Prohibiting RC4 Cipher Suites in TLS

http://datatracker.ietf.org/doc/draft-popov-tls-prohibiting-rc4

By: Andrei Popov andreipo@microsoft.com

RC4 is Popular

- Been around since 1987.
- High performance (7 cycles per byte on Pentium).
- Stream cipher: immune to BEAST attack on TLS1.0.
- As a result, ~90% of HTTPS sites surveyed by trustworthyinternet.org support some RC4 cipher suites.
- The popularity of RC4 on the server side prevents browser vendors from disabling this cipher.

RC4 is Insecure

- For over a decade, RC4 was known to have biases in the keystream:
  - Fluhrer, S., Mantin, I., and A. Shamir, "Weaknesses in the Key Scheduling Algorithm of RC4. Selected Areas in Cryptography, pp. 1-24", 2001.
  - Mantin, I. and A. Shamir, "A Practical Attack on Broadcast RC4. FSE, pp. 152-164.", 2001.
  - Paul, G. and S. Maitra, "Permutation after RC4 Key Scheduling Reveals the Secret Key. In Proceedings of the 14th Workshop on Selected Areas in Cryptography (SAC), pp. 360-377, vol. 4876, LNCS, Springer.", 2007.
- Recent cryptanalysis results exploit biases in the RC4 keystream to recover repeatedly encrypted plaintexts:
  - AlFardan, N., Bernstein, D., Paterson, K., Poettering, B., and J. Schuldt, "On the security of RC4 in TLS and WPA. USENIX Security Symposium.", 2013.

Applicability of Attacks to HTTPS

- The latest known attacks are on the verge of becoming practically exploitable. Currently they require 2^26 sessions or 13x2^30 encryptions.
- The attacker causes a browser to transmit many HTTP requests. Each request contains the same secret (cookie). Known biases in RC4 are used to recover plaintext.
- The attacker does not need to be located close to the server, and no packet injection capability is required.
- It suffices for the attacker to record encrypted traffic for later offline analysis.

Prohibiting RC4 Cipher Suites

- TLS clients MUST NOT include RC4 cipher suites in the ClientHello message.
- TLS servers MUST NOT select an RC4 cipher suite when a TLS client sends such a cipher suite in the ClientHello message.
- If the TLS client only offers RC4 cipher suites, the TLS server MUST terminate the handshake. The TLS server MAY send the insufficient_security fatal alert in this case.

Links and Contact Information

- AlFardan, N., Bernstein, D., Paterson, K., Poettering, B., and J. Schuldt, "On the security of RC4 in TLS and WPA. USENIX Security Symposium.", 2013, https://www.usenix.org /conference/usenixsecurity13/security-rc4-tls
- Prohibiting RC4 Internet-Draft: http://datatracker.ietf.org/doc/draft-popov-tls-prohibiting-rc4
- Andrei Popov andreipo@microsoft.com