About WPI Cybersecurity

Every day, criminals are breaking into individuals', business, and government laptops, personal computers, and wireless devices through hacks and bits of malicious code, according to the FBI. The result is billions of dollars lost every year repairing computers hit by cyberattacks, which take down vital systems, disrupting and sometimes disabling the work of hospitals, banks, and emergency response services across the U.S.

WPI is training the next generation of domestic cybersecurity professionals to help fill a growing national demand for experts, and address the increasing threats to the nation's critical infrastructure. The university's Cybersecurity Program was formalized in 2010, but WPI faculty have been active in cybersecurity research since 1995. Presently, 12 WPI faculty members in computer science, electrical and computer engineering, mathematical sciences, and social science and policy studies have active research programs in this field.

The university was recognized as a National Security Administration/Department of Homeland Security Center of Excellence in Information Assurance Research in 2013. More recently, in response to a critical national shortage of highly trained experts in cybersecurity, the National Science Foundation (NSF) awarded WPI more than $4.4 million to develop a program that will prepare professionals to address cybersecurity challenges and threats for the federal government. Funded through the NSF's CyberCorps: Scholarship for Service initiative, WPI's program will help bolster the national cybersecurity workforce by providing scholarships for 25 undergraduates and graduate students who will commit to government service after graduation.

- Professor of computer science Kathi Fisler’s research has been vital to organizations seeking to strengthen computer education at all levels. As a member of the SIGPLAN Education Board, she helped design the programming language component of new undergraduate computer science curriculum guidelines developed by the Association for Computing Machinery. She currently serves on the Massachusetts Digital Literacy and Computer Science Standards Panel, which is determining how to integrate computer science into the state’s K-12 technology literacy standards. Fisler developed and taught WPI’s first course in software security, a stepping stone toward deepening WPI’s cybersecurity offerings, and leading to recognition as a Center of Excellence in Information Assurance Research. She was also the principal investigator for the NSF Scholarship for Service award.
Last year (2014), professor Susan Landau, PhD, former senior staff privacy analyst at Google and a widely respected authority on cybersecurity, privacy, and public policy, joined the WPI faculty as the nation’s first professor of cybersecurity policy. Landau’s recent focus has been the security risks of embedding surveillance in communications infrastructures; she has briefed members of the U.S. and European governments and participated in several industry reports on the issue.

Landau has also addressed this and other privacy and cybersecurity concerns as a member of the National Research Council Computer Science and Telecommunications Board, and the advisory committee for the National Science Foundation’s Directorate for Computer and Information Science and Engineering. She previously served on the Center for Strategic and International Studies Commission on Cybersecurity for the 44th Presidency.

Professor Craig Wills’ research has primarily focused on Internet application performance and measurement with more recent work examining issues related to Internet privacy. This work has led to a number of research publications and presentations as well as visibility in venues such as the New York Times, Wall Street Journal and NPR Science Friday.

Assistant professor Craig A. Shue’s interests lie in computer networking and security, exploring future directions in computing from a systems, networking, and security standpoint. His earlier work focused on Internet-scale measurements to identify security weaknesses and under-provisioned systems that could cause widespread website outages if attacked or if they failed. Shue, a former cybersecurity researcher at the Oak Ridge National Laboratories, also serves as the coach for the WPI Cyber Defense Team.

Assistant professor Krishna Kumar Venkatasubramanian’s research focuses on the field of medical cyber-physical systems and their security. His current projects are focused on designing secure interoperable medical device systems, a credentialing system for facilitating open-source development of military vehicles, and environment-coupled security solutions for body area networks. His research has been featured in Discovery Channel website, ACM Tech News, and IEEE Engineering in Medicine and Biology Article Wearable Technology.

Associate professor Berk Sunar leads the Vernam Research Group at WPI, specializing in applied cryptography. His current research interests are in high performance cryptography (homomorphic encryption, cryptographic accelerators); physical security (integrated circuit & optical fingerprinting, physically inspired primitives, PUFs, hardware trojans); and side-channel attacks on the cloud.
Assistant professor Thomas Eisenbarth spent two years at the Center for Cryptology and Information Security (CCIS) at Florida Atlantic University before joining WPI. He does research in embedded systems security, side channel attacks and countermeasures, and efficient implementation of cryptographic systems.

Assistant professor Lifeng Lai’s research includes information theory, stochastic signal processing, and their applications in wireless network security, wireless communications and related areas.