A new Request for Comments is now available in online RFC libraries.

RFC 3562

Title: Key Management Considerations for the TCP MD5 Signature Option
Author(s): M. Leech
Status: Informational
Date: July 2003
Mailbox: mleech@nortelnetworks.com
Pages: 7
Characters: 14965
Updates/Obsoletes/SeeAlso: None

I-D Tag: draft-ietf-idr-md5-keys-00.txt

URL: ftp://ftp.rfc-editor.org/in-notes/rfc3562.txt

The TCP MD5 Signature Option (RFC 2385), used predominantly by BGP, has seen significant deployment in critical areas of Internet infrastructure. The security of this option relies heavily on the quality of the keying material used to compute the MD5 signature. This document addresses the security requirements of that keying material.

This document is a product of the Inter-Domain Routing Working Group of the IETF.

This memo provides information for the Internet community. It does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

This announcement is sent to the IETF list and the RFC-DIST list. Requests to be added to or deleted from the IETF distribution list should be sent to IETF-REQUEST@IETF.ORG. Requests to be added to or deleted from the RFC-DIST distribution list should be sent to RFC-DIST-REQUEST@RFC-EDITOR.ORG.

Details on obtaining RFCs via FTP or EMAIL may be obtained by sending an EMAIL message to rfc-info@RFC-EDITOR.ORG with the message body help: ways_to_get_rfcs. For example:

To: rfc-info@RFC-EDITOR.ORG
Subject: getting rfcs

help: ways_to_get_rfcs

Requests for special distribution should be addressed to either the author of the RFC in question, or to RFC-Manager@RFC-EDITOR.ORG. Unless specifically noted otherwise on the RFC itself, all RFCs are for

unlimited distribution.echo
Submissions for Requests for Comments should be sent to
RFC-EDITOR@RFC-EDITOR.ORG. Please consult RFC 2223, Instructions to RFC
Authors, for further information.