Cipher-suites in SIP draft-srivastava-sip-e2e-ciphersuites-00.txt

Samir Srivastava
Nortel Networks
samirsr@nortel.com

Acknowledgement

Thanks to Eric Rescorla, Rajnish Jain, Vijay Gurbani, Mike Hammer, Dave Oran and Francois Audet for contributing in this effort.

Problem Statement

> Level Of Security (Encryption, digest etc) is missing.

> Should we cleanup the mess of the SIPS also ?

> Should DTLS be considered also ?

Proposed Solution

1) Extend via to include Cipher-suites etc.

2) Define a header for UAC desired cipher-suites, secure protocol etc.

3) Define reverse channel for UAC to know the level of security applied in the path.

4) Define tags for Proxy-Require / Require to enforce UAC desired cipher-suites.

Alternate (Eric’s) Solution

1) Instead of using a separate header for cipher-suites, let TLS layer take care of cipher-suites from the intersection of offered and supported cipher-suites at each hop.

2) Relies on the mandatory cipher-suites as a common denominator to complete the call.

3) Proxies are trusted for upgrade /downgrade of mandatory cipher-suites.

Reasons for New Header

1. UAC has complete control over ciphers. Proxies cannot upgrade/downgrade ciphers at their own, unless two adjacent proxies collaborate. Evil proxy caught much earlier.

2. If UAC wants to have cipher-suites A,B,M in the order of preference, where M is mandatory cipher-suite.

   Then Proxies might end up using cipher-suite M, even if B is supported on the hop.

Reasons for New Header (Contd)

3. Proxy doing TLS to DTLS conversion need to know ciphers for other protocol. (Currently RC4 is not applicable to DTLS) Or SIP needs to define same set of mandatory cipher-suites for DTLS and TLS.

4. This is future proof. Mandatory cipher-suites changed earlier. What is the future of AES ?

OPEN ISSUES

1) Which solution to pick ?

2) Should we adopt it partially with SIPS ?

3) Impact of renegotiation of cipher-suites needs to be analyzed ?