Electrical Engineering DepartmentUniversity of Delaware
Technical Report 96-10-3 October 1996

Proposed Authentication Enhancements for the Network Time Protocol Version 4

David L. Mills

Abstract

This report describes proposed changes in the security model and authentication scheme for the Network Time Protocol Version 4, which is an enhanced version of the current Versing 3. The changes are intended to replace the need to securely distribute cryptographic keys in advance, while protecting against replay and man-in-the-middle attacks. As in other schemes described in the literature, the proposed scheme is based on the use of a public-key cryptosystem to verify a server secret and from this to generate session keys for each client separately. A particularly important consequence of this design in the case of NTP is that the mechanisms for time synchronization and cryptographic signature verification must be decoupled to preserving good timekeeping quality. The schemes to do this are the main body of this report, which also includes an extensive analysis of the vulnerabilities to various kinds of hardware and software failures, as well as hostile attack.

Keywords: computer network security, public-key cryptosystem, multicasting, anycasting.

Sponsored by: DARPA Information Technology Office Contract DABT 63-95-C-0046, NSF Division of Network and Communications Research and Infrastructure Grant NCR 93-01002, Northeastern Center for Electrical Engineering Education Contract A3036-92 619 43093, Army Research Laboratories Cooperative Agreement DAA L01-96-2-002, and Digital Equipment Corporation Research Agreement 1417.

Table of Contents

List of Figures