Cyber Security and Privacy Cluster

1 Evidence-based Impact Statement

In 2011, the White House Office for Science and Technology Policy and the National Science and Technology Council's "Networking and Information Technology Research and Development Program" established a national cyber research and development strategy that aims to foster research in this area. Budgets for research have been increasing, and in 2014 budgets for cyber security and information assurance were $802M, with large amounts in DARPA, NSA, and NSF. "Cyber" is at the top of everyone's list in the Department of Defense (DoD) in terms of needs and funding (see Appendix B). In 2015, cyber security continues to be a major bipartisan national priority both in terms of funding and economic goals, as explicitly stated by President Obama in his January 20th State of the Union address: "No foreign nation, no hacker, should be able to shut down our networks, steal our trade secrets, or invade the privacy of American families, especially our kids." Moreover, there is projected to be a national deficit of 400,000 Cyber professionals in the United States and an estimated 1,000,000 shortage globally. In April 2015, the Secretary of Defense issued the DoD's cyber strategy. Key points in this strategy are to accelerate research and development to build cyber capabilities and to establish a cyber modeling and simulation capability. Modeling and simulation fit well with UCF strengths.

Businesses are also very aware of the need to protect their security and the privacy of their customer's data. UCF cyber security students have received internships and job offers with major corporations including Microsoft, Google, Apple, Amazon, Facebook, Yahoo!, Disney, and Raytheon. There are over 200 students in the UCF Collegiate Cyber Defense Club, demonstrating a large student interest. A student team from this club won the national Collegiate Cyber Defense Competition (CCDC) in 2014 and again in 2015. UCF also has a hardware security team that has competed in the Final rounds in NYU Poly's CSAW Embedded System Challenge and won second place in both 2013 and 2014. The official job projections in cyber areas are better even than those for other computer-related jobs; according to the Bureau of Labor Statistics, Occupational Outlook Handbook (2014-15 Edition), "Employment of information security analysts is projected to grow 37 percent from 2012 to 2022, much faster than the average for all occupations."

2014 CCDC team with the Alamo Cup

2015 CCDC team with the Alamo Cup

2 Vision for the Cluster

We envision an energetic, university-wide research cluster that moves the needle for UCF in both research and teaching. This cluster will focus on security (a technical construct), privacy (a social construct), and their intersection (a socio-technical system). Research and consulting in these areas

will aid both businesses and government, and will enhance faculty expertise for teaching students. Work on these problems involves: human users, physical facilities, hardware, software, communication protocols, and potential attackers. For example, many security breaches are not caused by technology problems, but by people who use weak passwords or click on malicious email links. There are numerous ways to exploit infrastructure through such "social engineering" attacks. Therefore, the modern world needs a comprehensive combination of research that provides integrated solutions to both the human and technological causes of security and privacy problems. In order to produce comprehensive solutions, the work will span many disciplines, including Computer Science, Computer Engineering, Industrial Engineering and Management Systems, Legal Studies, Mathematics, Optics and Photonics, Philosophy, Political Science, Psychology, and Statistics. Integrating the technical and human aspects will set us apart.

We plan to hold regular meetings to work on problems of mutual interest. The plan is to alternate loosely structured sessions focused on:

- Discussions about the landscape of problems, policies, and ethical issues in cyber security and privacy, with the idea of discovering what problems are important and sensible to address in the current social and political context.
- Brainstorming about approaches to solving some class of problems, with the idea of exchanging information about how such approaches could be evaluated.
- Presentations on ongoing work, with the idea of getting feedback from multiple perspectives.

Through both structured and unstructured events, cluster members will also have opportunities to meet and socialize informally, so that they can form close working relationships.

2.1 Short and Long Term Cluster Objectives

The short term objectives of this cluster are to conduct world-class and impactful research on:

- Security and privacy for the Internet of Things (IoT).
- Tools and methods for preventing, discovering, and mitigating:
    - Security and privacy breaches,
    - Insider threats, and
    - Privacy risks and source-based self-censoring.
- Evaluation techniques for determining the efficacy, efficiency, and usability of such tools and methods.

The IoT is an area of rapid technological advance where humans interface directly with devices such as refrigerators and thermostats. However, the IoT opens new avenues for attack on systems, such as attacking through a network that maintains connectivity with devices (such as refrigerators or heating systems) for predictive maintenance. Software developers and systems analysts need tools and design methods that help prevent security and privacy breaches. By *tools* we mean software programs, but tools can also be embodied in hardware. By *methods*, we mean techniques (such as checklists, best practices, or algorithms) for developing software/hardware or for managing software or networks. Tools and methods can embody insights into topics such as: authentication, program analysis (using programs to discover properties of other programs), reverse engineering of malware, and forensics, as well as methods for secure software development. IT operations staff and cyber security professionals also need tools and methods to help discover when sophisticated attacks are underway and how to mitigate them. People's concerns about privacy, especially from the use of data gathered by IoT devices and other systems,

can cause underutilization of existing capabilities as a result of self-censorship. The slow penetration of information sharing across the healthcare sector is an example where physicians omit information from patient records due to such concerns. Modeling and simulation can be used to test system designs and how they affect such privacy concerns. Businesses and governments also need tools and methods for preventing, discovering, and mitigating attacks by insiders (people with some legitimate access). These insider threats were recently reinforced by the Snowden case. Having a large population of students interested in cyber security and privacy (including the UCF Collegiate Cyber Defense Club, which has over 200 members), makes it possible to do scientific studies of the efficacy, efficiency, and usability of such tools and methods. Such studies would not be possible at many other universities. The expertise needed to carry out such studies, along with other user studies related to security and privacy meshes well with our expertise in Psychology, Statistics, Industrial Engineering, and Modeling and Simulation. The problems of identifying and preventing insider attacks, promoting capability usage, as well as preventing and detecting attacks and omissions due to privacy concerns could be approached, in part, with AI and statistical techniques (data analytics), and solutions could apply expertise in team processes and team training (through modeling and simulation), all of which are UCF strengths. The analytic capabilities could also address other problems with significant security components (such as the Smart Grid). UCF's capabilities in human-computer interaction and visualization can also address these problems, as well as address the DoD's needs for modeling and simulation capabilities.

The long-term objectives of this cluster are to:

- Develop fundamental breakthroughs in security and privacy, as demonstrated by novel tools and methods.
- Develop fundamental knowledge about the factors that make tools and methods effective, efficient, and usable.
- Respond quickly and successfully to opportunities for funded research. This can be done in conjunction with industry partners for some federal grants and contracts.
- Give expert advice and consulting to government and businesses.
- Provide talented and well-trained students for government and businesses. This will help ensure that the cluster reflects the needs and interests of industry.

UCF has an existing base of researchers who can investigate the above topics. What UCF currently lacks, however, is a group of faculty who are primarily engaged in cyber security and privacy research, and who will lead our existing faculty towards solutions of large and complex problems. This new leadership will make it possible to capitalize on this area's growing opportunities for interdisciplinary and multidisciplinary work. Detailed recruitment plans and plans for enhancing research capacity are developed below.

2.2 Alignment between Cluster Objectives and Strategic Priorities

CECS has a strong interest in cyber security, due to interest from students and outside businesses and government. While CECS has two professors who primarily do research in security, and has hired one that does research in privacy, it does not have enough dedicated faculty to capitalize on many governmental and business funding opportunities. CECS hosts the Collegiate Cyber Defense Club (Hack@UCF); a group that is well-known, both on campus and beyond, and has over 200 members. Its success, and the success of UCF's hardware security team, make supporting cyber

security a top educational and research priority. CECS is investing in new hires, but believes that this cluster can knit together efforts across UCF, leading to greater impact.

COS has an emerging interest in cyber security and privacy, especially with respect to the role that research from Psychology, Political Science (with a new PhD program in Security Studies), Sociology, and Statistics can assume in Cyber Security. Specific areas of research in the social and behavioral sciences include: (a) the description, mechanisms, and identification of external and internal (insider) threats in organizations, (b) the selection, training, and career progress of cyber security personnel in both the offensive and defensive roles, (c) the study of teamwork in cyber security applications, and (d) the development, testing, and usability of cyber security tools, such as threat visualizations, etc. Related research interests from Statistics include efficient analysis of "big data," as well as supporting the analysis of "threat signatures" in communications and keystroke data, an area that is also of interest to the modeling, simulation, and training researchers at the Institute for Simulation & Training (IST). Mathematics has an interest in coding theory and cryptography (the latter being a crucial need at UCF).

IST, a multi- and inter-disciplinary unit with resident faculty from COS, CECS, CAH, and CON, is uniquely positioned to support this cluster. Also, due to its close interactions with all branches of the DoD, and its work with agencies such as the Department of Homeland Security (DHS), the Defense Intelligence Agency, Intelligence Advanced Research Projects Activity, the Nuclear Regulatory Commission, and the Federal Aviation Administration, IST can provide a ready-made conduit for critical tools and methods in cyber security and privacy. IST will be key to helping the cluster addressing the DoD's strategic priorities in cyber modeling and simulation.

We all believe that security and privacy are important and growing areas of opportunity and will remain so for the foreseeable future. Integrating the social and behavioral sciences with more technical areas will position UCF to compete and make fundamental contributions.

3 Cluster Leader and Participating Faculty

This cluster will initially be led by Professor Gary T. Leavens, chair of Computer Science. (We expect that leadership will eventually pass to a senior hire.) The following form the core faculty of the cluster, who are committed to ensuring its success:

- Computer Science (CS): Mainak Chatterjee, Ratan Guha, Gary Leavens, Cliff Zou
- Electrical and Computer Engineering (ECE): Yier Jin, Peter Yuan.
- Industrial Engineering and Management Systems: Waldemar Karwowski
- IST: Randall Shumaker
- Political Science: Ted Reynolds,
- Psychology: Peter Hancock, Florian Jentsch
- Statistics: Morgan Wang

The following are associated faculty who are interested in helping with research. They are from the above units and also from Legal Studies, Management, Marketing, Mathematics, Optics and Photonics, and Philosophy: Maureen Ambrose, Mostafa Bassiouni, Carol Bast, James Beckman, Rick Biehl, Joseph Brennan, Shawn Burke, Corey Bohil, Mason Cash, Robert Folger, Roger Handberg, Sumit Jha, Mark Johnson, Dana Joseph, Amit Joshi, Peter Kincaid, Sheau-Dong Lang, Joseph LaViola, Mingjie Lin, Ronald DeMara, Michael Macedonia, David Metcalf, Timothy

Ravich, Lauren Reinerman-Jones, Martin Richardson, Mark Schafer, Marshall Schminke, Mubarak Shah, Nancy Stanlick, Damla Turgut, Guo-Jun Qi, Zhihua Qu, and Petros Xanthoupoulos. The associated faculty will collaborate on research as opportunities arise, and will participate in discussions about security and privacy topics, but are not committing to work primarily on the cluster's topics.

4 Graduate and Undergraduate Curriculum Statement

4.1 Graduate Curriculum

The Modeling and Simulation Graduate degree program graduate certificate in Modeling and Simulation of Behavioral Cybersecurity. This program offers four cyber courses.

CECS offers 6 courses related to cyber security and hardware security at the graduate level. CS offers a MS in Digital Forensics degree that will be broadened to include more cyber security if more faculty can be hired in this area.

Political Science has a new graduate certificate in Intelligence and National Security, as part of the Intelligence Community Center for Excellence in Intelligence (IC-CEI) grant; this certificate will be offered starting in fall 2015. The PhD program in Security Studies needs faculty that support the social science aspects of cyber. The IC-CEI grant can arrange internships in cyber security and privacy at federal agencies such as the Dept. of State, IARPA, and the DoD.

4.2 Undergraduate Curriculum

UCF currently has no undergraduate degree in cyber security, but there are a number of courses offered by a variety of units (CS, ECE, Modeling and Simulation, Political Science). CS offers a Secure Computing and Networks Minor for undergraduates. Political Science is offering a course in Cybersecurity (fall 2015). In addition, Political Science has designed an interdisciplinary undergraduate minor on Intelligence Studies as part of the IC-CEI grant; courses on cyber security would enrich the current proposal.

Currently, UCF is applying to become designated as a National Security Agency (NSA) Center of Excellence in Cyber Operations. The courses behind this application are the CS and IT bachelor's degrees along with the Secure Computing and Networks minor. In the process of earning their degrees, students need to take several courses; CS is proposing that 15 specific courses that cover the NSA required Knowledge Units earn these students an undergraduate certificate. We plan to grow this certificate program into a BS degree program in cyber security and privacy.

5 Proposed Detailed Hiring Plan

The focus of hiring is to bring together UCF interests in cyber security and privacy. These interests are aligned with the cluster's short-term and long term objectives, and are shown as the rounded rectangles in Figure 1 below. We propose to hire at least 5 new faculty, which would be augmented by research faculty hired by the IST. The hires A-E (in ovals and circles) are explained below, but overall are targeted to bring in leaders who will tie together different research interests among our existing faculty.

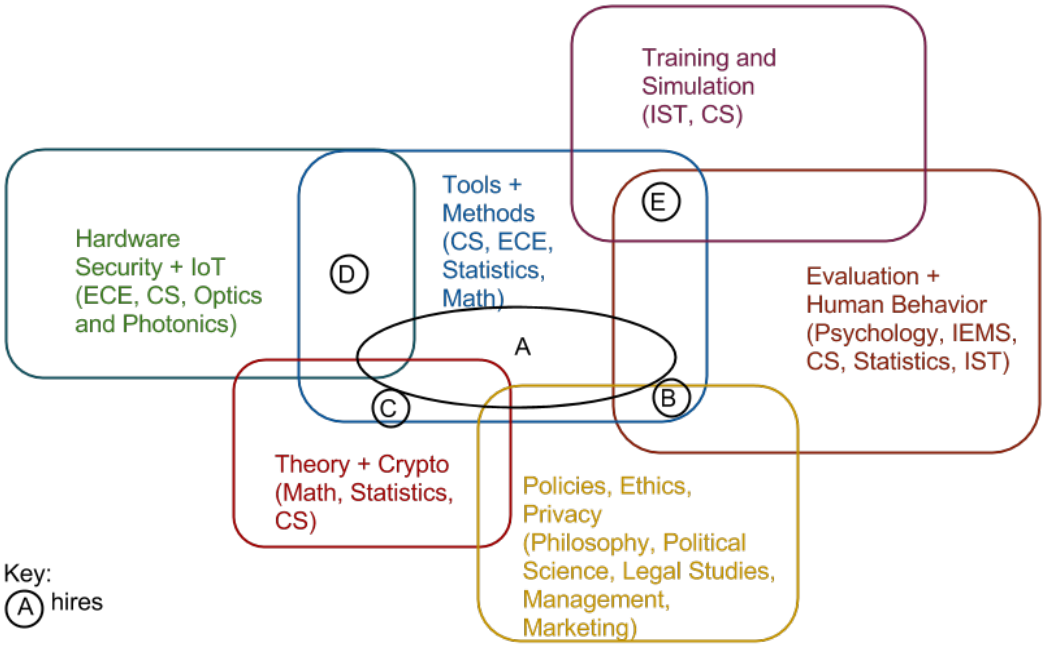

Figure 1: Relationship of research areas, units, and key hires.

Hire A would be a senior person who has both technical and leadership experience in cyber security and privacy, and whose expertise can unite our research from hardware and the IoT, through tools and methods, to evaluation of human behavior. This person also needs to have a grasp of the theory of security and privacy as well as policy and ethical issues. Such a polymath would be someone who has been playing a leading role in a center for security at a research university, and would form the "glue" that unites and leads our collaboration. Aside from someone who already leads such a center, we would look for someone senior who has not yet formally led such a center, but who is ready to lead our cluster.

Other hires would be targeted to bring together areas that already have overlapping research interests. Hire B would be targeted at the intersection between evaluation of human behavior and the policies and ethical considerations that influence those behaviors (as well as the tools and methods that enforce them). Hire C would fill a crucial educational and research gap at UCF in theory of security, particularly in cryptography. Hire D would unite research interests between software and hardware security. Hire E would unite research interests between training and simulation and evaluation of human behaviors, with an interest in evaluation of tools and methods for cyber security and privacy.

5.1 Hiring Details

All hires would be done by a cluster committee and would choose their tenure home based on their personal preference. Joint appointments would be made to link together the corresponding interests.

Space will be needed for offices for the new faculty hired in the cluster; in total 5 offices will be needed (roughly 110 square feet each, and perhaps a larger one for the senior hire). We prefer to

have all the new faculty hired located close to each other, and to have lab space for the graduate students of these faculty also located close to each other and to the new faculty offices. Lab space for graduate students would be about 20 square feet per student, and we estimate about 5 students per new faculty member in the long run (so a total of about 500 square feet). When these hires start, they would typically have fewer students, so in the short run we would only need space for about 2 students per new hire (except for the senior person, who might have about 4 students). Thus in the short term we could make do with about 240 square feet of lab space. We would like to locate the offices and labs for these new faculty centrally on the main UCF campus. Research in the cluster needs at least one lab with whose network can be made independent of the university's network (using routing equipment), so that network security experiments can be run.

If new space to co-locate the cluster is not available, then co-location of these new faculty with the research interests that they should bring together is also a possibility, especially in the short term. In any case, we plan to leave current faculty (and their students) in their existing offices (and labs).

Recruiting senior faculty will be a particular challenge. We plan to leverage our industry partnerships, given their close ties to the research community in cyber security and privacy. We will start active recruiting efforts by hosting visits from leaders who are near the top of the leadership of prominent cyber security centers (see Section 7). The process for hire A may take more than a single academic year to accomplish and will need flexibility and patience from UCF. To retain our hires we must pay them a generous salary, give them reasonable teaching loads, and provide them with good space and equipment. Retention of these faculty will also depend on the core faculty (current and those hired) coming together as a cohesive group in regular meetings and making progress on research together. The current core faculty are committed to this goal.

6 Further Plans

6.1 Plans for Achieving National and International Prominence

Our long term plan for achieving national and international prominence for our research is to gain a reputation for careful, scientific evaluation of the efficacy, efficiency, and usability of our proposals in demonstration prototypes. This would not stop UCF researchers from publishing ideas or theoretical papers before experimental evaluation, but we are committed to careful evaluation of tools and methods as soon as possible. This kind of evaluation will yield insights to both the faculty designing tools and methods as well as the faculty doing behavioral studies. Through such behavioral studies we hope to gain insights into the minds of technical specialists and ordinary users, which can contribute to fundamental knowledge of human behavior and also to ideas for developing better tools and methods. We believe that gaining a reputation for careful scientific evaluation will make a solid reputation for work done at UCF, and will also lead to increased understanding, not only among UCF researchers, but within academia, government, and business.

Furthermore, we plan to leverage the broad spectrum of interests in this cluster to ensure that our work is aimed at real problems and that the solutions proposed make sense in the context of society, ethics, and politics. We will ensure that problems and solution approaches are thoroughly discussed with our (mostly associated) cluster members in Legal Studies, Management, Marketing, Philosophy, and Political Science. This kind of exchange will increase the understanding of all the

faculty in the cluster as well as helping ensure that the problems and solutions we pursue are grounded in reality. In the long run, this will help the cluster enhance its reputation and impact.

Our short term plans for achieving national and international prominence are to focus on areas that leverage our unique capabilities (such as expertise in modeling and simulation) or that are becoming increasingly important, but which have not yet had an overwhelming number of researchers exploring them. In the short term we plan to focus on security and privacy for the Internet of Things (IoT) and on insider threats. Although these areas are not unknown to other researchers, their prominence is relatively new. In particular, they have only recently become a focus of funding efforts. In both of these areas, we plan to leverage our unique balance between the technical and behavioral aspects of cyber security and privacy.

6.2 Plans for Increasing Scholarly Work

Our plan for achieving national and international prominence does not rely on increasing the amount of scholarly work written and submitted for publication, but rather on increasing the quality of the cluster's collective scholarly output by making sure that it addresses real problems, has solutions that are ethically sensible in the current social and political context, and by careful, scientific evaluation. The scientific evaluations will be done in a cooperative manner, and may result in separate publications about evaluation methods. By this strategy, we plan to increase our reputation and the impact of our work, enhancing its influence (e.g., citations). This increased impact should lead to increased funding, which will result in more talented graduate students being hired, hence in more quality publications. Cooperation, between technical and behavioral interests in the cluster will be the key to getting such careful, scientific evaluations done without delaying publication, and in enhancing the value of cooperating with other faculty in the cluster.

6.3 Plans for Enhancing Research Capacity and Funding Base

Fundamentally, adding new faculty will allow UCF researchers to pursue large research projects and contracts. It would also help UCF leverage our growing relationship with cyber security firms (such as Raytheon). Having faculty leaders at UCF to focus efforts in this area and to get more faculty thinking about cyber security and privacy issues will draw more faculty time and talent to this area.

Currently UCF does not have funding from some federal agencies (e.g., DHS) in cyber security and privacy. Our senior hire (hire A) will have appropriate connections and will take groups of junior faculty to visit funding agencies and promote the strengths/capabilities of the cluster so that funding to the cluster can be enhanced.

Our plans for enhancing our research capacity and funding base also include becoming designated as an NSA center for cyber operations, which will give us access to funding opportunities that we would not otherwise have. This designation hinges on various technical courses and a commitment of faculty to consider cyber security and privacy in an integrated manner in various courses.

6.4 Plans for Enhancing Interdisciplinary Publications in Multiple Disciplines

Our plan is that interdisciplinary publications will emerge in several ways. First, the cluster's overall emphasis on collaboration between technical and behavioral interests and its commitment

to careful, scientific evaluation of tools and methods will result in a series of interdisciplinary publications. Second, the interactions between cluster members at the cluster's regular meetings to brainstorm about problems and solutions will spark papers that explore the landscape of problems and solutions. Such papers that are grounded in both technical knowledge and a knowledge of social, political, legal, and business perspectives will be able to use reasoning that is not limited to one of these perspectives. Finally, we have planned our hiring strategy to encourage interdisciplinary research between closely-related research areas, as each cluster hire is targeted to foster cooperation between at least two broad areas of interest in the cluster.

7 Related Centers at Other Universities

In this section we discuss other centers that focus on cyber security and privacy. We note that these centers are not focused on the combination of technical and behavioral aspects of cyber security and privacy as we are proposing.

The Georgia Tech Information Security Center (https://www.gtisc.gatech.edu/about-us.html) has members from the College of Computing, College of Engineering, College of Business, College of Liberal Arts, the Office of Information Technology and the Georgia Tech Research Institute. The projects mostly deal with secure communications hardware, prototyping, robotics & unmanned systems, threat systems, and test & evaluation. There is hardly any effort on the privacy aspects, end-user involvement, and human factors.

The Center for Education and Research in Information Assurance and Security (CERIAS) at Purdue University (http://www.cerias.purdue.edu) includes faculty from six different colleges and 20+ departments across campus. CERIAS has a huge array of projects that include Assured Identity and Privacy, Cryptology and Rights Management, End System Security, Human Centric Security, Network Security, Policy, Law and Management Prevention, Detection and Response, Security Awareness, Education, and Training. While some of these focus on behavioral aspects of security, most of these projects are led by a single PI and not really interdisciplinary.

CyLab at Carnegie Mellon University (https://www.cylab.cmu.edu/about/index.html) is one of the largest university-based cybersecurity research and education centers in the U.S. It has more than 50 faculty and 100 graduate students from more than six different departments and schools. Projects include Trustworthy Computing Platforms & Devices, Next-Generation Secure & Available Networks Mobility, Security of Cyber-Physical Systems, Secure Home Computing Survivable Distributed Systems & Outsourced Services, and Privacy Protection. However, these projects do not typically combine technical and behavioral aspects of security and privacy.

The University of Maryland's Cybersecurity Center (MC2) (http://www.cyber.umd.edu/about) is an NSA-designated Center of Academic Excellence in Information Assurance Research. With about 40 faculty involved, the research focus is primarily on wireless and network security, secure software, cyber supply chain security, privacy in social networks, cybersecurity policy, cryptography, attacker behavioral analysis, health care IT, multimedia forensics, and the

economics of cybersecurity. The scope of their work is broad and overlaps with some of the research we are proposing, but is not focused on the IoT and a combination of technical and behavioral research.

The Institute for Security, Technology, and Society (ISTS) at Dartmouth College (http://www.ists.dartmouth.edu/about/) has supported 64 faculty members. ISTS engages in interdisciplinary research, education and outreach programs that focus on information technology (IT) and its role in society, particularly the impact of IT in security and privacy. Current projects include areas of Healthcare Information Technology Security, Education Initiatives in Information Security and Privacy, and Network and Systems Security. There appears to be less emphasis on the combination of technical and behavioral issues than what we are proposing.

Virginia Tech (http://www.cyber.vt.edu/) has three "centers" related to cybersecurity. Virginia Tech offers technical undergraduate and graduate programs in cybersecurity, with faculty conducting research in information security, network security, hardware security, and software security. Research that combines technical and behavioral aspects has taken a back seat to this technical focus.

The Florida Center for Cybersecurity (FC^2, http://www.usf.edu/cybersecurity/) at the University of South Florida is intended to be a shared resource for all Florida's higher education, government, defense and business communities. The center was created in 2014 and research projects are just getting started in 2015. It has less of a technical focus than the centers described previously, and does not have a research focus that combines technical and behavioral aspects of security. Our plan is to cooperate with the FC^2 to enhance opportunities and education for all of Florida, with UCF providing technical and behavioral expertise to augment their business-focused efforts.

As can be seen from the above, many universities have centers already operating in cyber security. UCF's position as a leader in Modeling and Simulation (through the IST) will give us an edge in competing with these centers to provide cyber Modeling and Simulation capabilities (such as the ones that the DoD is seeking). Many of these centers follow the advice of the National Science Foundation and combine faculty experts from very different disciplines, as we are proposing. However, most of these centers do not emphasize behavioral aspects of cyber security and privacy as we propose.

Appendix A: Relevant Prior or Current Grant Funding

Gary Leavens:

- "TWC: Medium: Collaborative: Flexible and Practical Information Flow Assurance for Mobile Apps", NSF, $325K, 2012-2015.

Mainak Chatterjee: a proposal submitted to the Florida Center for Cybersecurity (FC^2):

- "Vulnerability and Survivability of Cyberspace: Basic Science to Applications," FL FC^2, $25K, 2014.

Sumit Jha:

- "Formal Methods for Security and Privacy in Cyber-Physical Systems", submitted to NSF, $1, 2014.
- "Provable Security for Next-Generation Nanoscale Computing Systems using High-Performance Formal Methods", submitted to FL FC^2, $9K, 2014.

Sheau-Dong Lang:

- "Forensic Science Center for Excellence Program," submitted to NIST, $3.5M, 2015.

Joseph LaViola: the following were to build systems for cryptographers:

- "Interaction and the Analyst Workstation of the Future", US Air Force Research Lab Award FA87500820202, $70,000, June 2008 – June 2009.
- "Sketching Mathematical Algorithms", US Air Force Research Lab A-SpaceX Award FA8750-08-C-0131, $53,078 of $250,000, Feb. 2008 – Feb. 2009.
- "Sketching Mathematical Algorithms", Disruptive Technology Office A-SpaceX Award N61339-06-C-0186, $75,943 of $350,000, Sept. 2006 – Dec. 2007.

Mubarak Shah:

- "Identity Assurance using Biometrics for Cybersecurity," $50K, FL FC^2, 2015.

Damla Turgut:

- "TWC: Small: Value of privacy in the mobile economy," submitted to NSF, $364K, 2015.

Changchun (Cliff) Zou:

- Modeling and Measuring Botnets," NSF Cyber Trust, $175K, 2006-2009.
- Intel Research Fund on vulnerability analysis and hardware validation, $53K, 2007-10.

Yier Jin and Changchun (Cliff) Zou:

- "Smart Grid Security Protection through Cross-Layer Approaches", FL FC^2, $33K, 2015.
- "EDU: Collaborative: Cybersecurity Bridging Courses for non-STEM Students and Professionals," submitted to the NSF, $100K, 2014

Yier Jin:

- "TWC: Small: Collaborative: Toward Trusted 3rd-Party Microprocessor Cores: A Proof Carrying Code Approach," NSF, 2013-2016.
- "SaTC: STARSS: RESULTS: Reverse Engineering Synthesis on Ubiquitous Logic for Trustworthiness and Security," submitted to NSF, $338K, 2015.

Peter Yuan: (also the MIST Center is doing research on hardware security):

- "Information Assurance for Secured Mobile Healthcare Systems," $50K, FL FC2, 2015.

David Metcalf: work with the Marines and DHS:

- Combat Hunter Profiling Part-Task Trainer Minigame Phase II Development and Evaluation Study, US JFCOM
- SIGNS Dept. of Homeland Security / Federal Law Enforcement Training Center

Waldemar Karwowski:

- Complex Systems Engineering for Rapid Computational Socio-Cultural Network Analysis, Award No.: N000141110934, 2011-2014, Human Social Cultural Behavioral Program, Office of Naval Research.

Mark Shafer and Michael Macedonia:

- "University of Central Florida Intelligence Community Center for Academic Excellence," DIA, 2014-2015.

Martin Richardson: a contract from DIA for advanced laser intelligence sensing:

- "Long-Range Laser Measurements and Signatures Intelligence," DIA, $150,000, 2009-2011.

Corey Bohil: (has also published research on cognitive games and user response patterns)

- "Active authentication using covert cognitive interrogation games." DARPA Active Authentication Program. 2012-2014

Shawn Burke:

- "Leadership-followership: Moving beyond traditional leadership to build highly functioning autonomous teams." NASA $100K, 2014-2015.
- "Shared Leadership: Moving Beyond Virtuality and Distribution to Build Capacity in Virtual Organizations". NSF $150K, 2010-2013.
- "Understanding, measuring, and modeling the effects of culture in negotiation and collaboration: A dynamic, multi-level view of culture. ARO MURI, $1.88M, 2008-14.
- "Investigating Methods for Improving Performance in Military Multiteam Systems (Leveraging Social Identity as a Way to Reduce Goal Conflict and Improve Coordination Within Military Multiteam Systems," Army Research Institute, $115K 2010-2011,
- "Promoting the understanding of team-level cognition within the warfighter: The application of metrics in simulation". With F. Jentsch. ONR, $215K 2007-2010.
- "Examining Leadership Processes in Complex Network Environments". Army Research Institute, $315K, 2008-2010**.**

Peter Hancock and Randall Shumaker:

- "RCTA FY2014 Task H1-3: Investigate the Role of Trust and System Transparency in SMM Development during Tactical HRI," General Dynamics, 2014-2015.

Florian Jentsch and Randall Shumaker:

- "RCTA FY2014 Task H1: Shared Mental Models for Soldier (SR) Teaming," General Dynamics, 2014-2015.

Dana Joseph: (work on deviant behavior in the workplace related to misuse of data):

- "Measuring Workplace Discrimination: Is Breadth Better than Depth?" National Inst. for Occupational Safety and Health, $13K, 2013-2014.
- "Blinded by the Light: The Dark Side of Traditionally Desirable Personality Traits," *Industrial and Organizational Psychology*, 2014.

Mark Johnson: related to digital forensics:

- Measuring the Frequency Occurrence of Handwriting and Hand-Printing Characteristics, National Institute of Justice, $500,132. 2010-present.

James A. Beckman: Author of a book and several articles on National Security, including *Comparative Legal Approaches to Homeland Security* (Ashgate, 2008).

Timothy Ravich: National expert on Aviation Law and one of only 37 board certified aviation lawyers in the State of Florida. Dr. Ravich is the author of several major books on the topic, including *Aviation Law After September 11th* (Vandeplas 2010), *Fundamentals of Florida Air*

and Space Law (forthcoming, 2015), and *Drone Law* (American Bar Association, forthcoming 2015).
Carol Bast: Author of multiple books on law and an expert on privacy, wiretapping, eavesdropping, and the Foreign Intelligence Surveillance Act. Dr. Bast's research on the topics of privacy, wiretapping and FISA have appeared in such forums as *The Lawyer's Guide to Ethics and Technology*, *The Oxford Companion to American Law*, *Criminal Law Bulletin*, *New York Law School Law Review, St. Mary's Law Review, Midwest Law Review*, and many others.
Amit Joshi: authored several articles on value/return on investments.
Marshall Schminke: authored several articles on workplace privacy issues including "The Impact of Individual Ethics on Reactions to Potentially Invasive HR Practices," *Jour. Bus. Ethics*, 2007, and "Employee Reactions to Internet Monitoring," *Jour. Bus. Ethics*, 2008.
Joseph Brennan: authored articles about coding in smart cards and medical devices including: "Low Complexity Multiplication in a Finite Field Using Ring Representation." *IEEE Trans. Comput.*, 2003; "Montgomery multiplication over rings," *Journal of the Franklin Institute*, 2009.
Nancy Stanlick: authored two books and several articles on ethics including: *Asking Good Questions: Case Studies in Ethics and Critical Thinking* (Indianapolis: Hackett, 2015); *American Philosophy: The Basics* (Routledge, 2012); "Reconciling with Harm: An Alternative to Forgiveness and Revenge," *Florida Philosophical Review*, 2010; "Individual-Centered Collaborative Research," *Teaching Philosophy*, 2007; grant: Core Commitments: Educating Students for Personal and Social Responsibility, AAC&U 2007-2009, $25000.

Appendix B: Citations for Cyber Security as a National Priority

The nominee for secretary of defense, Dr. Ashton Carter, considers cyber security a priority area (*bank info Security*, December 3, 2014): http://www.bankinfosecurity.com/cybersecurity-seen-as-dod-priority-under-carter-a-7634/op-1 .
Cyber security is the number 1 concern of federal chief information officers (CIOs), as described in the *2014 TechAmerica Federal CIO and CISO Survey*: http://www.techamerica.org/Docs/TechAmerica_2014_CIO_Survey%20June%202014.pdf .
Cyber security is an "all encompassing priority" for the intelligence community (*Federal News Radio*, January 22, 2015): http://www.federalnewsradio.com/502/3785456/DoD-intel-chief-Vickers-gives-cyber-premier-priority-status .
The shortages in jobs in cyber were reported at the 2014 RSA conference.
New DoD Cyber Strategy is found at: http://www.defense.gov/home/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf .

Appendix C: Responses to Panel Comments on the Pre-Proposal and at the Q&A

- "The critical mass of faculty seems way too big to manage." Note that there are only 12 core faculty, which would become 17 after hiring. The great interest from associated faculty is an asset, not a liability. We have clarified the role of associated faculty in providing context, for problem definition and solutions. Note that UCF currently has only 2 faculty that spend most of their research time on cyber security.
- "The faculty recruitment plan is ambitious and should be better justified…" We have scaled back our faculty hiring request to 5 faculty, and given detailed hiring and recruitment plans.
- "Articulate how UCF would move needle." This is addressed in detail above.
- "[Explain] why they are unique and not too late." We expanded on this, see especially section 7.

Appendix D: Support email from Jeff Snyder of Raytheon

Dr. A. Dale Whittaker
University of Central Florida
Provost and Vice President for Academic Affairs

Subject: Cyber Security and Privacy Cluster Proposal

Dear Dr. Whittaker;

As a Cyber Industry professional, I appreciate the great success that Dr. Michael Georgiopoulos and his team have displayed in the Cyber Domain, most recently with their second National Collegiate Cyber Championship, competing against about 200 other prominent Universities and 2400 acclaimed students. I expressly enjoy working with Michael and his team as a member of his Advisory Board and have been impressed with his thought leadership and commitment to the important Cyber Domain.

As we all know, this area is so important to our national security and economic stability when you consider the huge intellectual property theft our nation has experienced, cyber crime and financial theft, personal identity theft and cyber nuisance activities. The growth in this cyber threat environment has caused a significant shortage of qualified human capital estimated to be 400,000 in the United States today, 1,000,000 globally, and continuing to grow at a very rapid rate. Well thought out and executed Cyber programs aligned with Engineering and Computer Science are critical to firms like Raytheon, and industry in general, to help close this human capital gap to better protect our nation and its critical infrastructures.

I reviewed and commented on the Cyber Security and Privacy Cluster proposal and have significant belief in its foundation, objectives, and the benefit it will generate for UCF and the State of Florida. I am pleased with the proactive approach UCF is taking to expand its Cyber programs and student throughput capability in anticipation of the significant growth in the applicant pool you will experience, particularly in light of your back-to-back National Collegiate Cyber Challenge wins and industry's perception that UCF is a leading Cyber University.

In great respect for a great University.

Jeff Snyder
Vice President, Cyber Programs
Raytheon Company (UCF '85)