special Signaling Cipher Suite Value (SCSV) "TLS_EXTENDED_MASTER_SECRET".

- In its ClientHello message, a client MUST either send the "extended_master_secret" extension, or the "TLS_EXTENDED_MASTER_SECRET" SCSV.

- If a server receives either the "extended_master_secret" extension, or the "TLS_EXTENDED_MASTER_SECRET" SCSV, it MUST include the extended_master_secret extension in its ServerHello message.
Call for Action

• Triple Handshake attack is a published vulnerability in the TLS protocol.
• This vulnerability affects numerous deployed applications that depend on TLS channel bindings.
• Let’s consider adopting the Extended Master Secret I-D, or come up with a different mitigation.
Links and Contact Information


• Karthikeyan Bhargavan karthikeyan.bhargavan@inria.fr
• Antoine Delignat-Lavaud antoine.delignat-lavaud@inria.fr
• Alfredo Pironti alfredo.pironti@inria.fr
• Adam Langley agl@google.com
• Marsh Ray maray@microsoft.com