Deprecating Obsolete Key Exchange Methods in TLS

Carrick Bartle, Nimrod Aviram

TL;DR

- draft-aviram-tls-deprecate-obsolete-kex-01:
- ❌ RSA Key Exchange
- ❌ Static FFDH
- 👍 FFDHE: Only when fully ephemeral, with safe & well-known group >= 2048 bit.
- 👎 Static ECDH

In Previous Episodes…

- draft-bartle-tls-deprecate-ffdh-00:
  - ❌ Static FFDH
  - 👎 Static ECDH
  - 👍 FFDHE, when fully ephemeral
- draft-aviram-tls-deprecate-obsolete-kex-00:
  - ❌ RSA Key Exchange
  - 👍 FFDHE: Only in well-known group >= 2048 bit.

Is this practical? (YES!)

- Consistent with recommended configuration in Mozilla's Server Side TLS Guide (link)
- Compatible with nearly every [web] client released [since circa 2015]

Is this practical? (YES!)

- Consistent with recommended configuration in Mozilla's Server Side TLS Guide (link)
- Compatible with nearly every [web] client released [since circa 2015]
- Email Ecosystem may not be ready for this.
  - But email encryption possibly opportunistic [RFC7672].
- Previous discussion: Support for moving forward with deprecation.
  - IETF issues guidelines.
  - Market segments will apply new guidance at different rates (cf. PCI & RC4).
- Web is not isolated from problems in other ecosystems.

Cross-Protocol Attacks

- Cf. DROWN (2016 Bleichenbacher vuln.):
- 17% of web servers directly vulnerable.
- Additional 16% of web servers vulnerable because of key reuse, mostly from email servers.

Cross-Protocol Attacks

- Cf. DROWN (2016 Bleichenbacher vuln.):
- 17% of web servers directly vulnerable.
- Additional 16% of web servers vulnerable because of key reuse, mostly from email servers.
- DROWN allows signature forgery, so web clients with no RSA support would still be affected.
    - Attacker exploits DROWN against an email host to forge an RSA signature, then uses the signature to mount a MitM attack against web host.
- Other examples of cross-protocol attacks: Jager et al. 2015 [JSS15], “One Bad Apple” [JPS13], Mavrogiannopoulos et al. 2012 [MVVP12]...

Reminder: RSA Key Exchange = Attack Surface

- No Forward Secrecy
- RSA cipher suites already not recommended.
- New Bleichenbacher Attack every few years (ROBOT, DROWN, Usenix 2014)

Reminder: The Woes of FFDHE

- Discrete Log record: 795 bits.
  - So 1024 bit FFDHE is insecure. Draft requires >= 2048 bits.
  - Discrete Log computation is expensive per group. Once done, cheap per exponent.
- If not fully ephemeral: Raccoon Attack.
- With weird groups: Subgroup Attacks.

Why Not Static ECDH

- (Static ECDH merely a SHOULD NOT)
- No Forward Secrecy.
- Static ECDH cipher suites already not recommended.
- Secret reuse -> Potential for side-channel attacks.
    - E.g. Invalid Curve Attacks, PARIS256 attack.

Points from Mailing List Discussions

- We should deprecate RSA key exchange in parallel to limiting FFDHE parameters, lest people move from FFDHE to RSA -> done.
- Fully deprecate FFDHE?
  - The requirements in the draft should be enough to get security from FFDHE; FFDHE is not MTI. If someone needs it, and can operate it under these conditions, then fine (?)
- FFDHE only with safe, well-known groups:
  - Let’s take these points to the mailing list:
  - Treat built-in Postfix group as safe & well-known?
    - We lean towards safelisting it. If so, any other groups we might safelist?
  - Client MUST/SHOULD/MAY abort on other groups (of at least 2048 bits)?

TL;DR, again

- ❌ RSA Key Exchange
- ❌ Static FFDH
- 👍 FFDHE: Only when fully ephemeral, with safe & well-known group >= 2048 bit.
- 👎 Static ECDH

References

- DROWN: drownattack.com
- [JSS15]: Jager, Tibor, Jörg Schwenk, and Juraj Somorovsky. "On the security of TLS 1.3 and QUIC against weaknesses in PKCS# 1 v1. 5 encryption." CCS 2015.
- [JPS13]: Jager, Tibor, Kenneth G. Paterson, and Juraj Somorovsky. "One Bad Apple: Backwards Compatibility Attacks on State-of-the-Art Cryptography." NDSS 2013.
- [MVVP12]: Mavrogiannopoulos, Nikos, et al. "A cross-protocol attack on the TLS protocol." CCS 2012.