Deprecating MD5 for LDP
draft-nslag-mpls-deprecate-md5-04

Loa Andersson
Stewart Bryant
Andy Malis
Nic Leymann
George Swallow

IETF 104

Some History

- RFC 3036 (LDP) was published in January 2001
- Replaced by RFC 5036 in October 2007
- Both specified the use of the TCP MD5 Signature Option for authenticity and integrity of LDP messages, to prevent against spoofing
- As far back as 1998, the IETF was aware of problems with MD5 (see RFC 2385, for example)
- RFC 5925 (June 2010) deprecated the TCP MD5 Signature option and replaced it with the TCP Authentication Option (TCP-AO)
  - Cryptographic algorithms specified separately (RFC 5926) to allow them to be easily updated
- RFC 6952 (May 2013) recommended that TCP-based routing protocols move from MD5 to TCP-AO
- RFC 7454 (February 2015) specified the use of TCP-AO with BGP
  - But did not specify which cryptographic algorithm to use
- However, LDP continues to use MD5

draft-nslag-mpls-deprecate-md5

- Goal is to update LDP to also replace MD5 with TCP-AO
- However, the authors are LDP experts, not security experts, and thus have some questions
  - How successful has TCP-AO been for BGP? Is it in use in the field?
  - Which crypto algorithm should be chosen as the default? We would want one that is reasonably better than MD5 (otherwise, why bother), but can be implemented on a typical router processor, and which will provide adequate security without significantly degrading the convergence time of an LSR
  - Does anyone really care? Does anyone currently use LDP with MD5?
- We’re looking for advice on how to go forward