

Electrical Engineering Department University 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 Version 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

1.	Introduction.....	1
2.	NTP Security Model and Authentication Scheme	2
2.1	Protocol Modes of Operation	2
2.2	Security Model	3
2.3	Authentication Scheme	6
2.4	Server Discovery Schemes	7
3.	Design Issues	8
3.1	On Interactions Between Synchronization and Key Lifetimes	9
3.2	On Public-Key and Private-Key Cryptography	10
3.3	On Interactions Between Time, Keys and Certificates.....	14
4.	Extensions to the NTP Security Model and Authentication Scheme	15
4.1	Secure Network Services - DNS and RPC.....	17
4.2	Authentication in Symmetric (Peer-peer) Modes.....	18
4.3	Authentication in Client-server Modes	18
4.4	Authentication in Multicast Modes	19
5.	Protocol Security Analysis.....	20
5.1	Goals of the Intruder	21
5.2	Attacks on the Cryptosystem.....	22
5.3	Replay Attacks and Spoofing.....	23
5.4	Man-In-the-Middle Attacks.....	24
5.5	Clogging Attacks (Denial of Service)	25
5.6	Attacks on Specific NTP Protocol Fields.....	27
6.	Hardware and Software Fault Vulnerabilities	30
6.1	Vulnerabilities to Broken Hardware	30
6.2	Vulnerabilities to Interrupt Latencies	31
6.3	Vulnerabilities in the Clock Discipline Process	32
6.4	On Dealing with the Monotonic Requirement	33
6.5	Irregularities in Leap Second Processing	35
7.	Summary and Conclusions	35
8.	Bibliography and References.....	36

List of Figures

Figure 1.	RSA Key Pair Generation	11
Figure 2.	MD5 Hash Algorithm	12
Figure 3.	MD5/RSA Sign Algorithm	12
Figure 4.	MD5/RSA Verify Algorithm.....	13
Figure 5.	NTP Message Format	16
Figure 6.	Multicast Authentication.....	19