The CyberCorps® Scholarship For Service (SFS) is a unique program designed to increase and strengthen the cadre of federal information assurance professionals that protect the government’s critical information infrastructure. These scholarships are funded through grants awarded by the National Science Foundation.

Typical benefits for students in the SFS program include full tuition, fees and an allowance for textbooks. Recipients also receive a yearly stipend of $22,500 for undergraduates, or $34,000 for graduate students. Additionally, the program provides funding for professional development opportunities, conference attendance fees and travel.

This program is open to any United States citizens or permanent residents who are currently, or will be, full-time K-State students with three years or fewer remaining in their degree program during the semester they enter the SFS program. Recipients are expected to undertake coursework and/or research in the areas of cybersecurity or information assurance, and must maintain a minimum GPA of 3.2.

Upon completion of the program, recipients will be required to secure a full-time job in federal, state, local or tribal government for a period of time commensurate with the number of years the scholarship is awarded. Additionally, scholarship recipients will be required to complete a summer internship at a qualifying government agency.

Kansas State University researchers work to ensure that our automated daily reality does not compromise our safety. The National Security Agency and Department of Homeland Security has recognized our research by designating us a National Center of Academic Excellence for Research in Cybersecurity. K-State's world-class faculty and state-of-the-art facilities will enable graduates to better defend the world's networks in a connected, collaborative society.
Our Program

K State’s comprehensive cybersecurity specialization offered by the department of computer science within the College of Engineering includes five dedicated courses covering defensive and offensive aspects of cybersecurity, applied cryptography and secure software development.

Our commitment to one-on-one mentoring and individualized instruction provides our students with a personalized, well-rounded knowledge base, preparing them to solve cybersecurity challenges now and in the future.

Contact Us

For more information about the computer science program, or to apply, visit cs.k-state.edu.

Applications are accepted every semester.

Facilities and Research

Probabilistic and Information Theoretic Security (PITS) Laboratory

cs.k-state.edu/~amariucai

The PITS lab, founded by Professor George Amariucai in 2017, focuses on applying probability and information theory to cybersecurity with a broad cross-disciplinary scope. Projects include perfectly secure key establishment, physically unclonable functions (PUFs), secure information dissemination in social networks and biometric authentication. Lab personnel developed non-traditional key establishment protocols based on randomness harvested from ad-hoc wireless network metadata. They discovered the discharge inversion effect (DIE) in SRAM-based PUFs, which may cause catastrophic security failure. The team is also investigating computer-induced procedural biases to enhance continuous biometric authentication performance, and is working to model information-based user interaction in human networks to predict trends and contain the spread of misinformation.

Intelligent Systems, Computer Architecture, Analytics and Security (ISCAAS) Laboratory

cs.k-state.edu/~amunir/lab

The ISCAAS lab, founded by Professor Arslan Munir in 2017, investigates the design of secure and trustworthy intelligent systems, embedded systems, and cyber-physical systems via novel computer architectures, hardware designs, and machine-learning techniques that mitigate attacks on intelligent and complex adaptive systems. ISCAAS lab researchers have developed secure and dependable electronic control unit (ECU) architectures for automotive embedded systems that integrate security and dependability, while enforcing real-time constraints and minimizing energy use. Another result is a secure and dependable elliptic curve (ECC) processor resistant to power, timing and fault analysis attacks.

Research Opportunities

Systems and Network Security (SyNeSec) Laboratory

syneseclab.org

The SyNeSec lab, founded by Professor Eugene Vasserman in 2010, focuses on cross-disciplinary research on cyber-physical system security, including authentication, authorization and access control. An additional major area of research is security education and just-in-time intervention, usability, ease of use and risk perception. Notable accomplishments include protocols for Byzantine interoperability failure detection for medical systems, methods for non-intrusive black- and gray-box software integrity checking using power consumption and electromagnetic emissions of integrated circuits (sensitive enough to detect single instructions and/or operand changes), and deniable group off-the-record (GOTR) messaging. Currently, teams in the SyNeSec and SAnToS high-assurance software labs are developing safety-security co-design methodologies, and supporting software analysis and development tools to help safety engineers design secure systems, even without extensive (or any) security training.

Static Analysis and Transformation of Software (SAnToS) Laboratory

santoslab.org

SAnToS lab researchers develop foundational techniques, and robust tools and practical integrated methodologies for building safe and secure critical software systems. Since its founding in 1998, the lab has received more than $15 million in funding from national agencies and industry groups. Currently, SAnToS research is focused on building highly automated analysis and verification tools for embedded security devices, medical devices and building control systems.