Title: Securely Operating Through 5G Infrastructure – Overview

Abstract: George Mason University (GMU) the local institution of one of the 12 states selected by the U.S. National Science Foundation (NSF) for the Convergence Accelerator program 2022 cohort for the research topic – Track G: Securely Operating Through 5G Infrastructure. It is at accelerating 5G solutions to assist the U.S. government and critical infrastructure operators to communicate security anywhere and anytime. Partnering with AT&T and Michigan State University, the GMU team is developing a product, "WireText" that can expand the end user’s capability of securely commu-
nicating over non-cooperative 5G networks by building a covert and end-to-end se-
cure channel over indigenous 5G messaging and secure traffic. The multi-disciplinary team is comprised of researchers, inventors, and engineers with diverse backgrounds and expertise in cybersecurity, wireless communication, artificial intelligence (AI), nat-
ural language processing (NLP), and steganography. The team is also working with the University of the District of Columbia (UDC) to continue the product development and

traversal for underrepresented groups. More information for printfiddle: please see https://isocloud/udc.

Bio: Dr. Kai Zeng is currently an associate professor in the De-
partment of Electrical and Computer Engineering at George Ma-
son University. He received his B.S. and M.S. in Electronics Engi-
neering from Harbin Institute of Technology, China, and Ph.D. in com-
puter science from the University of California, Berkeley in 2003. He has been an assistant professor, associate professor, and professor at the University of California, Davis and Stevens Institute of Technology. He joined the AT&T Bell System in 1997 where he has been working on the development of network-centric applications for the Circuit Switched Network Infrastructure. He holds a bachelor’s degree and a master’s degree in computer science from the University of Science and Technology of China.

Title: How We Went From 5G to 5G Applications for AI (WindText)

Bio: Irvn Gerseng AT&T Fellow and Distinguished Inventive Scientist for AT&T Labs in Middlesex, NJ. He is responsible for Advanced Research for the Department of Defense (DoD), AT&T’s 5G mobility projects, emerging broadband infrastructure such as Project AirGig, Advanced RF Research technologies on Department of Defense programs, and heads up the AT&T Science and Technology Center. He holds a bachelor’s degree and a master’s degree in computer engineering from the University of California, Berkeley. After graduating from AT&T’s Wireless unit, he was responsible for the development of numerous advanced wireless technologies. Gerseng is also the lead inventor and co-inventor of 107 patents within the United States Patent Office on advanced technologies covering a vast array of wireless, wired, and emerging broadband technologies. In 2005, he was awarded AT&T’s Science and Tech-

nology medal. In 2002, he was inducted into the New Jersey Inventors Hall of Fame by the Governor of the State of New Jersey for his innovations and contributions to science and technology in the telecommunications industry. Today, AT&T, Gerseng is simply known as the father of Project AirGig™ which is a technology that enables Giga-bit data transmission on Electric utility power lines.

Title: Multi-path over 5G for Security and Resilience Enhancement

Abstract: Multi-path transmission exploits the availability of multiple paths through a network to improve the security of transmitted information. In this talk, we explore the idea of using multi-path transmission to enhance the secur-
ity and resilience of communicating over potentionally non-cooperative or even hostile 5G networks. Data transmission over multiple paths, in conjunction with encryption and erasure codes, can provide greater protection against adversarial threats such as eavesdropping and jamming. As we shall discuss, multi-path over 5G presents some in-
teresting tradeoffs between performance and security. Joint work with Masaan Kirit Baiju, Bjorn Hwang and Zeng, Kai.

Bio: Brian L. Kim is a professor in the Dept. of Electrical and Computer Engineering at George Mason University. He received his Ph.D. in electrical engineering from Princeton University and a B.A. in physics from the University of Pennsylvania.

Title: Location Privacy and Risk of 5G Devices

Abstract: Location services such as Apple’s FindMy and WhatsApp’s what’s up have become commonplace in our daily lives, allowing users to locate their friends, family, or lost pets, and even interact directly with them in real-time through social media. However, the data generated by these services also carries risk due to the largest single source of consumer privacy concern is location information. In this talk, we will discuss the potential risks of location tracking, including the increasing use of location data for marketing purposes, and the unintended consequences of location tracking, such as the risk of data breaches. We will also present our findings on the feasibility of using 5G networks for location tracking, and discuss potential solutions to mitigate these risks.

Bio: Dr. Anthony Asplund is an assistant professor in the De-
partment of Computer Science and Engineering at Michigan State University. He is a recognized expert in wireless communication security, and has conducted extensive research on the security of 5G and other wireless devices. He has also served on the editorial boards of several leading journals in the field of computer science. Dr. Asplund received his Ph.D. in computer science from the University of California, Berkeley, and holds an M.S. and B.S. in electrical engineering from Stanford University. He is a fellow of the IEEE, and was recently awarded the 2019 IEEE Communications Society Best Paper Award. His research focuses on the security and privacy of wireless devices, with a particular emphasis on 5G technology.

Title: Hiding Text in Test 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 edit-based, e.g., encoding information into the gaps between sentences. Generative AI, on the other hand, has the potential to hide texts in a natural way. The talk will describe a proof-of-concept system that uses a large language model to generate natural language text that contains hidden information.

Bio: Yin Xu is an Assistant Professor in the Department of Com-
puter Science at George Mason University, where she co-leads the Linguistic Steganography (LS) research group. Her research is focused on building natural language generation systems that can hide messages in a natural way. She has published extensively on this topic and has presented her work at several major conferences. Her research has been supported by the U.S. National Science Foundation and the Human Rights Watch.

Title: Assessing the Socio-economic Impacts of Secure Texting and Anti-Jamming Technologies in Non-Cooperative Networks

Abstract: Opening secure texting over 5G (and legacy) infrastructure is a challenge. In non-cooperative networks, malicious actors may try to decipher, block encrypted messages, or specifically jam wireless radio systems. Such activities can disrupt operations, from causing minor inconveniences to large-scale disasters like border control and unmanned aerial vehicle (UAV) traffic. In this talk, I will describe how we evaluated the socio-economic impacts of secure texting and anti-jamming technologies in non-cooperative networks. We used two open-source simulation models for assessing the socio-economic impacts of oper-
ing in uncooperative non-cooperative networks. The first focuses on using multiple non-
cooperative networks to transmit a message. The second model simulates a case where a message is transmitted to one of the destinations. We used empirical data from 5G networks and 5G untrusted non-cooperative networks and intercepted agents. The results are used to estimate economic losses for private, commercial, government and military sectors. The models use empirical data from 5G networks and 5G untrusted non-cooperative networks and intercepted agents. The results are used to estimate economic losses for private, commercial, government and military sectors. The simulation data and the open-source codebase is provided for reproducibility.

Title: WindText

Abstract: Tradicional linguistic steganography systems are mostly edit-based, e.g., encoding information into the gaps between sentences. Generative AI, on the other hand, has the potential to hide texts in a natural way. The talk will describe a proof-of-concept system that uses a large language model to generate natural language text that contains hidden information.

Bio: Irvn Gerseng AT&T Fellow and Distinguished Inventive Scientist for AT&T Labs in Middlesex, NJ. He is responsible for Advanced Research for the Department of Defense (DoD), AT&T’s 5G mobility projects, emerging broadband infrastructure such as Project AirGig, Advanced RF Research technologies on Department of Defense programs, and heads up the AT&T Science and Technology Center. He holds a bachelor’s degree and a master’s degree in computer engineering from the University of Science and Technology of China.

Event Organizer

Bio: Dr. Anthony Asplund is an assistant professor in the De-
partment of Computer Science and Engineering at Michigan State University. He is a recognized expert in wireless communication security, and has conducted extensive research on the security of 5G and other wireless devices. He has also served on the editorial boards of several leading journals in the field of computer science. Dr. Asplund received his Ph.D. in computer science from the University of California, Berkeley, and holds an M.S. and B.S. in electrical engineering from Stanford University. He is a fellow of the IEEE, and was recently awarded the 2019 IEEE Communications Society Best Paper Award. His research focuses on the security and privacy of wireless devices, with a particular emphasis on 5G technology.

Event Organizer

Bio: Dr. Anthony Asplund is an assistant professor in the De-
partment of Computer Science and Engineering at Michigan State University. He is a recognized expert in wireless communication security, and has conducted extensive research on the security of 5G and other wireless devices. He has also served on the editorial boards of several leading journals in the field of computer science. Dr. Asplund received his Ph.D. in computer science from the University of California, Berkeley, and holds an M.S. and B.S. in electrical engineering from Stanford University. He is a fellow of the IEEE, and was recently awarded the 2019 IEEE Communications Society Best Paper Award. His research focuses on the security and privacy of wireless devices, with a particular emphasis on 5G technology.