CISE Ph.D. Qualifying Exam Syllabus

Security Area

Introduction

The qualifying exam on security covers topics within network security, systems security, and applied cryptography. It includes fundamental concepts in computer security, common analysis techniques, classic protocols, and applications of these principles to modern computing systems and networks.

Topics covered include basic security principles, authentication, security protocol design and analysis, key management, public and secret-key cryptography and cryptographic primitives, security modeling, system vulnerabilities, capability systems, trusted computing, program safety, intrusion detection, DDoS detection and mitigation, architecture/operating systems security, security policy, group systems, biometrics, web security, virtual machines and security kernels, and distributed systems security including cloud computing.

Relevant Courses

CNT 5410 Computer and Network Security
CIS 5370 Computer and Information Security

Reading List


Reflections on Trusting Trust. Ken Thompson, Turing Award Lecture, 1983


Bishop, M. 2009. Reflections on UNIX Vulnerabilities. ACSAC.


Wulf, W., et al. 1974. HYDRA: The Kernel of a Multiprocessor Operating System. CACM.


Li, Yanlin, McCune, J., and Perrig, A. 2011. VIPER: Verifying the Integrity of PERipherals’ Firmware. In CCS.
