Be Cyber Safe: Lock Your Digital Doors

***Leon T. Geter**
Interim Dean and Founding Director, Benedict College

Keywords: cybersecurity, cyberattack, dark web, internet of things

Abstract

This presentation delves into the critical realm of cybersecurity, covering fundamental concepts and practical insights to safeguard digital assets. Attendees will gain a comprehensive understanding of: What is Cybersecurity: Exploring the multifaceted approach to prevent cyberattacks and mitigate their impact. Confidentiality, Integrity, and Availability (CIA) of Cybersecurity: Unpacking the CIA triad and its pivotal role in ensuring data security and reliability. Cybersecurity Threats: Delving into selected threats such as phishing, ransomware, and the growing menace of the Dark Web. Hackers' Targets: Analyzing why education and healthcare organizations are prime targets for cyberattacks. Dark Web: Highlighting the lurking dangers and illicit activities on the Dark Web. Internet of Things (IoT): Assessing the cybersecurity implications of interconnected devices. Cyber Safety Tips: Equipping attendees with actionable tips to bolster their cyber defenses and navigate the digital landscape securely by increasing awareness and locking one’s digital doors.

Maritime Cybersecurity: Cybersecurity Solutions for the Maritime Transportation Ecosystem

***Rick Siebenaler**
CEO Maritime Cybersecurity Institute,
University of South Carolina Beaufort
(USCB)

Presentation Keywords: Cybersecurity Maritime Transportation Supply Chain

Abstract:

The Maritime Transportation System handles approximately 90% of the imports and exports of the United States, representing 35-45% of the country's GDP. This vital industry requires a strong cybersecurity protection posture to ensure America's competitiveness, growth and national security. The complexities of the maritime industry, unique technologies utilized, historical under-investment in cybersecurity, and inadequate governance have all led to gaps in our nation's maritime cybersecurity posture.

Building off of a grant from the National Science Foundation and the State of South Carolina, the Maritime Cybersecurity Institute seeks to be a world-class Innovation Engine for the maritime transportation ecosystem with priorities around cybersecurity education, research, experimentation, investment and commercialization of solutions. The Institute is based in South Carolina, but anticipates having national and international impact on the industry.

Key Areas of Focus:

- Addressing cybersecurity challenges within the maritime transportation ecosystem of ports, ships, shipping lines, cargo, people, inland waterways and intermodal transfers.
- Research and solution development to address advances in technology being utilized within the maritime industry
- Improving understanding of maritime industry independencies, vulnerabilities and risks, along with the development of effective strategies to mitigate these risks.
- Catalyzing long term industry and economic growth backed by public-private collaboration and promoting investment in key cybersecurity technologies.
- Actively recruit and include partners from marginalized groups, including women, persons of color, and economically disadvantaged populations.
- Creating and encouraging a culture of innovation.

Leveraging Physical Side-Channel Information – from Attackers' and Defenders' Perspectives

***Zhenkai Zhang**
Assistant Professor, School of Computing, Clemson University, Clemson, SC

Keywords: Cyber Security, Side-channel Attack, Hardware Security, and Attack Detection.

Abstract

When an activity is conducted in a computing device, not only does it take CPU time and memory, but it also consumes power, issues heat, emits electromagnetic (EM) radiation, and possibly produces sound as well as light. These physical side effects of computation, often referred to as physical side-channel information, can in effect reveal a certain amount of knowledge about the ongoing activity. In the past, such information has been extensively exploited to form attacks to breach confidentiality. However, it has been recently realized that such information can also be leveraged to help build security defenses. Metaphorically, physical side-channel information can be used as a “double-edged sword” to cut both ways in the world of cybersecurity. In this talk, I will present how we can forge such a “double-edged sword” from certain EM emanations of computer systems. Specifically, I will demonstrate a new EM side-channel attack developed by our team that allows an attacker to steal sensitive information (e.g., which websites are browsed by a user) from GPUs at a distance. More notably, I will present how we can utilize EM side-channel information to our advantage for creating a novel detection-based defense system against a class of powerful attacks that exploit a widely existing hardware vulnerability known as the rowhammer bug.