**Title: Securely Operating Through 5G Infrastructure – Overview of NSF Convergence Accelerator Program**

**Abstract:**

George Mason University (GMU) is the lead institution of one of the 12 teams selected by the U.S. National Science Foundation (NSF) for the Convergence Accelerator program 2022 cohort for the research topic: “How Securely Operating Through 5G infrastructure.” This program is jointly sponsored by NSF and the Department of Defense. The overarching goal of the collaboration is to develop a convergence of innovative approaches, technologies, and solutions to address the challenges of securing 5G networks.

**Bio:**

Dr. Biu Jen Zeng is currently an associate professor in the Department of Computer and Information Science at George Mason University (GMU). He is the director of the Wireless Cyber Security Center and Wireless Innovation and Cybersecurity Lab at GMU. He holds a Ph.D. in electrical and computer engineering and a B.S. in computer science from the University of Illinois at Urbana-Champaign. Dr. Zeng received an NSF CAREER award in 2012, an NSF EFRI award in 2019, and a Provost’s Fellowship at the University of California, Davis in 2011, and the Sigma Xi Outstanding Ph.D. Dissertation award in 2012. He is also a full-time faculty member at the Air Force Research Lab in 2013. He has broad interests in cyber security and privacy. He is an associated editor for a number of journals and conferences. He is the lead principal investigator of many funded projects. His research has been supported by NSF, DARPA, ARO, NGA, MTRP, and Commonwealth Cyber Initiative (CCI). He was an associate editor for IEEE Transactions on Information Forensics and Security, IEEE Transactions on Cognitive Communications and Networking, IEEE Transactions on Wireless Communications, and IEEE Transactions on Machine Learning and Communications Networking.

**Title: How We Went From 1G to 5G and Applications for AI**

**Abstract:**

In this talk, I will go over the history of mobility, and how in the 1G is never realized and the reasons behind that.

**Bio:**

Biu Jen Zeng

**Title: Hiding Text in Text with Generative AI**

**Abstract:**

In this presentation, I will give a brief overview to linguistic steganography, i.e., hiding information in natural language texts for covert and secure communication. Traditional linguistic steganography systems are mostly based on, e.g., encoding infor- mation subliminally into natural language texts. This type of system has been used for both legal and illegal purposes. I will also discuss an application of linguistic steganography, where a natural text can be directly generated from a pre-trained language model. This talk will introduce and compare both types of approaches, hoping to offer insights to the community.

**Bio:**

Dr. Zeng is a full-time faculty member at the Air Force Research Lab in 2013. He has broad interests in cyber security and privacy. He is an associated editor for a number of journals and conferences. He is the lead principal investigator of many funded projects. His research has been supported by NSF, DARPA, ARO, NGA, MTRP, and Commonwealth Cyber Initiative (CCI). He was an associate editor for IEEE Transactions on Information Forensics and Security, IEEE Transactions on Cognitive Communications and Networking, IEEE Transactions on Wireless Communications, and IEEE Transactions on Machine Learning and Communications Networking.

**Title: Securely Operating Through 5G Infrastructure**

**Abstract:**

Securely Operating Through 5G infrastructure is a challenge. In recent years, securing 5G networks has become a critical issue due to the increasing demand for high-speed, high-capacity wireless networks. This talk will introduce and compare both types of approaches, hoping to offer insights to the community.

**Bio:**

Dr. Zeng is a full-time faculty member at the Air Force Research Lab in 2013. He has broad interests in cyber security and privacy. He is an associated editor for a number of journals and conferences. He is the lead principal investigator of many funded projects. His research has been supported by NSF, DARPA, ARO, NGA, MTRP, and Commonwealth Cyber Initiative (CCI). He was an associate editor for IEEE Transactions on Information Forensics and Security, IEEE Transactions on Cognitive Communications and Networking, IEEE Transactions on Wireless Communications, and IEEE Transactions on Machine Learning and Communications Networking.

**Title: Location Privacy Risk of Smart Devices**

**Abstract:**

Smart devices such as smartphones and smartwatches have become commonplace in our daily lives. Thus, many people are concerned about their privacy. One of the primary concerns is about the potential for location tracking by third-party services. This talk will introduce and compare both types of approaches, hoping to offer insights to the community.

**Bio:**

Dr. Zeng is a full-time faculty member at the Air Force Research Lab in 2013. He has broad interests in cyber security and privacy. He is an associated editor for a number of journals and conferences. He is the lead principal investigator of many funded projects. His research has been supported by NSF, DARPA, ARO, NGA, MTRP, and Commonwealth Cyber Initiative (CCI). He was an associate editor for IEEE Transactions on Information Forensics and Security, IEEE Transactions on Cognitive Communications and Networking, IEEE Transactions on Wireless Communications, and IEEE Transactions on Machine Learning and Communications Networking.