four times a year in *IEEE Design & Test* magazine. Chair: Joanne DeGroat, Ohio State University, 205 Dreese Lab, 2015 Neil Ave., Columbus, OH 43210-1272, phone (614) 292-2439, Compmail j.degroat.

The Distributed Processing TC addresses the technical aspects of specifying, designing, implementing, and evaluating distributed-computing systems. Specific topics of interest include executive and operating systems for decentralized control, logical and physical interconnection and communication, reliability and fault tolerance, systems and hardware architecture, distributed databases, and software specification, verification, applications, and systems. The TC sponsors workshops and conference sessions on these and related topics, as well as the annual International Conference on Distributed-Computing Systems, along with the annual Symposium on Reliability in Distributed Software and Database Systems. Chair: Bill Buckles, Dept. of Computer Science, Tulane University, New Orleans, LA 70118, phone (504) 865-5840, e-mail buckles@cs.tulane.edu.

The Fault-Tolerant-Computing TC is concerned with the design, analysis, testing, verification, and evaluation of systems subject to faults that occur during design or use. Technical activity in these areas ranges from basic research to current fault-tolerant-design practice and field experience. The TC cosponsors the annual International Symposium on Fault-Tolerant Computing and sponsors the Workshop on Fault Tolerance in Parallel and Distributed Computing. Chair: Jacob Abraham, Dept. of Electrical and Computer Eng., Engineering Science Bldg., University of Texas at Austin, Austin, TX 78712, phone (512) 471-8983, e-mail jaa@ece.utexas.edu.

The Mass Storage Systems and Technology TC is involved with the organization, storage and retrieval, and hardware requirements of large data collections. Unconventional data collections and processing systems are considered in addition to the conventional types, including special-purpose CPUs, mass storage devices, operating systems, and languages. The TC offers tutorials and workshops each year on these and other current topics. Chair: Sam Coleman, Lawrence Livermore National Laboratory, MS L-60, PO Box 808, 7000 East Ave., Livermore, CA 94550, phone (510) 422-4323, e-mail scoleman@llnl.gov.

The Mathematical Foundations of Computing TC is interested in the mathematics underlying the power, complexity, and design of computing devices, algorithms, and programs. It sponsors the annual Symposium on Foundations of Computer Science, which presents original research on such topics as automata and formal languages, computational complexity, data structures, formal semantics, mathematics of computation, mathematical studies of computer systems, and algorithm theory. Chair: Manuel Blum, University of California at Berkeley, Dept. of Computer Science, Berkeley, CA 94720, phone (415) 642-1662, e-mail blum@berkeley.arpa.edu.

The Personal Computing TC is dedicated to encouraging the development and application of personal computer technology in industry, business, and education. It holds workshops such as the Personal Computing Workshop, giving special emphasis to personal computer technology, software, and courseware. It provides a forum for interaction among educators, industry, and the user community. The TC encourages article submissions to *Computer* and *IEEE Micro* and sponsors user tutorials. It also plays an active role in personal computer activities and sessions at the major Computer Society conferences. The TC's newsletter is published four times a year. Chair: Stephen Ruth, Dept. of Decision Sciences, George Mason University, 4400 University Dr., Fairfax, VA 22030, phone (703) 993-1789, e-mail ruth@gmuvax.

"Authentication" revisited

T.Y.C. Woo and S.S. Lam, University of Texas at Austin

In our article published in the January 1992 issue of *Computer*,[1] the peer-peer authentication protocol shown in Figure 5 on page 47 needs augmentation. The protocol should read

$$(1)\ P \rightarrow A:\ P, Q$$
$$(2)\ A \rightarrow P:\ \{Q, k_Q\}_{k_A^{-1}}$$
$$(3)\ P \rightarrow Q:\ \{n_P, P\}_{k_Q}$$
$$(4)\ Q \rightarrow A:\ Q, P, \{n_P\}_{k_A}$$
$$(5)\ A \rightarrow Q:\ \{P, k_P\}_{k_A^{-1}},\ \big\{\{n_P, k, P, Q\}_{k_A^{-1}}\big\}_{k_Q}$$
$$(6)\ Q \rightarrow P:\ \big\{\{n_P, k, P, Q\}_{k_A^{-1}}, n_Q\big\}_{k_P}$$
$$(7)\ P \rightarrow Q:\ \{n_Q\}_k$$

Note that the letter *P* preceding the letter *Q* in steps (5) and (6) is missing in the previously published version. (We inadvertently submitted an old version of the figure to *Computer*, for which we apologize.)

As we analyzed the protocol in Figure 5, we also found a way to reduce the number of protocol steps for peer-peer authentication from seven to five:

$$(1)\ P \rightarrow Q:\ P, n_P$$
$$(2)\ Q \rightarrow A:\ P, Q, n_P, n_Q$$
$$(3)\ A \rightarrow Q:\ \{P, k_P\}_{k_A^{-1}},\ \big\{\{n_P, n_Q, P, Q, k\}_{k_A^{1}}\big\}_{k_Q}$$
$$(4)\ Q \rightarrow P:\ \big\{\{n_P, n_Q, P, Q, k\}_{k_A^{-1}}\big\}_{k_P}$$
$$(5)\ P \rightarrow Q:\ \{n_Q\}_k$$

Aside from being more efficient, this protocol is also interesting in that it can be viewed as an extension of the well-known three-way handshake protocol for establishing connections.[2] In particular, steps (1), (4), and (5) correspond to steps of the basic three-way handshake. But, in addition to establishing a new connection, the five-step protocol achieves mutual authentication.

References

1. T.Y.C. Woo and S.S. Lam, "Authentication for Distributed Systems," *Computer*, Vol. 25, No. 1, Jan. 1992, pp. 39-52.
2. DARPA Internet Program Protocol Specification, *Transmission Control Protocol RFC 793*, Information Sciences Institute, Marina Del Rey, Calif., 1981.

This work was supported in part by National Science Foundation Grant NCR-9004464.