Invited Address:

Applying Formal Methods to Cryptographic Protocol Analysis

Catherine Meadows

Naval Research Laboratory
Washington, DC 20375

Abstract. Protocols using encryption to communicate securely and privately are essential to the protection of our infrastructure. However, since they must be designed to work even under the most hostile conditions, it is not easy to design them correctly. As a matter of fact, it is possible for such protocols to be incorrect even if the cryptographic algorithms they use work perfectly. Thus, over the last few years there has been considerable interest in applying formal methods to the problem of verifying that these protocols are correct. In this talk we give a brief history of this area, and describe some of the emerging issues and new research problems.

E.A. Emerson and A.P. Sistla (Eds.): CAV 2000, LNCS 1855, p. 2, 2000.