CYBERSECURITY FOR CRITICAL INFRASTRUCTURE WORKSHOP

FIGURE 1: CYBERSECURITY FOR CRITICAL INFRASTRUCTURE WORKSHOP

Monday June 10, 2024

The University of Memphis Center for Information Assurance (CfIA) hosted the "Cybersecurity for Critical Infrastructure" workshop on June 10, 2024. It was held in the Fishbowl Room of the FedEx Institute of Technology. The hybrid-format workshop had 73 participants (i.e., 50 in - person, 23 virtual) and covered a wide range of topics centered around cybersecurity for critical infrastructure.

The workshop opened with remarks from Dr. Dipankar Dasgupta, Professor and Director of the CfIA, and Ms. Karen Bell, Associate Chief Information Officer for the University of Memphis (UofM). Dr. Myounggyu Won, UofM Associate Professor of Computer Science, served as the workshop moderator.

The morning technical agenda began with Dr. Jacqueline Mallet's overview of an Akira ransomware attack at Ireland's Reykjavik University where she serves as a cybersecurity professor. Due to the nature of the cyber-attack, she recommended that companies consider investing in offline or cold site backup systems in addition to standard cybersecurity measures.

Matthew White, the leader of Baker Donelson's Cybersecurity and Data Privacy Team, was our next speaker. His presentation was entitled "Current Cyber Threads Facing Critical Infrastructure." He provided a thorough analysis of the cyber-threat landscape and its escalating fiscal impact on corporate America.

Dr. Guillermo Francia, Professor and Director of the University of West Florida's Center for Cybersecurity, provided a presentation on an "Open Platform Infrastructure for Industrial Control System Security." The cybersecurity platform uses containers that can be easily shared and run on multiple hosts. As a result, it provides a feasible and more efficient testing and evaluation process for the security of most industrial control systems.

FBI Special Agent Brian McCloskey provided the last presentation for the morning session. His presentation was entitled the "FBI's Mission in the Cyber Space, Tools, and Resources."

The afternoon session began with Dr. Richard Maiti, Assistant Professor at Kentucky State University, giving a presentation on "Privacy and Security Matters Related to Use of Mobile Devices and Social Media." He discussed some common mistakes and vulnerabilities associated with using mobile devices and social media. Users who routinely share their location information, indiscriminately accept cookies, and use public Wi-Fi make themselves vulnerable to social engineering and other cyber-attacks.

AI & Cybersecurity
➢ AI is Computational Logic, Not Magic!
➢ Success hinges on the breadth and depth of Training Data Coverage ☺
➢ Pre-trained Models are vulnerable to Attacks ☹

FIGURE 2: PANEL DISCUSSION DURING MID-AFTERNOON BREAK

During the mid-afternoon break, a panel discussion was held on the “Challenges and Solutions for Cybersecurity for Grid Systems and Artificial Intelligence (AI).” The participants in the panel discussion were Dr. Dipankar Dasgupta, FBI Special Agent Brian McCloskey, Dr. Mohd Hasan Ali (UofM Associate Professor in Electrical and Computer Engineering), and moderator Dr. Myounggyu Won.

Hans Amelang, University of Memphis master’s degree computer science student, was next. He gave a presentation on “Cybersecurity Threats and Solutions for Satellite Communication.” His presentation focused on low Earth Orbit (LEO) satellite communication systems and the active and passive vulnerabilities associated with their use.

Katherine Stoddard, Professor at Arkansas State University – Midsouth, gave the closing presentation for the day. Her presentation focused on the risks associated with the internet-enabled devices associated with smart homes and Smart Grid.

Figure 3: UofM Faculty, Staff, and Student Worker Host Committee

The event closed with a raffle and closing remarks from Dr. Dipankar Dasgupta.