

Abstract

MEMO: A Hybrid Approach to Encrypted
Electronic Mail

B. P. Schanning
J. Kowalchuk
The MITRE Corporation
Bedford, MA 01730

This presentation will report on recent work performed at The MITRE Corporation aimed at developing a secure electronic mail system suitable for distributing unclassified, yet sensitive, correspondence on the MITRENET broadband local area communication network.

Exploiting the Diffie-Hellman discrete exponential algorithm for public key distribution and the DES algorithm for data encryption, all data is protected while transiting the cable network. In addition, all data stored locally on tape cartridges or centrally on a PDP-11/23 host is fully encrypted.