For decades, secure software development methodologies have focused mainly on keeping attackers out---by eliminating software vulnerabilities or by detecting and mitigating their exploitation. But aggressively keeping detected attackers out has an unfortunate side-effect: it denies defenders critical threat intelligence that is only observable from longer, more substantive adversarial interactions. Software cyberdeceptions, such as honeypotting, are an important avenue for gathering this prized threat data, but are often designed and deployed unscientifically, and with services that attract and deceive only weak threats whose TTPs are less valuable to defenders than those of skillful adversaries.

In this talk, I will argue that a more rigorous science of software cyberdeception has the potential to offer many powerful advantages for cyberdefense, and might even be considered an "easy win" relative to traditional strategies that are unscalable or provably hard by comparison. However, it requires a deeply interdisciplinary approach that forces us to rethink how we approach certain aspects of software engineering, testing and evaluation, economics of security, human-computer interaction, software virtualization, and risk management.
Computer Science at the University of Texas at Dallas, and director of the Software Languages Security Lab (SL)^2. His research on software binary analysis, formal methods approaches to security, malware active defense, and software cyberdeception has received numerous best paper awards, including twice receiving an NYU-Poly Best Applied Security Paper of the Year award, and has been spotlighted by thousands of news headlines worldwide, including in The Economist and New Scientist. He is the recipient of both the NSF CAREER and AFOSR Young Investigator Awards, as well as support from Navy, NSA, Army, and DARPA. Dr. Hamlen received his PhD from Cornell University and his BS from Carnegie Mellon University, where he received the Allen Newell Award for his research on proof-carrying code.

TRENT JAEGER

The Science of Attack Surfaces and Its Applications

Microsoft identified the principle of an attack surface as the number of "attack opportunities" that a program or system makes available to adversaries. Often adversaries take advantage of undefended opportunities to launch exploits, so understanding attack surfaces could be valuable in preventing vulnerabilities proactively. In this talk, I will discuss various research endeavors that the we and other researchers have explored in computing, representing, and reasoning about attack surfaces to identify where and how to augment defenses. Examples include the methods to use attack surface to compare relative security, identify vulnerabilities in file system access, compute exploits within programs, etc. Also, we will compare attack surfaces to alternative representations, such as attack graphs. We will discuss methods for computing attack surfaces in systems and for programs and challenges in applying the attack surface metric more broadly for developing intrusion detection techniques.

Trent Jaeger is a Professor in the Computer Science
Director of the Systems and Internet Infrastructure Security (SIIS) Lab. Trent’s research interests include operating systems security and the application of programming language techniques to software security. He has published over 125 refereed research papers and is the author of the book "Operating Systems Security," which examines the principles of designs for secure operating systems. Trent has made a variety of contributions to open source systems security, particularly to the Linux Security Modules framework, Linux Integrity Measurement framework, and recently, security namespaces for Linux containers. He was Chair of the ACM Special Interest Group on Security, Audit, and Control (ACM SIGSAC) from 2013-2017, is on the steering committees of two of the major computer security research conferences (ACM CCS and NDSS, as Chair), and is the Consortium Lead for the Army Research Lab’s Collaborative Research Alliance devoted to the science of security. Trent has an M.S. and a Ph.D. from the University of Michigan, Ann Arbor in Computer Science and Engineering, respectively, and spent nine years at IBM Research prior to joining Penn State.

REBECCA WRIGHT

Accountability in Computing

Accountability is used often in describing computer-security mechanisms that complement preventive security, but it lacks a precise, agreed-upon definition. Here, we argue for the need for accountability in computing in a variety of settings, categorize some of the many ways in which this term is used, and propose a punishment-focused view of "accountability." We formalize our view in a utility-theoretic way and then use this to reason about accountability in computing systems. We also survey mechanisms providing various senses of accountability as well as other approaches to reasoning about accountability-related properties.

This is joint work with Joan Feigenbaum and Aaron Jaggard.
Barnard. She is currently on leave from Rutgers University, where she served as
director of the DIMACS center and as the founding faculty advisor for the
Douglass-SAS-DIMACS Computer Science Living-Learning Community for first-
year Rutgers women in Computer Science. Wright's research is primarily in the
area of information security, including privacy, applied cryptography, foundations
of computer security, and fault-tolerant distributed computing. Wright serves as an
editor of the International Journal of Information and Computer Security and of the
Transactions on Data Privacy, and is a member of the board of the Computer
Research Association's Committee on the Status of Women in Computing
Research (CRA-W). She received a Ph.D. in Computer Science from Yale
University, a B.A. from Columbia University, and an honorary M.E. from Stevens
Institute of Technology. She is a Fellow of the IEEE and a Distinguished Member
of the ACM.