National Center for Information Assurance and Security

Background
Technology is rapidly creating a highly networked world in which software pervades every aspect of society. Consequently, cyber-attacks represent a major threat to our nation that endanger mission-critical systems and the lives and assets those systems protect. Trillions of dollars and the well-being of millions of people currently depend on the correct operation of software. Recent reports to the National Academy of Sciences have urged development of software with evidence of correctness ("correctness certificates") that can be automatically verified by a third party. In response to these challenges, the U.S. Department of Defense (DOD) has developed a “System Assurance Strategy” that emphasizes security throughout the life cycle of a project and requires DOD programs to account for system vulnerabilities. Researchers at Kansas State University (KSU) have a world-renowned reputation for developing software design tools and technologies that result in the construction of safe, secure systems.

Description
The Center for Information Assurance and Security (CIAS) has a long history of research, teaching, and outreach in the cybersecurity area:
- In 2010, CIAS was designated as a National Center of Academic Excellence for Research in Cyber Security (CAE-R) by the National Security Agency (NSA) and Department of Homeland Security (DHS).
- Since 1999, CIAS researchers have collaborated with partners such as Rockwell Collins, Lockheed Martin, Boeing, HP, Honeywell, Microsoft, and Idaho National Lab to develop techniques for designing large-scale, secure, mission-control systems. Many new collaborations for cyber-security research and education are currently being explored.
- CIAS has contributed substantially to the building of tools to secure the U.S. national infrastructure:
  - The Argus group in CIAS has developed tools to address the defense aspects of cyber warfare. Researchers at National Institute of Standards and Technology (NIST) which maintains the National Vulnerability Database (NVD) are using some of those tools to develop security metrics.
  - A team of CIAS researchers received a 2003 NASA Turning Goals into Reality (TGIR) award for their work on techniques to verify software system functioning.
  - The DOD and its major contractors build complex, software-controlled, highly networked systems by integrating hundreds of suppliers and commercial off-the-shelf components. However, current design techniques, acquisition procedures, and vulnerability assessment capabilities are inadequate and often result in security vulnerabilities and cost over-runs. CIAS researchers have developed tools to efficiently design and assemble large software systems at low cost.
- CIAS researchers have received several prestigious awards, including four CAREER awards from the National Science Foundation.

The proposed project will enhance CIAS capabilities in order to address challenges that confront the next generation of complex cyber-physical systems. The project will (1) tackle challenges for designing “zero-failure” mission-critical systems at lower cost and decreased completion time, (2) develop cyber-defense solutions to protect the U.S. critical infrastructures, and (3) partner with local, state, and national agencies and industry to educate people concerning cybersecurity challenges. CIAS is uniquely poised to address these challenges because of the following specific efforts:
- Utilizing partnership with various federal agencies, CIAS will develop threat assessment tools that holistically encompass system security management. Enabling techniques based on automated correlation and threat analysis will be researched in order to generate high-confidence alerts.
- CIAS will develop collaborations with companies specializing in cyber-security and bio-security in order to build a vibrant regional center and provide an attractive environment in which those companies would desire to expand to Manhattan, Kansas.
- A shortage of cyber-security engineers has been consistently cited as a potential threat to U.S. national security. CIAS has led development of and will continue to develop educational material for security.

Relevance
KSU’s CIAS has a world-renowned reputation of developing technologies that lead to the creation of secure software systems. Because of existing collaborations with leading cyber-security companies and the anticipated arrival of National Bio and Agricultural Defense Facility (NBADF), CIAS has the potential to form alliances with and attract a multitude of cyber- and bio-security companies to Manhattan. This project will stimulate these endeavors and establish a regional center in which the future cyber-security workforce can be trained.

Point of Contact
Dr. Kathleen Kaplan, MIT Fellow, AFOSR
875 Randolph Street
Arlington VA 22203
703-696-7312, kathleen.kaplan@us.af.mil
Summary: We adopt a human-centered approach in order to understand cybersecurity operation. Researchers extract “tacit knowledge” embedded in the operation, make that knowledge explicit in models and algorithms, and then use the knowledge to fundamentally improve cybersecurity.

Opportunity: Lack of effective automation in cyber defense has plagued cybersecurity for decades. Although attempts have been made to create technologies for automation, most technologies are not designed with consideration of human users. Few researchers strive to understand security operations before attempting to design technologies that purportedly help them.

Solution: We adopt a multidisciplinary approach in order to address the cyber defense challenge. In partnership with anthropologists, we study cybersecurity operations in their “native habitat.” Additional partnerships with security practitioners allows us access to tacit knowledge and opportunity to subject that knowledge to analysis and modeling, thereby creating improved, applicable technologies.

Impact: We have conducted ethnographic fieldwork at multiple security operation centers (SOCs) in higher education institutions and commercial firms. Findings from the fieldwork have been very informative to the research and practitioner community. One SOC analyst asserted, "This anthropological study has helped us understand the big picture of our work!"

Equipment and Expertise: Cybersecurity, Anthropology, Cybersecurity Operations