Survivable, Real Time Network Services

Defense Advanced Research Projects Agency
Contract F30602-98-1-0225, DARPA Order G409/J175

Quarterly Progress Report
1 April 2000 - 30 June2000

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 Qoing Li and Tamal Basu. The project continues previous research in network time synchronization technology jointly funded by DARPA and US Navy. 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. Specific applications benefiting from this research include multicast topologies, multimedia, real-time conferencing, cryptographic systems, and management of distributed, real-time systems.

This quarterly report is submitted in traditional report form on paper. As the transition to web-based information dissemination of research results continues, almost all status information and progress reporting is now on the web, either on pages belonging to the principal investigator or to his students. Accordingly, this and future progress reports will contain primarily schedule and milestone data; current status and research results are reported on web pages at www.eecis.udel.edu/~mills in the form of papers, technical reports and specific briefings.

2. Autokey

The main focus of work during the last quarter continued to be the implementation, test and deployment of the Autokey public-key cryptographic authentication scheme in NTP Version 4. The Autokey protocol design is summarized on the web status page and briefing slides at www.eecis.udel.edu/~mills/autokey.htm. These documents have been updated to the current state of the security model and authentication scheme. As of late March, the Autokey design had been implemented, tested and deployed at selected sites in CAIRN. There were several unanticipated problems in this deployment which were discussed in the last quarterly progress report.

The most significant problem in the deployment was the need to distribute public keys and agreement parameters in advance. In the scheme first deployed, the private and public values were generated on each server separately and then the public values were transmitted to all clients using conventional file transfer services. When a client discovered a server, the client searched for the matching public key and, if found, validated the server. In a large network where clients are discovering servers and changing allegiances all the time, this is silly.

Accordingly, the autokey protocol was redesigned so that the public values could be retrieved as an integral function of the protocol. However, this feature widens the knotholes that could be exploited by an intruder. A good deal of time was spent recrafting protocol details, in particular the intricate details on how to timestamp various quantities and order the checking and signature computations to harden the client and server against an attack on cryptographic clogging. A series of tests was conducted using local servers and clients, as well as the core routers in the CAIRN testbed. The core routers are equipped with GPS radios and nanosecond kernels, so extremely precise time determinations can be made in order to calibrate the that might be introduced by the cryptographic operations.

The situation in late June is that the cycle of analyzing possible security vulnerabilities, especially in replay and clogging attacks on the public-key infrastructure of the protocol is winding down. A set of assertions has been developed and documented that have narrowed the attack space vulnerabilities to small and well known boundaries. It does not seem possible to eliminate the vulnerability space completely, since to do so makes the protocol very unresponsive when keying material is refreshed. However, what space that does remain is in the initial acquisition of the cryptographic values such as public key, host name and agreement parameters. Once these have been acquired and the protocol states completed to the point the authentic bit is set, the protocol is extremely hard to jam.

One of the things added in the latest protocol enhancement was the use of filestamps. Cryptographic keys and agreement parameters are generated in the form of files that are later loaded by the running protocol or transported over the network. It is necessary to reliably order the generated versions, since the files are regularly regenerated and old data deprecated by new data. For convenience, it is desirable that the generation identifier of each file be available without scanning its contents. The solution is to append the seconds value of the NTP timestamp at the time of creation. When the file is loaded, the fielstamp is parsed and attached to the data. Thereafter, as the data is distributed on request to other clients and peers, the filestamp follows the data. In addition, a timestamp is captured at the time the data are signed, in order to deflect replay attacks.

The filestamps and timestamps serve as a partial order relation in order to securely establish the validity of timestamped data and the original files from which the data derives. This makes it very difficult to attack the network by topological cut-and-paste, for instance. It also makes it very difficult to attack the key generation process by replaying old public keys, for example

In order to provide a basis for discussion and to pin down the security model assumptions and assertions, a technical report on the initial autokey protocol and algorithms has been prepared. The process of eventually standardizing version 1 of the protocol has begun with the production of an Internet Draft, which has been submitted to the IETF for discussion and comment. The document includes a semiformal description of the protocol state machine, transition functions and state variables. It also contains a discussion of the security model and protocol variations, called dances, that apply in each of the NTP association modes. While developed and first applied to NTP, there seems to be no reason why the same technology could be applied to other protocols where the autokey PDU is piggybacked on an existing protocol. The DNS protocols come immediately to mind.

2.1 Future Plans

The latest enhancements of the autokey protocol and algorithms provide for a completely automatic generation, transmission, installation and validation of public keys and agreement parameters. However, there are unique public keys for each server in the network and they are never reused. On the other hand, agreement parameters (and the leapsecond table) are common to all servers and clients. Currently, a set of Diffie-Hellman parameters is generated each time the key generation program is run, but only one set must be distributed in the network. The same is true for the leapsecond table, but that table is generated by NIST and distributed from their NTP and FTP servers. For completely automatic version management, a distributed protocol is needed to disseminate these data while insuring only the latest filestamps survive and all older data reliably deprecated.

Candidate algorithms that can be used to perform this function are known and can be incorporated in the protocol. However, this is a relatively low priority task at this time due to a more pressing need to move on to the autoconfigure issues. The state of the autoconfigure algorithms is currently near deployable status, but crucial components need to be implemented. The most important component is a mechanism to prevent implosion when a number of servers receive a manycast request from a client. The present plan is to use a p-persistence algorithm with properties similar to the algorithms sometimes used in slotted-Aloha networks. Work on this approach is to continue during the next quarter.

3. Infrastructure

The CAIRN core routers have been upgraded to FreeBSD 3.4 with nanokernel support and the API interface defined in a recent RFC. The latest NTPv4 software with autokey has been deployed and a suitable peering configuration established. As configured, the system has six mutually independent peers, which should provide for one Byzantine failure plus two fail-stop failures. In other words, even if one radio turns Albanian (two-faced clock) and two routers fail-stop, a sufficient number of radios/routers remain to elect an authentic source. Since NTP symmetric modes are used throughout, the flow of synchronization is bidirectional, depending on the best source (smallest synchronization distance) remaining.

There are a few other NTPv4 stories in the infrastructure news. One is that NIST has begun to convert their public time servers to NTPv4, including the autokey and leapsecond table functions. In fact, NIST has adopted the same filestamp convention used in autokey, which means that soon any NTP server running on the UTC timescale can in principle run on atomic time (TAI) as well. This will please the folks at the Canadian Metrology office, who have requested the feature.

It has been observed over the years that deploying NTP over the globe has something of the thrill of an amateur radio operator working Pitcairn Island for the first time. At first the goal was to deploy the NTP subnet throughout the US and then western Europe. That accomplished, the next goal was to avoid the Sun ever setting on NTP and then to avoid even getting close to the horizon. That accomplished, the next goal was to deploy on every continent and the Pacific Rim, South America and Africa have followed. We have needed the last continent.

Antarctica has now been heard from. We how move on to the Interplanetary Internet.

4. Publications

All publications, including journal articles, symposium papers, technical reports and memoranda are now on the web at www.eecis.udel.edu/~mills. Links to the several publication lists are available on that page, as well as links to all project descriptions, status reports and briefings. All publications are available in PostScript and PDF formats. Briefings are available in HTML, PostScript, PDF and PowerPoint. The project descriptions are cross-indexed so that the various interrelationships are clearly evident. Also included are the documentation pages for various public software distributions. Links to other related projects at Delaware and elsewhere are also included on the various pages. Hopefully, the organization of these pages, which amount to a total of about 300 megabytes of information pages and reference documents, will allow quick access to the latest results and project status in a timely way.

Following is a retrospective list of papers and reports supported wholly or in part on this project and the immediately preceding project “Scalable, High Speed, Internet Time Synchronization,” DARPA Order D012. The complete text of all papers and reports, as well as project briefings, status reports and supporting materials is at www.eecis.udel.edu/~mills.

4.1 Papers

1. Mills, D.L. Cryptographic authentication for real-time network protocols. In: *AMS DIMACS Series in Discrete Mathematics and Theoretical Computer Science, Vol. 45* (1999), 135-144.

2. Mills, D.L. Adaptive hybrid clock discipline algorithm for the Network Time Protocol. *IEEE/ACM Trans. Networking 6, 5* (October 1998), 505-514.

3. Li, Qiong, and D.L. Mills. On the long-range dependence of packet round-trip delays in Internet. *Proc. IEEE International Conference on Communications* (Atlanta GA, June 1998), 1185-1191.

4. Mills, D.L., A. Thyagarajan and B.C. Huffman. Internet timekeeping around the globe. *Proc. Precision Time and Time Interval (PTTI) Applications and Planning Meeting* (Long Beach CA, December 1997), 365-371.

5. Mills, D.L. Authentication scheme for distributed, ubiquitous, real-time protocols. *Proc. Advanced Telecommunications/Information Distribution Research Program (ATIRP) Conference* (College Park MD, January 1997), 293-298.

6. Mills, D.L. The network computer as precision timekeeper. *Proc. Precision Time and Time Interval (PTTI) Applications and Planning Meeting* (Reston VA, December 1996), 96-108.

7. Mills, D.L. Improved algorithms for synchronizing computer network clocks. *IEEE/ACM Trans. Networks 3, 3* (June 1995), 245-254.

4.2 Technical Reports

8. Mills, D.L. Public key cryptography for the Network Time Protocol. Electrical Engineering Report 00-5-1, University of Delaware, May 2000. 23 pp.

9. Mogul, J., D. Mills, J. Brittenson, J. Stone and U. Windl. Pulse-per-second API for Unix-like operating systems, version 1. Request for Comments RFC-2783, Internet Engineering Task Force, March 2000, 31 pp.

10. Sethi, A.S., H. Gao, and D.L. Mills. Management of the Network Time Protocol (NTP) with SNMP. Computer and Information Sciences Report 98-09, University of Delaware, November 1997, 32 pp.

11. Mills, D.L. A precision radio clock for WWV transmissions. Electrical Engineering Report 97-8-1, University of Delaware, August 1997, 25 pp.

12. Mills, D.L. Clock discipline algorithms for the Network Time Protocol Version 4. Electrical Engineering Report 97-3-3, University of Delaware, March 1997, 35 pp.

13. Mills, D.L. Proposed authentication enhancements for the Network Time Protocol version 4. Electrical Engineering Report 96-10-3, University of Delaware, October 1996, 36 pp.

14. 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, 18 pp.

15. Mills, D.L. Simple Network Time Protocol (SNTP). Network Working Group Report RFC-1769, University of Delaware, March 1995, 14 pp.

16. Mills, D.L. Simple Network Time Protocol (SNTP). Network Working Group Report RFC-1769, University of Delaware, March 1995, 14 pp.

4.3 Internet Drafts

17. Mills, D.L. Public-Key Cryptography for the Network Time Protocol. Internet Draft draft-ietf-stime-ntpauth-00.txt, University of Delaware, June 2000, 36 pp.

18. Mogul, J., D. Mills, J. Brittenson, J. Stone and U. Windl. Pulse-Per-Second API for UNIX-like Operating Systems, Version 1.0. Internet Draft draft-mogul-pps-api-05.txt, Compaq Western Research Laboratory, August 1999, 30 pp. (obsoleted by RFC-2783)

19. Mills, D.L., T.S. Glassey, and M.E. McNeil. Authentication Scheme Extensions to NTP. Internet Draft draft-mills-ntp-auth-coexist-01.txt, University of Delaware and Glassey-McNeil Technologies, September 1998, 9 pp. (expired)