Electrical Engineering DepartmentUniversity of Delaware
Technical Report 00-5-1 May 2000

Public Key Cryptography for the Network Time Protocol

David L. Mills

Abstract

This report describes a scheme for authenticating servers to clients for the Network Time Protocol. It extends prior schemes based on symmetric-key cryptography to a new scheme based on public-key cryptography. The new scheme, called Autokey, is based on the premise that the IPSEC schemes proposed by the IETF cannot be adopted intact, since that would preclude stateless servers and severely compromise synchronization accuracy. In addition, the IPSEC model presumes timestamps are always available using authenticated means; however, the authentic timestamps requires interaction between the timekeeping function and authentication function in ways not yet considered in the IPSEC model.

The main body of the report contains a description of the security model, approach rationale, protocol design and vulnerability analysis. A detailed description of the protocol states, events and transition functions is included. Detailed packet formats and field descriptions are given in the appendices along with a model for key generation and public values distribution. A prototype of the Autokey scheme conforming to this document has been implemented, tested and documented in the NTP Version 4 software distribution for Unix, Windows and VMS.

Keywords: network security, public-key infrastructure, digital signatures, computer time synchronization

Sponsored by: DARPA Information Technology Office Order G409, Contract F30602-98-1-0225, and Digital Equipment Corporation Research Agreement 1417.

Table of Contents

1. Introduction........1
2. Security Model........1
3. Approach........3
4. Autokey Authentication Scheme........3
4.1 Public-Key Signatures........6
4.2 Error Recovery........7
4.3 Autokey Protocols........8
4.3.1 Client/Server Modes (3/4)........9
4.3.2 Multicast/Manycast Mode (5)........10
4.3.3 Symmetric Active/Passive Mode (1/2)........11
5. Security Analysis........13
5.1 Specific Attacks........14
6. Present Status........15
7. Future Plans........15
8. References........16
9. Appendix A. Packet Formats........17
9.1 Public Key (1)........19
9.2 Association ID (2)........19
9.3 Cookie (3)........20
9.4 Autokey (4)........20
9.5 Public Value (5)........21
9.6 Host Name (6)........22
10. Appendix B. Public Key Distribution and Management........23

List of Figures

Figure 1. Autokey Format........4
Figure 2. Client/Server Protocol........9
Figure 3. Multicast/Manycast Protocol........10
Figure 4. Symmetric Mode Protocol........12
Figure 5. NTP Packet Header........17
Figure 6. Extension Field Format........18
Figure 7. Request Message Format........19
Figure 8. Public Key Response Message Format........19
Figure 9. Association ID Response Message Format........20
Figure 10. Cookie Response Message Format........20
Figure 11. Autokey Response Message Format........21
Figure 12. Public Value Response Message Format........21

Figure 13. Host Name Response Message Format..22