Cybersecurity, Privacy, and Trust

Proposal Leads:
Aidan Browne, Associate Professor, College of Engineering
Bill Chu, Professor, College of Computing and Informatics
Heather Richter Lipford, Professor, College of Computing and Informatics

Participating Units:

- College of Computing and Informatics
  - ➔ Department of Software and Information Systems
  - ➔ Department of Computer Science
- The William States Lee College of Engineering
  - ➔ Department of Electrical and Computer Engineering
  - ➔ Department of Engineering Technology and Construction Management
- Cato College of Education
  - ➔ Department of Educational Leadership
- College of Liberal Arts & Sciences
  - ➔ Department of Political Science and Public Administration
  - ➔ Public Policy Ph.D. Program
- Belk College Of Business
  - ➔ Department of Business Information Systems and Operations Management

Targeted Category:
Existing and Emerging Excellence

Additional Keywords:
Information assurance, Resilience, Cyber-physical systems

Executive Summary

The field of cybersecurity is focused on issues related to the confidentiality, integrity, and availability of digital information. With the widespread use of digital technologies, core issues that are the focus of research in cybersecurity have an ever-growing direct impact on people's lives, as well as our culture and society at large. Privacy and Trust are two areas that directly address the impact of cybersecurity on research issues in data and social sciences. Privacy is focused on preventing abuses of personal information, making sure the use of information is authorized, and assuring awareness of information collection. Trust is focused on ensuring the integrity of public information, responsible use of data, and resiliency of the digital infrastructure upon which vital digital and social services depend.

At the inception of the College of Computing and Informatics 20 years ago, UNC Charlotte was at the forefront of focusing on cybersecurity, which has remained a key strength and broadened to include faculty in 4 other colleges. UNC Charlotte has been recognized by the National Security Agency and the Department of Homeland Security as a Center of Academic Excellence in cybersecurity research since 2008. The 17 faculty involved in this proposal are all members of the CyberDNA Center, currently led by Dr. Bill Chu, which has an established track record of promoting cybersecurity research, education, and community service. In the past five years, the CyberDNA center has attracted faculty from a majority of colleges at UNC Charlotte as a platform of collaboration on research and education issues related to Cybersecurity. In particular, research issues related to Privacy and Trust are emerging areas of excellence.

In the past five years, $44.9 million in external funding has been awarded to UNC Charlotte for research and education activities related to cybersecurity. Research activities are funded by a variety of federal agencies such as the National Science Foundation and Department of Defense, demonstrating alignment with national priorities. Additionally, support and collaboration with local companies demonstrates that faculty research directly contributes to economic development. Cybersecurity, privacy, and trust research impacts four Ph.D. programs on campus: Computing and Information Systems, Electrical and Computer Engineering, Public Policy, and Curriculum and Instruction. There has been a significant number of well-funded, collaborative research projects that involve faculty from different colleges over the past five years. Based on the level of activities and sustained interest among faculty and students, we believe that such collaboration will continue to experience healthy growth.

Cybersecurity is also a critical aspect for other prominent research areas at UNC Charlotte such as Smart Cities, Energy, Data Science, Artificial Intelligence, and Bioinformatics. Synergetic relationships can lead to increased research activities in all of these areas. With heightened societal attention on the safety and integrity of digital information as well as the reliability of information infrastructure, UNC Charlotte is well positioned to increase its research profile by leveraging this existing strength and making strategic investments in participating colleges to make Cybersecurity, Privacy, and Trust a focus area of excellence.

Evidence of Strength and Excellence

The research program in cybersecurity at UNC Charlotte is recognized by the foremost national agencies in security. The National Centers of Academic Excellence in Cybersecurity is managed by the National Security Agency (NSA) to establish standards for cybersecurity curriculum and academic and research excellence. UNC Charlotte has been recognized as a Center of Academic Excellence in Cyber Defense Education since 2001, and in Cyber Research since that designation was first available in 2008. These recognitions have been continuously granted through the present. The research recognition is based on the quality of peer-reviewed publications in cybersecurity as well as research expertise and impact.

The National Science Foundation has also recognized UNC Charlotte through the establishment of an Industry-University Cooperative Research Center. UNCC faculty launched the Center for Cybersecurity Analytics and Automation (CCAA) in 2013, an IUCRC funded by the NSF, in collaboration with George Mason and Colorado State Universities. This center is only one of 20 such centers in the area of Information, Communication and Computing in the U.S. Center research is supported by industry and government members, which have included NIST, NSA, Bank of America, Northrup Grummon, CyberRisk Research, and several other corporations.

Faculty research has been extensively supported, with $43.9 million in active grants over the past 5 years alone. Participating faculty members have a wide range of research expertise across many specialized areas of cybersecurity, privacy and trust. Most activities can be described by one of the following core thrusts:

- **Hardware and Infrastructure security** deals with the security of hardware, networks, and software that provide infrastructural support for the everyday computing needs of businesses and individuals. External funding: 6 awards by NSF. Collaborative partners include: California Institute of Technology, Carnegie Mellon University, Florida State University, Jet Propulsion Laboratory, Lawrence Berkeley National Laboratory, North Carolina A&T State University, and University of North Texas
- **Privacy and digital citizenship.** Research includes privacy-preserving data analysis, policies for mobile devices/applications and social networks, policies and ethics for genomic and health data, and research on digital citizenship education for K-12 students. External funding: 5 awards by NSF.
- **Usable security** is concerned with designing security and privacy systems, including access management and policy settings, that can be easily used by people. External funding: 6 awards by NSF and Bank of America.
- **Security analytics and automation** aims at detecting and mitigating threats facing enterprises, exploring solutions with cyber threat intelligence, adaptive cyber defense, malware analysis, and cyber deception. External funding: 9 awards by NSF, ARO, NSA, ONR, Bank of America and Wells Fargo. Collaborative partners include Carnegie Mellon University, George Mason University, and University of Texas at Dallas.

Faculty utilize their expertise within domains requiring secure, private, and trustworthy operation. This research aims to not only examine core contributions within cybersecurity, but to enable advances in technology and infrastructure that address critical societal issues. Each of the

below thrusts is funded by large-scale external grants from a variety of federal agencies, with collaborations involving a number of the participating faculty.

- **Information Infrastructure:** Developing secure and private infrastructure to accelerate data-driven research and multidisciplinary collaboration. Contributions include a dynamic secure container-based infrastructure which enables online adaptive analytics from unshareable data at distributed locations.
- **Energy:** Identifying potential cybersecurity attacks within the power grid and smart energy grid. Research funded by Duke Energy has contributed guidance and strategies for mitigating security risks.
- **Manufacturing:** Developing and implementing unique approaches to improving manufacturing capabilities and information security within the US manufacturing and defense industrial base (M&DIB) and the digital thread that serves as an information conduit throughout the entire US manufacturing supply chain. Contributions include a test bed for prototyping new technologies as well as determining the ability of small to medium sized enterprises to fulfill the minimum security controls defined by federal regulations.
- **Cyber-physical systems and Internet of Things:** Securing Internet-connected devices that interact with the physical world. Funded by the NSF, DOE, and the Department of Labor, research contributes to the security of control systems such as within the power grid and water treatment facilities, and has identified vulnerabilities and user behaviors of consumer devices.

These research thrusts have resulted in more than 187 published papers related to cybersecurity, privacy, and trust in the last 5 years. Examples of these publications can be found in faculty member biosketches. Publication venues span top-ranked journals and conferences focused on cybersecurity and privacy, as well as venues focused on the domain areas highlighted above. We note that in computing, conferences are often the primary publication venue, with rigorous peer-review and low acceptance rates.

Faculty are also heavily involved in mentoring and training the next generation of researchers. There are currently 23 Ph.D. students in cybersecurity, privacy, and trust. Our faculty have graduated 18 students in the last 5 years who have gone on to academic and industrial positions throughout the country, including 12 in tenure-track faculty positions. In addition to supporting students on research grants, faculty have received competitive grants to fund cybersecurity Ph.D. students through the Graduates in Areas of National Need (GAANN) and the Scholarship for Service (SFS) programs, funded by the Department of Education and NSF respectively.

Finally, our faculty are contributing to funded educational research and curriculum development activities, with over $2.2 million in awards in the past 5 years. In addition to developing new courses that follow the latest advances in computer security (e.g. cloud computing security, quantum computing, wireless and 5G security), participating faculty have also designed stackable modules on security and privacy enforcement for other disciplines such as the power industry and smart grid, manufacturing, K-12 schools, and intelligent transportation. For example, UNC Charlotte is part of a coalition of universities and community colleges participating in a nearly $6 million Cybersecurity Workforce Development grant funded by the NSA and DHS, developing a cybersecurity certification-based national training program.

Alignment with Regional and National Priorities

Cybersecurity is a critical feature of many of the innovations of the 21st century. For example, our faculty are involved in research that falls within 4 of NSF's 10 Big Ideas, including the Future of Work at the Human-Technology Frontier, Harnessing the Data Revolution, Mid-Scale Research Infrastructure, and Quantum Leap. Cybersecurity is a critical aspect of the Industries of the Future listed by the Office of Science and Technology R&D 2022 Priorities, namely Quantum Information Science, Advanced Communication Networks, Advanced Manufacturing, and IoT. Security is also one of the five OSTP priorities, with cybersecurity playing an ever-growing role in the safety and resiliency of individuals, businesses, communities, and government agencies.

The Charlotte economy is heavily reliant on technology innovations, including within cybersecurity, and regional organizations have established strong research relations with our faculty. Through external contracts as well as the Center for Cybersecurity Analytics and Automation, collaborative research has been conducted with many local organizations. In addition, Bank of America has provided funding for an endowed professorship in Cybersecurity. Cybersecurity faculty also serve the region through cutting-edge curricula and activities that bring together students and professionals. The cybersecurity concentration of the undergraduate degree in Computer Science has 251 students, while the Master's degree in Cybersecurity, the first in the Carolinas, currently serves 95 students. The UNC Charlotte Annual Cybersecurity Symposium, held annually since 2001, serves the professional education needs of the cybersecurity community through nationally renowned speakers, and exposes UNC Charlotte students to best practices of cybersecurity in industry.

In addition to our current strengths, we see a number of emergent areas for further growth. Cyberspace has emerged as a domain of conflict among political and criminal actors. As a result, cybersecurity is not only a technical challenge but also a political and social challenge: anticipating and understanding cybersecurity incidents requires situating these events within the social and political contexts in which they occur, involving researchers within political science, public policy, and criminal justice. These developments require incorporation of research on cyberspace regulation and governance, privacy laws and data protection, and ethical frameworks and codes of countries with diverse political cultures. Cybersecurity crosses national and territorial borders, compelling multilateral regional organizations, e.g., the Asia Pacific Economic Cooperation (APEC) forum and the Carribean Community (CARICOM) to create cybersecurity frameworks and codes of practice to thwart activities of criminal actors and mitigate conflicts among political actors globally. As countries increase implementation of the IoT, privacy and trust become forefront of regional and national priorities in gaining technology acceptance and advancement amid challenges of cybersecurity risks.

Finally, Cybersecurity, Privacy and Trust is strategically positioned to promote synergistic growth with other research strengths at UNC Charlotte. These emerging research areas include: trust and security of machine learning algorithms must be adequately addressed for the wide adoption of AI applications; security and privacy are key requirements for the design of a smart city, and data analysis in finance and health care must comply with privacy policies as well as achieving business benefits.

Supporting Documents

The following faculty are participating in this proposal, as faculty doing research within cybersecurity, privacy, and trust.

Name	Title & Department	Contribution/Expertise
Aidan Browne	Associate Professor, Engineering Technology and Construction Management, William States Lee College of Engineering. Director, M.S. Applied Energy & Electromechanical Systems Program	Cyber-physical system security; Security for Manufacturing.
Badrul Choudhury	Professor, Electrical & Computer Engineering jointly with Systems Engineering and Engineering Management, Lee College of Engineering, Asst. Director, EPIC	Cyber-physical systems; energy forecasting; data-driven optimization
Bill Chu	Professor, Department of Software and Information Systems	Application security, and cybersecurity analytics.
Benjamin J. Radford	Assistant Professor, Political Science & Public Administration; Public Policy Ph.D. Program Affiliated Faculty Member, School of Data Science	Machine learning for cybersecurity incident detection and attribution. Cyberspace as a domain for political conflict.
Cheryl Brown	Associate Professor and Chair, Political Science and Public Administration; Affiliated Faculty in School of Data Science, Social Aspects of Health Initiative (CLAS), and CyberDNA Center (CCI)	Data privacy and trust, technology and culture, global privacy regulations and ethical responsibility, health data privacy and ethics in autonomous and intelligent systems, algorithmic and implicit bias in healthcare and education
Fareena Saqib	Assistant Professor, Department of Electrical and Computer Engineering	Hardware security and trust, supply chain risk management and security, and computing for embedded electronic devices.

Florence Martin	Professor, Learning, Design and Technology, Cato College of Education	Cybersecurity Education for K-12 students and educators, Educational Technologies and Online Education
Heather Lipford	Professor, Dept. Software and Information Systems Associate Dean, College of Computing and Informatics	Usable Security and Privacy. Investigates the security and privacy needs and behaviors of users, particularly within the Internet of Things and for software developers.
Jinpeng Wei	Associate Professor and Graduate Program Director, Software and Information Systems	System security and active cyber defense (e.g., cyber deception). Theory, methods, and tools that enhance the security of widely used systems software in a non-traditional way, in the context of real cyber attacks and new threats in emerging computing environments (e.g., Internet of Things).
Lina Zhou	Professor, Business Information Systems and Operations Management	Online deception detection, usable mobile user authentication
Liyue Fan	Assistant Professor, Computer Science	Data Privacy. Develops provable privacy methods for data sharing and analysis, e.g., for health and behavioral research domains.
Meera Sridhar	Assistant Professor, Software and Information Systems	Software and Systems Security, Mobile, Web & IoT Security, Cyber Physical Systems (CPS) Security
Mohammed Shehab	Associate Professor, PhD Graduate Program Director College of Computing and Informatics	Usable Security, Software and Systems Security, Mobile Systems, Access Control, and Privacy
Tom Moyer	Assistant Professor, Dept. Software and Information Systems	System security, resilient systems, and smart-building security
Weichao Wang	Professor and Chair, Dept. Software and Information Systems	Wireless network and cyber-physical system security, infrastructure protection

William Tolone	Associate Dean, College of Computing and Informatics; Professor, Department of Software and Informations Systems	Integrated Modeling and Simulation, Critical Infrastructure Analytics and Security, Visual and Data Analytics
Yongge Wang	Professor, Dept. Software and Information Systems	Cryptography, post-quantum security, blockchain