

Empowering Engineering and Information Technology (IT) Students to Become Evolutionary Cybersecurity Tinkers

Aparicio Carranza, PhD

The City University of New York (CUNY) :: New York City College of Technology
New York, USA

With the continuously rising importance of how information is acquired, processed and manipulated, verified and validated; and the general management of the interrelated technological components all happening in the physical and the cyberspace, there is an ever growing need for cybersecurity education programs to help address a significant global shortage of engineering and information technology professionals in this field. A flipped classroom is a pedagogical model in which the typical lecture including laboratory portions of the course are reversed in the way that is delivered and conducted – With this perspective, the instructor acts as mentor and the students are empowered with integral responsibilities, such as to prepare case studies and report their findings in class, conduct guided research individually or collaborate in small groups. The notion of a flipped classroom has been studied extensively, and inherits concepts such as active learning, student engagement, and hybrid design. As technology immeasurably improves day to day so does the vulnerabilities and threats – accordingly, the need for security becomes progressively vital. It is becoming more common to hear news about businesses being hacked, sensitive information such as credit card information being stolen, and attacks done by Denial of Service (DoS). The discussion of how Engineering Technology and Information Technology (IT) students have become empowered to conduct their own course of study in the realm of cybersecurity activities will be presented. Furthermore, results of students' work performance will be briefly summarized such as: "Technologies that help ensure privacy in the digital age", "Implementing defenses in the cybersecurity landscape", "The impact of cybersecurity in today's world", "Penetration testing using virtual and physical networks", "automated wireless network penetration testing using wifite and reaver" and "comparison of wireless network penetration testing tools on desktops and raspberry pi platforms".