Information Security Education and Foundational Research

Linda Morales
Computer Science Department
Texas A&M University-Commerce
Linda_Morales@tamu-commerce.edu

Melissa Dark
School of Technology
Purdue University
dark@purdue.edu

The mini-track on Information Security Education and Foundational Research is a forum for the discussion of advances in two important areas of information security: education and basic research. The information security education area is concerned information security curriculum design at the national and institutional levels, innovative approaches to teaching information security, evaluations of existing approaches, emerging needs for information security curriculum, innovative approaches to faculty development and capacity building, challenges faced by institutions and programs, and other topics relevant to information security education.

The fundamental research area is concerned with advances in the theory and foundations of information security such as new analytic results, mathematical developments and proofs. Topics covered in this category include cryptography and cryptographic protocols, mathematical analyses of secure computing systems, foundations of network security, ethical and legal issues in information security, the theoretical foundations of information security, information security management policy and response, and other foundational topics.

Nine papers have been accepted for the minitrack this year. Afinidad, Levin, Irvine, and Nguyen present a model for temporal access control in A Model for Temporal Interval Authorizations. In Efficient Algorithms for Batch Re-keying Operations in Secure Multicast, Heydari, Morales and Sudborough present “algorithms to improve on the number of re-keying messages (overhead) needed to add and delete sets of users to a secure multicast group”, and discuss upper and lower bounds. Spears and Cole “examine the information security implications of the Sarbanes-Oxley Act of 2002” in A Preliminary Investigation of the Impact of the Sarbanes-Oxley Act on Information Security.

In Assessment of Enterprise Information Security - The Importance of Information Search Cost, Johansson, Ekstedt and Johnson describe a “method for assessing the level of enterprise information security”, expressing “the credibility of the results in terms of confidence levels” and estimating “the cost of searching for security evidence”. In Programming Education in the Era of the Internet: A Paradigm Shift, Harrison, Hanebutte and Alves-Foss discuss “the need to incorporate basic information assurance knowledge into general CS classes”. In Foundations for Security Aware Software Development Education, Yasinsac and McDonald “propose that security-specific coding techniques need to be integrated pedagogically alongside robustness so that students can differentiate the two.” They propose “a shift in instructional methods based on this distinction to help future programmers, developers, and software engineers produce ‘security-aware’ software”.

In Experiences With Honeypot Systems: Development, Deployment, and Analysis, McGrew and Vaughn present “a summary of university research performed on honeypot techniques” and offer “recommendations to improve the usage of honeypots as an attack profiling tool by improving the control measures that make a honeypot easy to detect”. In Cyber Defense Competitions and Information Security Education: An Active Learning Solution for a Capstone Course, Conklin describes the use of “a Cyber Defense Competition to provide a hands-on opportunity for students to test their skills and develop team based management skills in an operational business environment”. In Design and Implementation of a Multi-use Attack-Defend Computer Security Lab, Caltagirone, Ortman, Melton, Manz, King, and Oman describe “the rationale, design and implementation of a Reconfigurable Attack-Defend Instructional Computing Laboratory (RADICL)” as well as “the ethical and pedagogical considerations for creating and using a lab that instructs and develops not only student’s abilities to secure a system, but also their ability to attack a system.”