From the Editor in Chief

Editor in Chief: M. Satyanarayanan ■ CMU and Intel Research ■ satya@cs.cmu.edu

Roger Needham, 1935–2003

M. Satyanarayanan

Roger Needham, one of the giants of computer science, passed away on 1 March 2003. At the time of his death, he was the Director of Microsoft's Cambridge Research Lab, which he founded in 1997. Prior to joining Microsoft, he was associated with Cambridge University for nearly half a century—as an undergraduate and graduate student, as a researcher, and eventually as a professor and head of the Computer Laboratory.

In this EIC message, I focus on the significance of Needham's research contributions to pervasive computing. These contributions are foundational in character. We are so dependent on them that we hardly realize that they each required a leap of imagination and creativity to bring into existence. In that respect, they meet Mark Weiser's criterion for a profound technology: they "weave themselves into the fabric of everyday lives until they are indistinguishable from it."

Every time you authenticate yourself to a remote system, you probably use a derivative of a technique that Needham and his colleague Michael Schroeder originally developed. In the mid 1970s, they were both involved in Xerox PARC's pioneering effort to create a personal computing environment. Part of that vision included using shared resources, such as laser printers and file servers, from many different clients over a network. The need to control access to these resources led naturally to the need for user authentication.

Needham and Schroeder formulated the authentication problem in a fundamentally different way from its prior formulation in the context of time-sharing systems. Not only did a computer system have to be assured of the user's identity, but the reverse also had to be true: the human user had to be confident that he or she was not interacting with a compromised remote computer. In other words, the problem was one of *mutual authentication* between untrusted parties. What made the problem especially challenging was the assumption that the network was completely open. Malicious third-party machines could eavesdrop on all communication between the parties desiring mutual authentication. A malicious machine could also inject communication into the network, letting it masquerade as one of the parties. It could do this, for example, by replaying communication that it had recorded earlier during a genuine authentication.

Needham and Schroeder's approach combined several simple ideas into an elegant whole. First, it used end-to-end encryption to convert an open network into a secure communication channel. Second, it inferred the possession of a shared secret (the keys used for encryption and decryption) from the ability to generate a correctly encrypted response to a challenge. Third, it foiled replay attacks by ensuring that each authentication attempt involved a fresh instance of a random component (called a *nonce*). We now regard the 1978 paper describing the Needham-Schroeder authentication protocol as a classic in the field.[1] The importance of security and privacy in pervasive computing cannot be overstated—indeed, the previous issue of this magazine focused on that very topic.

A decade prior to this seminal work, Needham invented another important technique relevant to security. The time-sharing systems of the mid 1960s stored user passwords in the clear in their local file systems. This meant that an unscrupulous human operator could steal a password and masquerade as its user. Needham realized that we could avoid the unsafe practice of storing passwords in the clear by using the properties of one-way functions. Such a function is computationally cheap, but its inverse is computationally intractable. Unix and many other operating systems adopted this technique, which continues to be used to this day.

By the late 1980s, interest in authentication techniques had exploded and

Published by the IEEE CS and IEEE ComSoc ■ 1536-1268/03/$17.00 © 2003 IEEE

ROGER NEEDHAM: 50 AND 5

A celebration to honor Roger Needham was held on 17 March 2003. The event was entitled “Roger Needham: 50 and 5,” reflecting his 50 years at Cambridge University and 5 years at Microsoft Research. Computer scientists from all over the world attended, contributing a volume of invited papers. See www.research.microsoft.com/~aherbert/needham_50_5.aspx for details of the event and the volume. See www.cl.cam.ac.uk/~ksj/RogerNeedham.html for biographical details of Roger Needham’s life.

many new protocols were published. Several of these protocols had subtle flaws buried deep inside them. Sometimes, these flaws passed the critical review of protocol developers and of reviewers of research publications. To Needham’s chagrin, a small but significant bug was found in his own published protocol! Although easily fixed, this incident exposed a critical need for intellectual tools to help ensure the correctness of authentication protocols. In collaboration with graduate student Michael Burrows and colleague Martin Abadi, Needham developed the framework and associated tools for reasoning about authentication protocols. Using these, many authentication protocols in use (including my own[2]) or proposed as standards were shown to have bugs. We now regard the paper reporting on the framework and tools as another classic in the security field.[3] Today, we expect any proposed authentication protocol to be formally verified before acceptance.

Besides security, Needham also made foundational contributions to other technologies important to pervasive computing. In the 1970s, he was involved in creating a ring network operating at 10 Mbits/s and a later version operating at 100 Mbits/s. These were early examples of a local area network. With collaborators Andrew Birrell, Roy Levin, and Michael Schroeder, he built a decentralized naming system called Grapevine that used asynchronous data propagation and eventual consistency to achieve scalability and failure-resistance.[4] Grapevine was the intellectual forerunner of systems such as DNS (Domain Name Server) and LDAP (Lightweight Directory Access Protocol), which are in widespread use today.

On a personal note, it is an honor and a privilege to have known Roger Needham as a colleague and friend. His warmth and friendliness masked his impressive intellect and his keen powers of observation. He conducted himself with humility, recognizing that talent takes many forms—not all of which are easily observable in a person. He had a wonderful, dry sense of humor that could send an audience into peals of laughter—the perfect antidote to a dreary post-lunch session at any conference! His life has enriched his friends and the field of computer science in many ways.

REFERENCES

1. R.M. Needham and M.D. Schroeder, “Using Encryption for Authentication in Large Networks of Computers,” *Comm. ACM*, vol. 21, no. 12, Dec. 1978, pp. 993–999.

2. M. Satyanarayanan, “Integrating Security in a Large Distributed System,” *ACM Trans. Computer Systems*, vol. 7, no. 3, Aug. 1989, pp. 247–280.

3. M. Burrows, M. Abadi, and R. Needham, “A Logic of Authentication,” *ACM Trans. Computer Systems*, vol. 8, no. 1, Feb. 1990, pp. 18–36.

4. A. Birrell et al., “Grapevine: An Exercise in Distributed Computing,” *Comm. ACM*, vol. 25, no. 4, Apr. 1982, pp. 260–274.

IEEE Computer Society Publications Office

10662 Los Vaqueros Circle, PO Box 3014
Los Alamitos, CA 90720-1314

STAFF

Associate Lead Editor
Shani Murray
smurray@computer.org

Group Managing Editor
Crystal Shif
cshif@computer.org

Senior Editor
Dale Strok

Associate Editor
Dennis Taylor

Assistant Editors
Rebecca Deuel and Denise Kano

Editorial Assistant
Joan Hong

Magazine Assistant
Pauline Hosillos
pervasive@computer.org

Contributing Editors
Kirk Kroeker, Anne Lear, Christine Miller, Keri Schreiner, and Joan Taylor

Design Director
Toni Van Buskirk

Layout & Technical Illustrations
Carmen Flores-Garvey and Alex Torres

Production Assistant
Monette Velasco

Publisher
Angela Burgess

Assistant Publisher
Dick Price

Membership & Circulation Marketing Manager
Georgann Carter

Business Development Manager
Sandra Brown

Assistant Advertising Coordinator
Debbie Sims

Submissions: Submit two copies of all articles and track proposals to *IEEE Pervasive Computing*, Magazine Assistant, 10662 Los Vaqueros Circle, Los Alamitos, CA 90720-1314; phone +1 714 821 8380; pervasive@computer.org. Manuscripts should be approximately 5,000 words long, preferably not exceeding 10 references. Visit http://computer.org/pervasive for editorial guidelines.

Editorial: Unless otherwise stated, bylined articles as well as products and services reflect the author’s or firm’s opinion; inclusion does not necessarily constitute endorsement by the IEEE Computer Society or the IEEE.

IEEE pervasive COMPUTING
MOBILE AND UBIQUITOUS SYSTEMS