Statistical Engineering Division Seminar (Information Technology Laboratory)

Monday October 7, 1996, 11:00 am

Room 618, Bldg 820/NN
NIST
Gaithersburg, MD

Multivariate Anomalies: Computer Security Applications

David Banks

Carnegie Mellon University

The potential costs of compromised computer systems are enormous. To discover attempted intrusions, one must continually monitor the state of complex networked systems for threatening patterns of activity. Such monitoring entails tracking dozens to hundreds of variables, which raises the statistical problem known as the Curse of Dimensionality. This talk addresses a number of strategies for minimizing the impact of the curse. Specific topics include the problem of estimating local dimensionality, automatic adaptation to evolving and periodic computational environments, pattern recognition of intrusion signatures, and a more powerful test for multivariate drift in process monitoring. Each of these topics addresses a different aspect of anomaly detection in computer (or other) systems. A practicable solution requires the coordinated combination of these and other statistical methods, in partnership with computer scientists and application-specific experts.

David Banks received his B.S. degree from the University of Virginia in 1977, his M.S. degrees in statistics and applied mathematics from Virginia Polytechnic Institute in 1980 and 1982, and his Ph.D. in Statistics from Virginia Polytechnic Institute in 1984. He spent two years as an NSF postdoctoral research fellow at the Department of Statistics at the University of California at Berkeley, and one year as visiting assistant lecturer at the Department of Pure Mathematics and Mathematical Statistics at the University of Cambridge. He joined Carnegie Mellon University in 1987, and is now associate professor of statistics.

Professor Banks' research interests include nonparametric Bayesian computer-intensive data analysis, complex multivariate data, process monitoring, genetics, statistical analysis of shape, and inference for objects in non-standard metric spaces.

[NIST contact: Raghu Kacker 301-975-2109, and Tim Grance 301-975-3359]