Scalable, High Speed, Internet Time Synchronization

Advanced Research Projects Agency
Contract DABT 63-95-C-0046

Quarterly Progress Report
1 September 1996 - 30 November 1996

David L. Mills
Electrical Engineering Department
University of Delaware

1. Introduction

This report covers the work done in support of the DARPA Information Technology Office program in computer networking. Contributors to this effort include Prof. David L. Mills and graduate students Ajit Thyagarajan and Bradley Cain. The project continues previous research in network time synchronization technology jointly funded by DARPA, NSF, US Navy and US Army. The technology makes use of the Network Time Protocol (NTP), widely used in the Internet, together with engineered modifications designed to improve accuracy in high speed networks, including SONET and ATM, expected to be widely deployed in the next several years. Specific applications benefiting from this research include multicast topologies, multimedia, real-time conferencing, cryptographic systems, and management of distributed, real-time experiments.

Recent projects reported in papers, technical reports, project reports and technical memoranda include advances in precision timekeeping technology, improved clock discipline algorithms, and engineered security models and protocols for scalable, distributed server systems. Past projects include a relatively inexpensive precision timing receiver using the LORAN-C radionavigation system, and an optimum matched-filter receiver/decoder using DSP technology. Software developed with joint funding includes the NTP Version 3 implementation for Unix and Windows and a set of precision-time kernel modifications for major Unix workstation manufacturers. Finally, the joint projects involve the conduct of experiments designed to evaluate the success of the research and assist technology transfer to computer manufacturers and network providers.

2. Present Status

Most of the effort during the quarter was concentrated on the analysis, and design and implementation of the security model and authentication scheme described in previous project reports and technical reports. A summary of the progress in this area during the quarter is as follows:

2.1 Network Time Protocol (NTP) Version 4

Work continued on the adaptation of the software distribution of the NTP daemon for Unix and Windows to the GNU Autoconfigure system. The goal of this effort is to align the configuration features of the distribution to other packages intended for multiple platforms. Previously, there have been occasional intricate and elusive bugs due to various porting problems. With GNU Autoconfigure, much of the special tailoring required for the over two-dozen architectures and operating systems supported is handled automatically in one place.

Work continued on the autoconfigure scheme proposed for NTP and the subject of a pending dissertation by Mr. Ajit Thyagarajan. The design revisions to the association-management algorithms for unicast, multicast and anycast modes has been completed and documented in the form of an annotated state diagram. Besides providing guidance for specification and implementation, it corrects certain anomalies in the existing NTP Version 3 specification and implementation.

The proposed NTP Version 4 authentication scheme is described in [], along with a comprehensive security analysis. A paper describing its main features appeared in the ATIRP 97 Conference [] and a briefing on it and other aspects of the project was given at the DARPA/ITO Principal Investigator's Meeting. Most details of the implementation have been worked out, including the data structures and cryptographic algorithms. The initial suite of cryptographic algorithms to be used is based on the RSA-DSI library; however, the cryptographic algorithms themselves will not be included in the public distribution, other than the MD5 keyed-hash algorithm, which has been included in the distribution for the last several years. We expect implementation to begin in earnest beginning in June. Further information on this project, including a status report and set of briefing slides, is on the web at http://www.eecis.udel.edu/~mills/authentic.html.

2.2 Collaboration Projects

The CAIRN collaboration has suffered a slow start, both due to the press of current projects at UCL, SAIC and U Delaware, as well as plans for the SAIC hardware connection at Washington, DC. The U Delaware near-term plans and status report has been supplied as requested by the DARTnet/CAIRN directorate. A status report and set of briefing slides is on the web at http://www.eecis.udel.edu/~mills/status.html.

A third NTP primary server has been installed at ISI for DARTnet/CAIRN service. The other two primary servers are at LBL and U Delaware, all synchronized by GPS. Provision of three primary servers with interlocking configurations allow clients to discover misbehaving servers and vote them out of service. Not all DARTnet and CAIRN sites are members of the NTP synchronization subnet at this time. Further study has been deferred until NTP Version 4, with its automatic configuration capability, comes online.

2.3 Infrastructure

Repairs and upgrades of the research infrastructure continue to be a significant demand on quality research time. The resources to fix things that break, upgrade operating systems and maintain hardware are very few. With respect to Sun hardware and software, this has not been a problem, since the department has a laboratory and staff to maintain standard configurations. With respect to the Digital Alpha, Hewlett Packard and Intel workstations, repairs and upgrades must be done by the principal investigator and students. During the quarter, a new Windows 95 system was installed and another was upgraded. The Digital and HP machines were reconfigured and additional operating system components were installed. One of our three HP cesium clocks was refurbished and backup batteries installed. A major problem, so far not completely resolved, is the harmonization of the Unix and Windows networking systems, including mounted file system and printer support.

2.4 Meetings

A meeting of the End-to-End Research Group was held in November 1996 using DARTnet teleconferencing facilities.

3. Plans for the Next Quarter

Our plans for the next quarter include continued development of the NTP Version 4 protocol model, specification and implementation. Specifically, we plan to begin implementation of the new authentication scheme and integration with the current NTP Version 3 daemon for Unix and Windows. The daemon is to be tested first in the research net, then the DARTnet/CAIRN community. As the extensions are backwards compatible, the new features can be activated and tested in regular operation without impacting current users.

We plan to complete the design and implementation of the new autonomous configuration scheme, as well as the theoretical analysis, simulation and experimental justification of the scheme, as represented by Mr. Thyagajan's dissertation.

4. Publications

Mills, D.L. Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI. Network Working Group Report RFC-2030, University of Delaware, October 1996, 14 pp. Also published in PostScript: Ibid. Electrical Engineering Report 96-10-2, University of Delaware, October 1996, 14 pp. URL: see http://www.eecis.udel.edu/~mills/reports.html.

> Abstract
>
> This report describes the Simple Network Time Protocol (SNTP) Version 4, which is an adaptation of the Network Time Protocol (NTP) used to synchronize computer clocks in the Internet. SNTP can be used when the ultimate performance of the full NTP implementation described in RFC-1305 is not needed or justified. This report obsoletes RFC-1769, which describes SNTP Version 3. Its purpose is to correct certain inconsistencies in the previous document and to clarify header formats and protocol operations for current NTP Version 3 (IPv4) and proposed NTP Version 4 (IPv6 and OSI), which are also used for SNTP.

Mills, D.L. Proposed Authentication Enhancements for the Network Time Protocol Version 4. Electrical Engineering Report 96-10-3, University of Delaware, October 1996, 37 pp. URL: see http://www.eecis.udel.edu/~mills/reports.html.

> 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.

[Note: This report was originally submitted as an RFC in ASCII format to the RFC Editor. As there are a number of figures in the document which cannot be rendered in ASCII, the PostScript version must be considered the definitive one and would ordinarily be published as an RFC in PostScript format. However, current procedures require RFCs in PostScript format must be identical to the ASCII version, except for minor formatting differences. It was eventually concluded that the ASCII version could result in substantial misinterpretation of the algorithms, so the submission was withdrawn. This should result in no loss of availability, since the PostScript version is easily accessable on the web.]