Survivable, Real Time Network Services

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

Quarterly Progress Report
1 October 2000 - 31 December 2000

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 Tamal Basu. Graduate student Qiong Li has completed his dissertation and been granted the PhD degree. 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. Autonomous Authentication

The Autokey protocol has mostly stabilized, although we expect some changes when an interface is developed for the Secure DNS. Several minor bugs have been caught and fixed, mostly resulting from restarting the daemons while the protocol was in progress. Of most concern is the possible occurrence of a livelock condition where a pair of symmetric mode peers oscillate between protocol states as the result of a targeted intruder attack. Of necessity, the protocol vulnerability is greatest while the Autokey protocol is running and before the server identity and synchronization have been validated.

The problem with hosts and routers with more than one interface has been fixed. This required a considerable redesign of the association mobilization code along with a crafty invasion of the Unix sockets paradigm to reveal the local interface address before the first packet is sent. The code, which uses only standard Unix semantics, has been tested on Alpha, Sun and FreeBSD. This was the last remaining obstacle for deploying the Manycast mode in a meaningful configuration such as the CAIRN routers.

The current status of the Autokey protocol and implementation is available via the web at www.eecis.udel.edu/~mills/autokey.htm.

3. Autonomous Configuration

The main focus of work during the last quarter was the deployment and test of the Manycast autonomous configuration scheme. In this scheme a multicast client sends an ordinary request packet to a multicast group address and potential multicast servers in TTL range have the opportunity to respond with an ordinary unicast message. Each received message causes the client to mobilize an ephemeral association, which then proceeds as if the server were originally configures. This functionality was implemented by Ajit Thyagarajan in connection with his dissertation research and has been available for some time; however, it was not practical until the Autokey protocol had become available.

As in many such things, the devil was in the details. First, the problem with more than one interface had to be fixed, since this affects Manycast operations as well. Second, a robust add/drop heuristic was necessary to manage the server population and preserve a quasi-optimal hierarchy of servers and clients. It was always the plan that the existing carefully crafted mitigation and combining algorithms would be the basis of the add/drop heuristic and this has in fact been found to work very well.

Initial experiments with the DCnet routers and CAIRN routers have demonstrated a clique of Autokey/Manycast routers do in fact automatically reconfigure when something breaks and recover the necessary security configuration as required. The extreme paranoia characteristic of the Autokey protocol provoke some awesome pinball-like recovery situations, but recover they do. There still remain some tricky points, like how to avoid implosions when large numbers of servers are available, as mentions in the section on future plans below.

The current status of the Manycast mode and implementation is available via the web at www.eecis.udel.edu/~mills/autocfg.htm.

4. Publishing

This investigator has been under some serious pressure to do a braindump on NTP technology and history in the form of a book. There is only one thing that requires more fastidious care than writing a book, and that is writing a formal protocol specification. Nevertheless, this investigator has agreed to join a cabal of NTP enthusiasts to do just that. In point of fact, there is enough stuff that can be mined in technical reports and other documentation to almost write a book by itself.

The paper on the history of NTP cited at the end of this report may make interesting reading. It was not a trivial task to rummage in the Internet dustbins and prize out historic milestones. The paper is somewhat peculiar for the usually genteel journals - it is not clear which editor’s desk to drop this on. There were also two papers at the recent PTTI meeting cited, one on a scheme being hatched by Judah Levine at NIST and this investigator to provide International Atomic Time (TAI) in addition to UTC. The issue of whether to continue or discontinue leap seconds in the UTC timescale has become a contentious touchstone in the timekeeping community, so this paper may well fan the flames. The other paper is on a crafted set of kernel modifications that can in principle improve the resolution of the system clock to the nanosecond. Such would seem the

required response to gigahertz workstations showing up now on desktops. A third paper on long-range dependencies in computer networks was based on work done for Mr. Li's dissertation.

5. Infrastructure

NTP with Autokey and Manycast has been deployed to several CAIRN routers running FreeBSD 3.4 and now in regular operation. The very latest code as of late December 2000 has not been officially released, although release is expected no later than February 2001. The volunteer development corps continues to refine the code and fix occasional bugs as they are found.

Over the Christmas holiday we were victimized by a cracker who exploited a known security bug in a Linux system on a DCnet subnet used by another professor in this department. The system was purchased from Dell with Linux already installed. The cracker managed to infiltrate via a hole in the FTP daemon. He then proceeded to index a number of machines elsewhere in the Internet looking for the same security bug. This set off alarm bells in several places, including the CERT, and in turn resulted in a number of concerned messages imploding on this investigator as responsible person of record for DCnet 128.4.

The student responsible as sysadmin for the machine was yanked from his home in another state to find and resolve the problem and he performed admirably. He diagnosed the problem as described above and found the machine from which the immediate attack was launched. In Solvenia. We lay a good deal of blame on Dell, who should have kept up with CERT alerts that previously described the problem and recommended upgrade of the FTP server to a bug-resistant version.

The web documentation for this investigator's home page, the DCnet and CAIRN pages, the NTP home page and the NTP documentation pages have all been brought up to date. These pages have proliferated to the better part of a hundred megabytes with text, pictures and sounds. The web should be much easier to walk and the pages much more interconsistent and accurate. Besides all papers, technical reports, technical memoranda published at Delaware for the last 14 years, there are a number of technical briefings on projects funded by DARPA, US Navy and US Army agencies. DARPA status reports, yearly reports, final reports, quad charts and news stories are all archived at www.eecis.udel.edu/~mills/support.htm. Desktop wallpaper and a couple of interesting historic lessons are included in the www.eecis.udel.edu/~mills/gallery.htm.

6. Future Plans

The latest enhancements of the Autokey protocol and Manycast mode provide for a completely automatic autonomous deployment function. However, the ultimate security of the public-key protocols depends on certificate validation. High on the list for future work is rewriting the NTP daemon name resolution code, which has been heavily encrusted with useless stubs and excessively rigid format checking, making new features almost impossible to implement. A complicating factor is that the resolver code is closely bound to the remote configuration code and shares its awkward authentication mechanism (which is a separate scheme quite different from Autokey).

Initial experience with the Manycast rollout suggests it needs more work on the server side schemes. Servers do not respond unless they are themselves synchronized to valid sources and the stratum is equal to or lower than the client. Since a potentially destructive implosion can occur at

the client if too many servers respond, some means is needed for the servers to selectively discard requests before generating a response. We have discussed several means to do this, including multicasting the response so other servers in range can hear it. There is already a rate limit implemented in the code that discards a packet if more than a given number of packets have been heard from the same network within a given interval. We plan to explore these schemes and others that might come to mind.

7. 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.

7.1 Papers

1. Levine, J., and D. Mills. Using the Network Time Protocol to transmit International Atomic Time (TAI). *Proc. Precision Time and Time Interval (PTTI) Applications and Planning Meeting* (Reston VA, November 2000).

2. Mills, D.L., and P.-H. Kamp. The nanokernel. *Proc. Precision Time and Time Interval (PTTI) Applications and Planning Meeting* (Reston VA, November 2000).

3. Mills, D.L. A brief history of NTP time: confessions of an Internet timekeeper. Submitted for publication; please do not cite or redistribute.

4. Li, Qiong, and D.L. Mills. Investigating the scaling behavior, crossover and anti-persistence of internet packet delay dynamics. *Proc. 1999 IEEE GLOBECOM 99 Symposium* (Rio de Janerio, Brazil, December 1999).

5. 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.

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

7. 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.

8. 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.

9. 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.

10. 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.

11. 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.

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

7.2 Technical Reports

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

14. 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.

15. 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.

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

17. 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.

18. 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.

19. 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.

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

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

7.3 Internet Drafts

22. 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.

23. 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)

24. 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)