Cybercrimes, Cyber-Physical Innovations, and Emerging Investigation Challenges Minitrack

William Bradley Glisson, University of South Alabama bglisson@southalabama.edu
Kim-Kwang Raymond Choo, University of South Australia Raymond.Choo@unisa.edu.au

As technology is incorporated into more aspects of daily life, cybercrimes evolve and diversify, resulting in data intensive environments. Increasing smart-phone sales, increasing digital evidence requests in legal environments, the increasing generation and storage of digital transactions through the integration of the ‘Internet of Things’ (IOT), and the development of cyber-physical attacks all point to the broad societal impacts of technology. The dangers of cyber-physical threats are evidenced by a recent attack on a German steel mill that destroyed a blast furnace [1].

A variety of responses are needed to address the resulting concerns. There is a need to research a) technology investigation efficiency, b) technical integration and solution impact, c) the abuse of technology through cyber-physical attacks along with d) the cost effective analysis and evaluation of large data repositories. The mini-track submissions this year focus on identifying and validating innovative technical solutions to access data from technologies, and also on introducing new students to computer security and digital forensics concepts.

The paper on “Service Set Identifier Geolocation for Forensic Purposes: Opportunities and Challenges” highlights the possibility of using selected passive wireless devices and location inferences from a forensics perspective [2]. Their idea is to endeavor to draw connections between the ever elusive digital world and the physical world, a conflict that every digital investigation struggles to reconcile. The paper on “Capture the Flag as Cyber Security Introduction” attempts to address an issue that is near and dear to educators in the security arena [3]. The authors present their experiences integrating a capture the flag style of competition in GenCyber camps as an approach for engaging future security students. The paper on “Utilizing the Cloud to Store Hijacked Camera Images” highlights the idea that the cloud can be used to store stolen information and that this information is not blatantly acknowledged by forensics tools [4]. This in itself raises questions about the development of future tool functionality. However, more significantly, the paper subtly raises the idea that the cloud can be used as a vehicle for propagating malicious code and that the impact of this propagation is not fully understood from a forensics investigation impact perspective.

Given the relatively new and changing face of the ‘Internet of Things’ and cyber-physical threats, it is important to continue involving interdisciplinary expertise and research capacity in designing state-of-the-art security solutions that can be deployed in a cyber-physical environment.


