Call for Workshop Participation

New Directions in Scalable Cyber-Security in Large-Scale Networks: Deployment Obstacles

March 13-14, 2003, Lansdowne, Virginia

Sponsored by Large-Scale Network Group of Interagency Working Group on Information Technology R&D (DOE, NSF, NSA, NIST, NASA, and DARPA)

Background - As the critical functions of government such as commerce, transportation, defense, energy, science, *etc.*, are increasingly performed in cyber space, new questions are being raised about the ability of computing and large-scale network infrastructures to survive sophisticated and coordinated cyber attacks. In particular, large-scale networks, which provide the critical computer and communication functions in cyber space, will almost certainly become the target of cyber attacks. Thus the development of critical basic science and technologies necessary to adequately secure the nation's network infrastructures has become a strategic priority. Although network security and related cyber-security systems have been built for many years, a number of recent and related trends in technologies, economic factors, increased use of COTS products, and sophistication of cyber attacks have created a new environment that challenges traditional approaches to large-scale cyber security, drawing attention to radical new directions, and calling for comprehensive evaluation of non-technical impediments that hinder the development of large-scale secure-network infrastructures.

Call for Participation

This workshop is intended to address the challenging issues of large-scale cyber security R&D and deployment obstacles. The attendance will be limited to 50 participants. The participants will be selected on the basis of the merit of position papers and presentations submitted to the workshop committee. The workshop has two main objectives:

- The development of a long-term R&D vision to address the technical and non-technical challenges in cyber-security systems deployment in large-scale networks.
- To identify and develop strategies to address the fundamental impediments to cyber-security systems deployment in large scale networks.

The scope of the workshop will include but not be limited to cyber-security issues in large-scale networks, ultra high-speed networks, wireless/sensor networks, research/experimental networks, and related cyber-science activities such as economic issues in deployment of security technology, large-scale scientific

collaboration, grid infrastructures, and embedded systems. Other related topics of interest may include but are not limited to:

- Radical new directions in cyber security for large-scale networks
- Non-technical obstacles to large-scale cyber-security deployment
- Cyber-security systems for open-source environments
- Scalable cyber-security systems for ultra high-speed networks
- Science and engineering approaches to cyber security
- Economic and human factors in cyber-security systems
- Investments in cyber security
- Sharing of information about cyber-security breaches
- Perverse economic incentives in cyber security
- Cyber security for critical-infrastructure protection

Submission

Draft position papers (up to 5 pages) or presentations (up 10 slides) should be sent electronically on or before **January 30, 2003** to the workshop co-chair:

Dr. Joan Feigenbaum, Yale University, Department of Computer Science, 51 Prospect Street, New Haven, CT 06511. Tel: (203) 432-6432, Email: joan.feigenbaum@yale.edu

Participation will be limited to those whose position papers or presentations have been submitted, reviewed, and recommended by the organizing committee.

Important Dates:

January 30, 2003: Deadline for submission
February 15, 2003: Acceptance notification
March 13-14, 2003: Workshop Dates

For more information on the workshop, please contact the workshop co-chairs:

Joan Feigenbaum – joan.feigenbaum@yale.edu
Lawrence Gordon – lgordon@rhsmith.umd.edu