PERSONAL STATEMENT
Shuyuan Mary Ho

The use of computer-mediated communication (CMC) technologies, while providing substantial social convenience, has also significantly increased our exposure to online deception, identity theft, fraud, and theft of intellectual property, along with corporate espionage. These problems have fostered my research interest in **computer-mediated deception in trusted human-computer interactions**. I am a sociotechnical, psycholinguistic, behavioral scientist, and my research draws upon theories of social, psychological, and organizational sciences; adopting a statistical and computational machine learning approach while contributing to progress in social-computational scholarship and discovery. My teaching focuses on information systems security, to equip students with concepts, knowledge, and skillsets to defend networks and systems technically, as well as operationally and managerially against potential cyber threats. As such, I am an assistant professor of record for information systems and more specifically information systems security. My efforts contribute to cybersecurity and privacy in academic and practitioner communities. In this statement, I introduce my academic accomplishments and advancement in three categories: research and scholarship, teaching excellence, and service contribution.

1. Research and Scholarship

I have established the iSensor Research Lab since 2010. The goal of the lab is to study and provide analysis on very specific interactive information behavior that cannot be studied in the real world. My research examines human factors as they relate to cyber threats and trust violation in the context of human computer interaction (HCI). I adopt mixed methods and unique experimentation to examine these phenomena. This research can be complex, as it involves a focus on sociotechnical systems and landscapes. The data collected comes from cognitive (subjective) inferences of human sensors, along with the interpretation of (objective) language-action cues as a way to represent traceable artifacts of information behavior. All my publications, inventions, and creative artifacts are highly focused, having been built on this unique research theme.

Research Theme and Contributions

The underlying theme of my research lies in human computation analysis of information artifacts based on simulations of computer-mediated threat and deception-incurring scenarios. The iSensor Laboratory produces online game experiments to study human high-risk factors that often endanger the establishment of trust in society. This line of research has appeared in quite a few high impact[1] refereed articles. Since 2012, I have written and published ten (10) refereed journal articles[2], and more than twelve (12) articles in refereed conference proceedings.

Theme 1: Computer-mediated deception in group communication

Theorizing is a process that requires careful construct development, and logical hypothetical assumptions with rigorous justification. Theory development is considered the most challenging literature to compose as compared to empirical studies. The first theme of my research is to build a sociotechnical detection system framework, based on trust and attribution theories, to counter organizational insider threat problems. I boldly posit that a social actor's deceptive intent, while at times invisible and hard to trace, can be detected by human sensor networks within group communication. A manuscript that discusses the dyadic attribution mechanism to codify the attribution and identification of deceptive insiders based on human sensors network's subjective (cognitive) attributions was published by the ***Journal of the Association for Information Science and Technology*** (Ho & Benbasat, 2014). A second manuscript describing the use of finite-state machines to dissect insider threats in cloud

[1] An impact factor of ≥ 0.8 for refereed journals in the fields of information science is considered high impact. The impact factor for each of my journal articles is included in my curriculum vitae.
[2] Complete references for self-cited works in this statement are found in the candidate's C.V.

communications was published by the ***Journal of Wireless Mobile Networks, Ubiquitous Computing and Dependable Application*** for a special issue titled *Frontiers in Insider Threats and Data Leakage Prevention* (Ho & Lee, 2012). A third manuscript that adopts agent-based modeling to virtualize trustworthiness, was published in ***International Journal of Mobile Network Design and Innovation*** for a special issue titled *Detecting and Mitigating Information Security Threats for Mobile Networks* (Ho & Katukoori, 2013). One book based on this theme was published by *Lambert Academic Publishing* (Ho, 2014). A fourth manuscript that describes the design principles and development strategies of this sociotechnical system and how it was empirically tested was published by ***Information Systems Frontier*** (Ho & Wartentin, 2017). A fifth manuscript that describes the empirical test of the efficacy of human sensors network's objective attribution manifested in detecting the "***ethical dilemma***" of a deceptive social actor from group communication, was recently accepted for publication in the ***Journal of the Association for Information Science and Technology*** (Ho, Hancock***, et al.***, in press). I am currently establishing a sociotechnical research program based on my theory of trustworthiness attribution, and this inquiry has been accepted for publication at the ***Journal of the Association for Information Science and Technology*** (Ho, Kaarst-Brown***, et al.***, in press).

This line of research has also been published in the ***Proceedings of the 49th Hawaii International Conference on Systems Sciences*** (HICSS-49) (Ho, Hancock, Booth, Burmester***, et al.***, 2016), the 2015 ***ACM SIGMIS Computers and People Research*** (CPR) (Ho, Fu***, et al.***, 2015), the ***Encyclopedia of Information Science and Technology*** (Ho & Hollister, 2015), and the ***Social Computing, Behavioral Modeling and Prediction*** (SBP) (Ho ***et al.***, 2014).

Sociotechnical systems refer to the interaction between society's complex infrastructures and human behavior. As building rigor into the capture of data is critical in producing high impact research, the sociotechnical research system[3] I have developed can function as a data collection instrument to capture rich information about interactions in specific contexts (Ho & Wartentin, 2017). These real-world interactive scenarios are developed in the form of online games to stimulate and motivate certain behavior, and thus generate meaningful interactive data in realistic settings. This sociotechnical research system resulted in one ***NSF Secure and Trustworthy Cyberspace*** (***SaTC***) ***EAGER*** grant (#1347113, #1347120, $199,998, 09/01/13—08/31/15). As a result of a collaboration with Professor Jeffrey Hancock (Stanford), Professor Mike Burmester (FSU), and Professor Xiuwen Liu (FSU), the EAGER grant led to the subsequent ***NSF Innovation Corps*** (***I-Corps***) grant (#1505195, $50,000, 12/15/14—12/30/16). While this sociotechnical system research idea may be a bit ahead of its time, this research will eventually lead to more grants and proposal submissions (discussed further in Grants section).

Computational modeling, enabled by the design of the sociotechnical systems, can provide accuracy and precision through repeated experiments and simulations of behavior. Causal models can be constructed using mixed modeling and machine learning approaches. The intellectual property of my invention based on research theme 1 has been filed with the FSU Office of Commercialization. This patent[4] (pending) describes a reasoning computational system for discovering humans' deceptive intent and motivation based on interactive communicators' language-action cues in online communication. In fact, this innovation has many applications that address the need to protect information against insider threats for government agencies, military organizations, and large corporate enterprises. This innovation also has another potential application; allowing for online polygraph testing in spontaneous, online communication. This invention resulted in an award from the ***NSF I-Corps*** Program. I am actively seeking investors who share similar visions to turn this research into a commercialized product.

Theme 2: Computer-mediated deception in interpersonal communication

A fundamental research question exploring the possibility of detecting online deception in interpersonal communication is based on theme 1. One significant discovery was that computer-mediated deception can be more accurately detected by machine learning algorithms when processing human

[3] http://isensoranalytics.com/
[4] FSU 15-167 Ho.

sensors' objective communication rather than subjective identification with human eyes. The strategies revealed in computer-mediated deception and computational modeling using the machine learning approach were highlighted in the ***Journal of Management Information Systems*** (JMIS) (Ho, Hancock, Booth, & Liu, 2016), ***Social Computing, Behavioral-Cultural Modeling & Prediction and Behavior Representation in Modeling and Simulation*** (SBP-BRiMS) (Ho, Liu***, et al.***, 2016). Based on these findings I have developed several innovative ideas and a research plan to model, design and develop an online polygraph system—codifying online deception in spontaneous, virtual communication.

The results of this research theme have been published in the ***Proceedings of the 49th Hawaii International Conference on Systems Sciences*** (HICSS-49) (Ho, Hancock, Booth, Liu***, et al.***, 2016), and the ***Proceedings of the 2015 IEEE International Conference on Intelligence and Security Informatics*** (Ho, Hancock***, et al.***, 2015). A discussion of context using language-action cues to codify spontaneous computer-mediated deception ha been submitted to the ***Computers in Human Behavior*** journal (Ho & Hancock, Submitted).

Interpersonal deception is not only codify-able by language-action cues, but can also be factored using communicators' cognitive perceptions. A gender deception experiment was designed and conducted to examine gender deception online through perceptions of given statements. The cognitive factors that influence the interactivity of deception and detection of deception were explored using structural equation modeling (SEM) and published in ***Information Processing and Management*** (IP&M) (Ho, Lowry***, et al.***, 2017). An early finding of this study was also published in the ***Proceedings of the 76th Annual Meeting of Association for Information Science and Technology*** (ASIS&T) (Ho & Hollister, 2013).

Theme 3: Human Factors

The third theme of my research focuses on human factors (or, high-risk human factors *per se*) that affect either cloud security or organizational security. As cloud computing has become a popular information curation solution for organizations, more corporate proprietary information is stored in the cloud, and thus concerns about cloud information security increases. My first illustration of human factors research focuses on the investigation in the causal effect of perceived risk and subjective norms on users' trust intention to adopt cloud technology. This manuscript is currently under review by ***Computers and Security*** (Ho ***et al.***, Submitted). A partial least squares structural equation modeling (PLS-SEM) analysis was adopted to assess latent variables and examine moderating effects on cloud technology adoption. This early work was published in the ***Proceedings of the 2015 Americas Conference on Information Systems*** (AMCIS'15) (Ho & Ocasio Velázquez, 2015).

The second illustration of this human factors research is a usability study of a digital library, the IntegraL project, exploring the idea of how enhanced access to information through virtual integration of digital library sources can help users make better sense of information. This study was published by the ***Journal of the Association for Information Science and Technology*** (Ho ***et al.***, 2013). With my collaborators from New Jersey Institute of Technology, I envision to use IntegraL as the base of the SpiderSense project that studies cognitive factors that influence and enhance the general public's security awareness and self-efficacy through this service infrastructure (i.e., a federated digital library).

A third illustration adopts a unique theoretical lens through which to explore the expansive learning opportunities in a cyber defense team when viewed as an activity system. Through this lens, I am interested in studying the transformation of an organizational information security culture. An early report of this framework has been published and presented at 2017 ***Twelfth Annual Symposium on Information Assurance*** (ASIA) (Ho, von Eberstein***, et al.***, 2017).

The fourth illustration of my human factors research identifies clinical high-risk (CHR) symptoms of psychosis (e.g., schizophrenia, depression, or anxiety). These types of mental disorders can lead to destruction and harm in society (e.g., mass murder). I am interested in the early identification and predictive analysis of CHR symptoms appearing in social media (e.g., Facebook).

Grants

During most recent five years, I submitted a total of thirty-two (32) grant proposals as the principal investigator, requesting more than $15 million in funding. Of these, twenty-five (25) were submitted to federal government agencies including the National Science Foundation (NSF), the National Security Agency (NSA), the Department of Homeland Security (DHS), the National Institutes of Health (NIH), the Intelligence Advanced Research Project Activity (IARPA), the Department of Defense (DOD), and the Airforce Sponsored Research (AFOSR). Two (2) were submitted to Israel funding agencies, two (2) submitted to the Florida Center for Cybersecurity, and four (4) submitted to FSU. Seven (7) of those proposals were awarded, for a total of **$413,859**. It is also worth mentioning my future research proposals:

a) One proposal idea is to extend my current research on computer-mediated deception, and integrate online users' textual and voice-to-text data to examine fake and deceptive communication intent in social media context. One specific goal is to design an online polygraph system; a lie detector for social media, which takes a communicator's language input to dynamically process, extract and identify deception on the fly (in near real-time).

b) One selectable proposal (depending on available funding) reviewed by DHS PARIDINE Program (2017), is to tackle a grand challenge of attributing root causes of malicious network/ Internet disruptive events (NIDEs) from various networks. The research team will study event correlation mechanisms and develop a causal learning engine to make sense of the near real-time Internet traffic.

I envision that the research detailed above will contribute significantly to the sociotechnical cybersecurity research community, and support predictive measures for human high-risk factors in clinical psychometrics. In the next five years, I will continue sociotechnical psycholinguistic behavioral research (illustrated in themes 1 and 2), the human factors research (illustrated in theme 3), and will submit additional proposals to the NSF Secure and Trustworthy Cyberspace Program, the Department of Defense, and the National Security Agency (NSA), as well as several more refereed research articles.

2. Teaching Excellence

I enjoy teaching technical subjects related to information systems and cybersecurity. My teaching has been influenced by the fact that I have been a cybersecurity professional in both academic and industry contexts, and my professional experience affects my students' career choices. This work is complex and very technical. My students experience significant challenges in the very rigorous coursework, but if they persist they find highly compensated jobs upon completion of their undergraduate or graduate degrees.

Teaching Philosophy

Providing education on ever-changing technology is always challenging, but especially so with leading-edge cybersecurity concepts and technologies. My teaching philosophy can be best characterized by the idea that theory and practice must be integrated and interesting. I use lectures and hands-on labs in conjunction with small-group mentoring, as well as periodic quizzes leading up to each significant test.

Innovative Pedagogical Approach

Cybersecurity is a critical subject that has been characterized recently by interest on the part of the federal government. In order to engage students in this challenging content, I continue to develop curricula, lab activities, and extracurricular activities for students who want to develop advanced technical hands-on experience. Hands-on labs are designed and incorporated into weekly cyber defense learning activities that utilize the virtual lab[5] resources. Students in the undergraduate program can learn basic information security systems concepts in the introduction class and then continue on to install and configure firewalls, intrusion detection systems, honeypots, and penetration testing in the dynamic settings of the advanced class. In the distance-learning course setting, students are not only given live hands-on security exercises for the installation and configuration of security tools on a weekly basis, but they also work in virtual teams to analyze network traffic, and make sense of big datasets generated by the simulated lab computing

[5] https://labs.cci.fsu.edu

environment. This innovative platform affords the ability to perform exercises on networking connectivity, penetration testing, activity monitoring, and cyber defense.

Aside from security-related content, I developed and taught a required course on Information Systems Management. This course incorporates team-based virtual lab exercises for students from library and communication disciplines who typically have less technical knowledge and experience. This class is highly interactive and experiential. Students are assigned to virtual teams and explore the practical application of using information technology in support of business decisions and operations while evaluating and learning from each other's experiences. Students in this class are said to enjoy and benefit from the virtual lab experience and ensuing discussions.

These courses cover a wide breadth and depth of domain knowledge across multiple disciplines including information systems, information science, organizational science, management science, and social science. Course content is carefully crafted to be readily absorbed based on students' personal interests and existing knowledge. Diverse classroom activities illustrate theoretical concepts through the study of current events in the industry. Students' learning performance is reinforced with quizzes, homework assignments, team projects, and oral presentations. These courses have been kept up-to-date and aligned with practitioners' best practices in information systems, technology, and cybersecurity.

In my view, a professor not only can educate and enlighten students with theories, knowledge, skills, and experience but can infuse the next generation with professional integrity and ethical standards. These courses also prepare students with a strong ethical code of conduct as information professionals.

Student Performance

Teaching students "troubleshooting" and critical thinking ability to defend networks from intrusions and incidents in an iSchool is pioneering. It is worth noting that these information security courses are not designed to teach students merely how to "use" information systems, but how to "troubleshoot" system problems. Students' expectations for learning tend to settle at "use" level activity, rather than "troubleshooting." This makes for a great challenge. These classes include complex technology and systems configurations requirements in the lab environment of a large classroom setting.

To give a few examples, students enrolled in my current Information Security courses often experience uneasiness in the first few weeks. However, post-class feedback consistently indicates that they learn a great deal from hands-on exercises while building out information systems via team collaboration, and enjoy the structured class assignments and video case discussions. Enrollment in these classes continues to increase despite the rigor and the ever-evolving technical challenges that have been designed into these courses. Generally, students with a significant interest in information security prefer a rigorous teaching style, while students without technical background tend to find my classes quite difficult. And yet, my course evaluations are on a trajectory of consistent improvement, with over 75% of students in the last 2 years rating my courses as being above satisfactory.

My students easily find meaningful jobs—with high compensation upon graduation—becoming security analysts at NASA, Deloitte, Harris Corporation, State Farm, Lockheed Martin, managed security services integrators at ReliaQuest, and penetration testers at A-Lign. This should be considered an important indicator of my instructional design and teaching capability. Students with a focus and significant interest in cybersecurity can receive a high-end pay scale position even when freshly graduated from the College undergraduate or master's programs.

Cybersecurity Club – An experiential blend of Theory and Practice

To help students gain more hands-on experience in information security, I identified the need for students to form their own interest group in cyber defense and penetration activities, and thus I founded the FSU Cybersecurity Club student organization in 2013. As faculty advisor, I work with students on technical and management skills in a variety of settings; participation in the regional Southeast Collegiate Cyber Defense Competition (SECCDC) as well as sponsored Capture-the-Flag (CTF) competitions (e.g., Cyber Security Awareness Week (CSAW), CyberSEED, and Boston Key Party, etc.). I find this to be rewarding, as students' genuine interest and work in defending cyberinfrastructure are stimulated and encouraged.

3. Service Contribution
Service provides an important opportunity to promote research and education, and thus contribute to the growth of the school, the university, and the professional community.

Service to the School
I am currently a faculty advisor to fifteen (15) graduate students (2017), serve as a chair, and a committee member for doctoral committees. I have participated in reviewing curriculum design and development for both undergraduate and graduate courses. I served as a member of the Technology Services Committee (2013-14), the Personnel Committees for faculty and chair searches (2012-2018), and on the Research and Scholarship Committee since 2014.

Service to the University
As a faculty advisor for the Cybersecurity Club[6] student organization, I have the opportunity to provide oversight and guidance to students across campus. It is my strong belief that the University would benefit from an interdisciplinary Center for Cybersecurity[7]. I have been working with senior faculty members Chuck McClure and Mike Burmester, and others to create the FSU Cybersecurity Center for Research, Education, Policy, and Assessment. I am providing administrative and technical support for the establishment of this Center, which will advance the University's capacity for cybersecurity research and education, while drawing funding from federal agencies as well as state government.

Service to the Profession
As a cybersecurity professional in both the academic and practitioner community, I have been an active member of several academic communities; AIS, AOM, ACM, ASIS&T, and IEEE. I have been a long-standing member of several professional associations; (ISC)2 and Information Systems Audit and Control Association (ISACA). I served as Research Coordinator for the ISACA Tallahassee Chapter during 2012—2015, and trainer for ISACA Cybersecurity Nexus (CSX) Certificate Training (2016—2017).

I have been nominated as Best Associate Editor (AE) for the ICIS 2016 Security and Privacy Track, and served as an AE for the PACIS 2016 Security and Privacy Track. I served as Publicity Chair for the AMCIS 2016 conference. I have served regularly as a Program Committee (PC) member and a reviewer for several refereed journals (e.g., ***JASIST***, ***JMIS***, ***Computers and Human Behavior***) and conference venues (e.g., iConferece, HICSS, Social Computing Workshop, and ACM Group Workshop) during 2012-2017. I co-organized a sociotechnical systems workshop at iConference 2013, co-organized a workshop on interdisciplinary practice among iSchools at the iConference 2014 in Berlin, and co-organized a Big Data Analytics for Behavioral Modeling Tutorial Workshop at the 2015 SBP conference in Washington DC. I believe these efforts promote the academic standing within the iSchools, information systems, social computing community, as well as the cybersecurity academic community.

Future Directions
I intend to continue my iSensor research while pursuing funding support from the federal and state governments, as well as the University and private business entities. Overall, I feel that my research, instructional teaching, and service to the community—as well as to the University—has been important in promoting the academic image and growth of the College. I continue to appreciate the ongoing support of my colleagues, the School, the College, and the University that affords me a platform to create and advance my intellectual discovery, providing significant contributions to the sociotechnical cybersecurity research and professional community.

[6] https://cybersecurity.fsu.edu/club/
[7] https://cybersecurity.fsu.edu

References

Ho, S. M. (2014). ***Cyber insider threat: Trustworthiness in virtual organizations***: LAP Lambert Academic Publishing, pp.1-436, 978-3-659-51702-0.

Ho, S. M., & Benbasat, I. (2014). Dyadic attribution model: A mechanism to assess trustworthiness in virtual organization. ***Journal of the American Society of Information Science and Technology, 65***(8), 1555-1576.

Ho, S. M., Bieber, M., Song, M., & Zhang, X. (2013). Seeking beyond with IntegraL – A user study of sense-making enabled by anchor-based virtual Integration of library systems. ***Journal of the American Society for Information Science and Technology, 64***(9), 1927-1945.

Ho, S. M., Fu, H., Timmarajus, S. S., Booth, C., Baeg, J. H., & Liu, M. (2015). Insider threat: Language-action cues in group dynamics. ***Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research***, New York, NY, 101-104, ACM.

Ho, S. M., & Hancock, J. (Submitted). Context in a bottle: Language-action cues in spontaneous computer-mediated deception. ***Computers in Human Behavior (submitted)***, 1-22.

Ho, S. M., Hancock, J. T., & Booth, C. (in press). Ethical dilemmas: Deception dynamics in computer-mediated group communication. ***Journal of the Association for Information Science and Technology***, 1-14.

Ho, S. M., Hancock, J. T., Booth, C., Burmester, M., Liu, X., & Timmarajus, S. S. (2016). Demystifying insider threat: Language-action cues in group dynamics. ***Proceedings of the 2016 Hawaii International Conference on System Sciences***, 2729-2738, IEEE.

Ho, S. M., Hancock, J. T., Booth, C., & Liu, X. (2016). Computer-mediated deception: Strategies revealed by language-action cues in spontaneous communication. ***Journal of Management Information Systems, 33***(2), 393-420.

Ho, S. M., Hancock, J. T., Booth, C., Liu, X., Liu, M., Timmarajus, S. S., & Burmester, M. (2016). Real or Spiel? A decision tree approach for automated detection of deceptive language-action cues. ***Proceedings of the 2016 Hawaii International Conference on System Sciences***, 3706-3715, IEEE.

Ho, S. M., Hancock, J. T., Booth, C., Liu, X., Timmarajus, S. S., & Burmester, M. (2015). Liar, Liar, IM on Fire: Deceptive language-action cues in spontaneous online communication. 157-159, IEEE.

Ho, S. M., & Hollister, J. (2013). Guess who? An empirical study of gender deception and detection in computer-mediated communication. 1-4, ASIS&T.

Ho, S. M., & Hollister, J. (2015). Cyber insider threat in virtual organizations. In Khosrow-Pour, M. (Ed.), ***Encyclopedia of Information Science and Technology, Third Edition*** (Third ed., pp. 741-749). USA: Information Science Reference (an imprint of IGI Global).

Ho, S. M., Kaarst-Brown, M., & Benbasat, I. (in press). ***Trustworthiness attribution: Inquiries into insider threat detection***. Journal of the Association for Information Science and Technology.

Ho, S. M., & Katukoori, R. R. (2013). Agent-based modeling to visualize trustworthiness: A socio-technical framework. ***International Journal of Mobile Network Design and Innovation, Special Issue of Detecting and Mitigating Information Security Threats for Mobile Networks, 5***(1), 17-27.

Ho, S. M., & Lee, H. (2012). A thief among us: The use of finite-state machines to dissect insider threat in cloud communications. ***Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, Special Issue of Frontier in Insider Threats and Data Leakage Prevention, 3***(1/2), 82-98.

Ho, S. M., Liu, X., Booth, C., & Hariharan, A. (2016). Saint or Sinner? Language-action cues for modeling deception using support vector machines. In Kevin Xu, D. Reitter, D. Lee, & N. Osgood (Eds.),325-334, Springer International Publishing Switzerland.

Ho, S. M., Lowry, P. B., Warkentin, M., Yang, Y., & Hollister, J. (2017). Gender deception in asynchronous online communication: A path analysis. ***Information Processing & Management, 53***(1), 21-41.

Ho, S. M., & Ocasio Velázquez, M. (2015). Do you trust the cloud? Modeling cloud technology adoption in organizations. AIS.

Ho, S. M., Ocasio Velázquez, M., & Booth, C. (Submitted). Trust or consequences? Causal effects of perceived risks and subjective norms on cloud technology adoption. ***Computers & Security***.

Ho, S. M., Timmarajus, S. S., Burmester, M., & Liu, X. (2014). Dyadic attribution: A theoretical model for computationally interpreting words and action. In Kennedy, W. G., N. Agarwal, & S. J. Y. (Eds.) (Eds.),1-8, Springer.

Ho, S. M., von Eberstein, A., & Chatmon, C. (2017). Expansive learning in cyber defense: Transformation of organizational information security culture. In Goel, S. (Ed.),1-6, IEEE.

Ho, S. M., & Wartentin, M. (2017). Leader's dilemma game: An experimental design for cyber insider threat research. ***Information Systems Frontiers, 19***(2), 377-396.