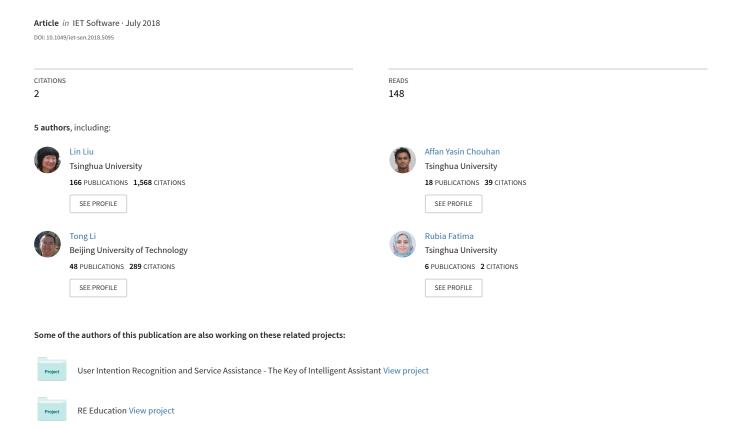
Improving Software Security Awareness Using A Serious Game



Improving Software Security Awareness Using A Serious Game

Lin Liu, Affan Yasin, Tong Li, Rubia Fatima, Jianmin Wang

IET Software, July 2018, the Institution of Engineering and Technology (the IET)

DOI: 10.1049/iet-sen.2018.5095

Improving Software Security Awareness Using A Serious Game

What is it about?

The digital era of today is marked by proliferation of software systems across various platforms used in our daily lives. Examples include mobile phones, laptops, smart watches, etc. It is of utmost importance that the systems continuously provide us with their intended services. The importance of security and privacy protection of these systems has drastically increased due to their penetration in every walk of life. e.g., business, hospitals, education, etc. Software security emphasizes upon the matter which makes software work correctly even under malicious attacks. Attaining and sustaining security level impose complex and interdisciplinary challenges. To make software systems work as they are intended, the training, awareness, and education of the end users regarding system security is of great importance. Similarly, the security personnel of software systems need to understand not only the technical but also the social aspects of security to better defend against cyberattacks.

In this paper, we have: i) designed a serious game to compensate the deficiencies in the literature; ii) performed empirical evaluations including survey, brainstorming and observation to the proposed game.

Why is it important?

- 1. We present the design and implementation of an educational game that embeds: security concepts to evaluate the impact of game-based training on player's cyber security awareness.
- 2. We evaluate the effectiveness of the game through an empirical evaluation using quantitative and qualitative analysis. Based on the outcome of the evaluation we suggest various observations and possible future work.

Perspectives



In sum, this paper explicates a serious game aimed at improving software security awareness of system stakeholders. The design rationales of the game are discussed in detail to highlight the assumptions and prerequisites of a game that is to deliver security related concepts and principles to players who have zero to minimum background knowledge in security. This includes the selection and execution of viable game elements into the game processes. We evaluated the designed game and game



In partnership with:



View publication stats

design approach by running it in a classroom setting, and then collecting the game outcomes and feedbacks from 96 players. The results were encouraging since all participants acknowledged that they understood the security concepts and principles that the game tried to convey. By developing attack scenarios by oneself and then exchanging them with teammates, players understand the attacker's intention in a more realistic way and know of possible countermeasures to mitigate these situations. Thus, CSRAG is interdisciplinary outcome which not only addresses one of the most dire needs of the world of software but also does so in a practical, feasible, user-friendly and an intellectually engaging way.

Read Publication

The following have contributed to this page: Affan Yasin



PDF generated on 19-Aug-2018 Create your own PDF summaries at www.growkudos.com.