The Role of Gamification in Attacker-Centric Cyber-Security Education

Gamification is defined as applying game mechanics in a non-gaming context; Game players regularly exhibit persistence, risk-taking, attention to detail and problem solving; behaviours that are ideally suited for effective cyber-security training[1]. Existing cyber-security teaching practices and methods use defensive strategies, in line with the current dominant practice in cybersecurity training. The training/learning is aimed at delivering strategies for defensive reaction against attacks and not on anticipatory or offensive strategies. Moreover, there is a general lack of attacker-centricity within cyber-security education due to various reasons. In a University setup, the network and IT security constraints inhibit the setting up of a hacking lab. For effective cyber-security training it is critical to incorporate characteristics of attacker to not only enabler the students to understand the attacker-behaviour but also to anticipate attacks, which is nifty skill to possess as a cyber-security professional. Lack of safe training environment that emulates the real world scenarios make is challenging to impart ethical hacking skills.

The CyberGaTE project [2] is aimed at building gamified cyber-security training environment. One of the games developed as part of Cyber-GaTE is particularly aimed at investigating the effectiveness of attacker-centric cyber-security training on student learning and engagement. This is achieved by: Creating challenge-based, 'think like a hacker' –type learning resources that would be gamified. Some gaming techniques that shall be explored are real-life problem-based storytelling that would form the basis of the learning content and the use of characters (avatar/role play) and the use of narrative to create a bond between the learner and the avatar thereby enhancing engagement as suggested by literature[3]. CyberGaTE aims to use the known characteristics of cyber-attackers to train participants in anticipating an attacker's motivation and behaviour in carrying out certain attacks. This anticipation enhances the creation and application of both offensive and defensive strategies against cyber-attacks.

[1] Bada, M., Sasse, A., & Nurse, J. R. (2014). Cyber Security Awareness Campaigns: Why do they fail to change behaviour?. Report). Global Cyber Security Centre. [2] CyberGaTE, http://www.cybergate.org.uk [3] Klopfer, E., Osterweil, S., & Salen, K. (2009). Moving learning games forward

Dr Chitra Balakrishna
Senior Lecturer
Edge Hill University