TLS Attacks and TLS BCP Drafts

draft-ietf-uta-tls-attacks-01
draft-ietf-uta-tls-bcp-01

Peter Saint-Andre
Ralph Holz
Yaron Sheffer (presenting remotely)

IETF-90, Toronto

TLS Attacks

- Latest revision:
  - Added SSL Stripping, attacks related to certificates, Diffie Hellman parameters and denial of service
  - Expanded on RC4 attacks
- Next revision:
  - New text from Kohei re: mitigation of Lucky 13 attack
  - Mention Renegotiation and Triple Handshake

TLS BCP: Last Revision

- Clarified that specific TLS-using protocols may have stricter requirements
- Changed TLS 1.0 from MAY to SHOULD NOT
  - But may still fallback to TLS 1.0 (unfortunately)
- Added discussion of "optional TLS" and HSTS
- Recommended use of the Signature Algorithm and Renegotiation Info extensions
- Use of a strong cipher for a resumption ticket: changed SHOULD to MUST
- Added an informational discussion of certificate revocation, but no recommendations

TLS BCP: Next Revision

- Remove missing reference to IP scans
- Review Sec. 3.4 and 4.1, eliminate overlap and possibly restructure
- Add recommendation to implement SNI
  - But not a recommendation to deploy it → local policy
- Add recommendation to implement RFC 4492 extensions (ECDH)
- “Implementations MUST NOT negotiate cipher suites with an effective key length of less than 112 bits”
- Triple Handshake mitigation

Opens: 128-bit vs. 256-bit Ciphers

- Wording around 128-bit and 256-bit cipher suites
  - Current should-implement cipher suites are:
    - TLS_DHE_RSA_WITH_**AES_128**_GCM_SHA256
    - TLS_ECDHE_RSA_WITH_**AES_128**_GCM_SHA256
    - TLS_DHE_RSA_WITH_**AES_256**_GCM_SHA384
    - TLS_ECDHE_RSA_WITH_**AES_256**_GCM_SHA384
- Current text is vague: “Implementations SHOULD prefer cipher suites that use algorithms with **at least 128 (and, if possible, 256)** bits of security”
- Propose to remove this text. Offer both 128-bit and 256-bit for interop, which to “prefer” should be left to local policy

Opens: Fallback to Earlier Versions

- Currently: Fallback to TLS 1.0 but not to SSLv3
- We must allow fallback because TLS 1.0 is still very common
  - Secure fallback solutions are still not there
- Some criticism because the protocols are similar
- But there are in fact differences, including support for extensions which is critical
- Propose to keep as-is

Opens: Mention Other Bad Practices

- Proposal to mention a few things that are deemed insecure:
  - Anonymous cipher suites, MD5, static DH
- My view: should mandate against bad things that are widely implemented, such as RC4
- Question to WG: are any of the above widely implemented?


Thank You!