

Cybersecurity Seminar Series presents:

“Blueprint for a Science of Security”

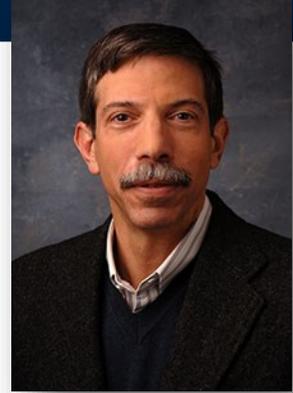
By Fred Schneider

Samuel B. Eckert Professor of Computer Science,
Cornell University

Friday, September 11, 2015 | 2:00 pm

Information Sciences Building, 3rd Floor Theatre

Light refreshments provided prior, with Q&A to follow



Cybersecurity today is focused largely on defending against known attacks. We learn about the latest attack and find a patch to defend against it. Our defenses thus improve only after they have been successfully penetrated. This is a recipe to ensure some attackers succeed—not a recipe for achieving system trustworthiness. We must move beyond reacting to yesterday's attacks and instead start building systems whose trustworthiness derives from first principles. Yet, today we lack such a science base for cybersecurity. That science of security would have to include attacks, defense mechanisms, and security properties; its laws would characterize how these relate. This talk will discuss examples of such laws and suggest avenues for future exploration.

Fred B. Schneider is a Samuel B. Eckert Professor of Computer Science at Cornell University, and chair of the department. Schneider currently also serves as the Chief Scientist for the NSF-funded TRUST Science and Technology Center, and on numerous boards and committees.

Schneider's research has focused on various aspects of trustworthy systems—systems that will perform as expected, despite failures and attacks. His early work concerned formal methods to aid in the design and implementation of concurrent and distributed systems that satisfy their specifications. He is author of two texts on that subject. He is also known for his research in theory and algorithms for building fault-tolerant distributed systems. More recently, his interests have turned to system security. His work characterizing what policies can be enforced with various classes of defenses is widely cited, and it is seen as advancing the nascent science base for security. He is also engaged in research concerning legal and economic measures for improving system trustworthiness.

Schneider is a frequent consultant to industry, believing this to be an efficient method of technology transfer and a good way to learn about the real problems. He provides technical expertise in fault-tolerance and computer security to a variety of other firms, including Intel, Lincoln Laboratories, and Riskive. In addition, Schneider has testified about cybersecurity research at hearings of the US House of Representatives Armed Services Committee (subcommittee on Terrorism, Unconventional Threats, and Capabilities), as well as the Committee on Science and Technology (subcommittee on Technology and Innovation and subcommittee on Research and Science Education).

Sponsored by the University of Pittsburgh School of Information Sciences and the Laboratory for Education and Research on Security Assured Information Systems (LERSAIS)