PANEL SESSION: INFORMATION SECURITY RESEARCH AND DEVELOPMENT IN ACADEMIA

Panel Chair: Dr. Susan M. Bridges, Mississippi State University
Panelists: Dr. Blaine W. Burnham, Georgia Tech
Dr. Dipankar Dasgupta, The University of Memphis
Dr. James A. Davis, Iowa State University
Dr. Cynthia Irvine, Naval Postgraduate School

SESSION ABSTRACT

Research and development activities in information security within academia have been rather limited until quite recently. An increased interest in the field has been prompted by the large number of high visibility breaches of network security and the sudden importance of e-commerce to the national and world economy. This increase in interest is also reflected in an increase in funding available from government agencies such as NSF, DARPA, and NSA for research in information security and it is likely that more universities will be moving into this area. This panel will present a sampling of the types of research in the area of information security that are being conducted at universities and will also address issues related to the establishment of a university research program in this area. These issues include but are not limited to questions such as the following. Where does information security "fit" in an academic setting? How does one establish an information security research program in an academic setting? How does one set up an interdisciplinary research team? Are there appropriate publication outlets for research in this area? What is the role of "development" in an academic setting?

Biographical Sketch: Susan M. Bridges

Dr. Susan M. Bridges is an associate professor in the Computer Science Department at Mississippi State University. Her research is in the area of artificial intelligence with a focus on data mining and knowledge discovery from scientific data. Her research projects in data mining from remotely sensed data are supported by the Navy Oceanographic Command and by NASA. Dr. Bridges and her colleague, Dr. Rayford Vaughn, established an information security research group about two years ago. They have subsequently directed the research of six Master's students in this area and published a number of papers describing the application of fuzzy data mining techniques to the intrusion detection problem. Dr. Bridges holds bachelors and masters degrees in biology and a Ph.D. in Computer Science from the University of Alabama in Huntsville.

Contact Information: Mississippi State University
Department of Computer Science
Mississippi State University
Address: Box 9637, Mississippi State, MS 39762
Phone: 662-325-7505 FAX: 662-325-8997
Email: bridges@cs.msstate.edu

Position Statement: Dr. Blaine W. Burnham

This presentation will discuss some of the background leading up to university research in information security, who does it and why, what are some of the enablers and obstacles. It will explore the positioning of an information security program in the university context and what elements need to come together to enable the program. It will share some thoughts on the content of a university information security program.

Biographical Sketch: Dr. Blaine W. Burham

Dr. Burnham joined Georgia Tech on December 14, 1998 as a Principal Research Scientist in the College of Computing to serve as the Director of the Georgia Tech Information Security Center (GTISC). He most recently served as program manager for the National Security Agency (NSA) at Ft. Meade, Maryland. While at NSA Dr. Burnham established, promoted and sustained the Information Security Research Council for the Department of Defense as well as the intelligence community as a whole. He also achieved an operational prototype of a trusted client/server operation system; created and developed the Product Security Profile (PSP); and directed the Infosec Criteria and Guidelines organization that published half of the guideline documents, the Rainbow Series, and crafted the Federal Criteria. Dr. Burnham also did stints on the technical staffs of the Los Alamos National Laboratory and Sandia National Laboratory developing tools and techniques for achieving higher levels of information security. Dr. Burnham received his Ph.D. and master's in Mathematics from Arizona State University and a B.S. in Mathematics from Idaho State University.

Contact Information: Director, Georgia Tech Information Security Center (GTISC)
Atlanta, GA 30332
Phone: 404-385-0270
FAX: 404-385-0332
Email: burnham@cc.gatech.edu

Position Statement: Dr. Dipankar Dasgupta

I will discuss an intelligent network security system for the protection of information infrastructure. This new technique focuses on applying immunological principles in designing a multi-agent system for network intrusion detection. Specifically, the immunity-based agents roam around the machines, nodes (or routers), and monitor the situation in the network (i.e. look for changes such as malfunctions, faults, abnormalities, misuse, deviations, intrusions, etc.). They can mutually recognize each other's activities and can take appropriate actions according to the security policies. Such an agent can learn and adapt to its environment dynamically and can detect both known and unknown intrusions. The main goal of this research is to develop a multi-agent detection system that can simultaneously monitor networked computer's activities at different levels (such as user level, system level, process level and packet level) in order to provide both host-based and network-based detection capabilities. The proposed intrusion detection system is designed as flexible, extendible, and adaptable in order to meet the needs and preferences of network administrators.

Biographical Sketch: Dr. Dipankar Dasgupta
Dr. Dasgupta is a faculty of Computer Science at the University of Memphis. He has been working on computational models of the immune system and their application for several years. Dr Dasgupta's previous research with real and simulated data has been very encouraging. In 1996, he received the "Best Paper Award" at the International Conferences on Intelligent Systems for his description of the application of an anomaly detection algorithm in time series data. He organized special tracks and offered tutorials on Artificial Immune Systems at a number of International Conferences since 1997. He also edited a book on "Artificial Immune Systems and Their Applications", published by Springer-Verlag, Inc, 1999. He published more than 50 technical papers in his areas of research, and presented a paper on security at National Information Systems Security Conference (NISSC), October 18-21, 1999. One of his current research interests is to develop immunity-based intrusion detection systems and he has received funding from DARPA to conduct this research.

Contact Information: Division of Computer Science
Mathematical Sciences Department
The University of Memphis
Memphis, TN 38152
Phone: 901-678-4147
FAX: 901-678-2480
Email: dasgupta@msci.memphis.edu

Position Statement: Dr. James A. Davis

There is a consensus in our community that research, in its varied forms, is an essential component of a robust education program in Information Assurance. Additionally, we have started to broaden our vision of Information Assurance to include non-networking fields such as *cyber policy*. There are many examples of important real-world security problems whose solutions are most effectively achieved through a diverse multidisciplinary team. As the educational component of academic programs moves towards a true interdepartmental, multidisciplinary effort, will academic research follow? How do we bring together researchers from fields that have not historically worked together? Are funding agencies ready to accept proposals that contain a significant ethical or political work component? As we bring our Masters of Science degree in Information Assurance to realization at Iowa State University, we are learning how to overcome some of the barriers to interdisciplinary research. I will briefly discuss these and other related issues as a "work in progress".

Biographical Sketch: Dr. James A. Davis

Dr. Jim Davis is an Associate Professor of Electrical and Computer Engineering at Iowa State University. He is co-director of the Information System Security Laboratory, designated as a Center of Excellence in Information Assurance Education by the National Security Agency, and is the first program chair of Iowa State's new interdepartmental Masters of Science degree in Information Assurance. Jim teaches graduate courses in computer security and an undergraduate course in software systems integration. Current projects include a DoD funded effort to develop countermeasures for denial of service attacks and an NSF funded project to develop INFOSEC course modules that can be easily integrated into non-INFOSEC courses. Jim is a Miller Faculty Fellow at Iowa State and is active in Project LEARN, a faculty-driven, in-service program that mentors and teaches faculty to enhance student learning through innovative teaching methodologies.

Contact Information: Department of Electrical and Computer Engineering
2413 Coover Hall
Iowa State University
Ames, Iowa 50011
Phone: 515-294-0659
FAX: 515-294-3637
Email: davis@iastate.edu

Position Statement: An Argument for Academic Research in Information Security

Cynthia E. Irvine

When computer science and computer engineering first evolved from mathematics and electrical engineering, substantial academic research in information security took place. Our evidence is the existence of seminal papers in information security written by academics during the first decades of the field. This "required reading list" includes papers by Saltzer and Schroeder, Dorothy Denning, and Popek. Unfortunately, during the 1980s and 1990s, as information security became passe in academe, only a handful of universities conducted significant research programs in the area.

We now pay the price for this lack of attention both in academe and industry: massive systems for which security is merely an afterthought. Today, there is growing recognition that security must be a factor in the basic engineering of modem systems and that there is a large deficit of talented scientists and engineers able to address security from a coherent system perspective. In an academic setting, research in information security can involve students in current and emerging problems.

The design and construction of an operating system or a physical database is an art form to be learned through apprenticeship with a master. Such mentoring can take place either in universities or in industry laboratories. As is the case for these areas of computer science, most of what one needs to know to conduct research in and learn about secure systems is not found in books. Thus the design and implementation of secure systems must be fostered through a research program that permits the mentor to build a system while involving the students. This allows students to internalize the concepts presented in the classroom as well as interact with members of the research team.

Because enforcement of security policies must be considered within the context of systems with functional requirements, a broad range of knowledge and experience is required to address security in the large. Hence, there is a need for a group of complementary researchers. Although these individuals may not necessarily collaborate on all research projects, implicit collaboration takes place through frequent, perhaps daily, casual encounters. Such a group will have sufficient "critical mass" to maintain an energetic and diverse research program. Collaborations with industry can enhance the academic environment by stimulating research on emerging problems. The benefits include support of academic research and additional mentoring of students by commercial sector research and development teams. However, a potential danger of such collaborations, is constrained proprietary research that may not nurture significant paradigm shifts or innovations.

A challenge to be addressed when attempting to initiate an academic program in information security is that of bringing together the necessary talent. The number of current security practitioners is relatively small and there is no simplistic approach to increasing those numbers. Instead new academic talent must be developed by wise investment in existing resources and then providing incentives for these emerging information security scholars to take positions at universities where new programs can be initiated.

Biographical Sketch: Dr. Cynthia Irvine

Cynthia Irvine is the Director of the Naval Postgraduate School Center for INFOSEC Studies and Research at the Naval Postgraduate School (http://cisr.nps.navy.mil). Dr. Irvine has over twelve years experience in computer security research and development, particularly in the design and development of high assurance multilevel systems. Her current research involves characterization of security within quality of service frameworks, architectural issues for modern high assurance networked systems including the effective use of hardware security features. She has supervised the thesis research of dozens of graduate students. In 1998 and 1999 Dr. Irvine received the Naval Postgraduate School awards for outstanding research achievement. She is a senior member of the IEEE.

Contact Information:

Code CS/Ic
Computer Science Department
Naval Postgraduate School
Monterey, CA 93940-5000
Phone: 408-656-2461
FAX: 831-656 2814
Email: irvine@cs.nps.navy.mil

Target Audience: This panel will discuss issues that should be of interest to all those who participate in information security research, who support such research, or who wish to make use of the results of the research.