WORKSHOP

Inside the Black-box: Playing Digital Security

Rogado, J.[1,2]; Sousa, C.[1]; Costa, C.[1] &Henriques, S.[1]

[1]Centre for Research in Applied Communication, Culture and New Technologies (CICANT) – ULHT

[2]Copelabs – Cognition and People Centric Computing Labs

Abstract

As it has been extensively studied, games characteristics and design models, such as goal oriented tasks, rules, challenges and interactions, can be used to engage students and increase learning. They may also promote an emotional connection to the subject under study, providing opportunities for learning by doing.

In particular, when dealing with aspects related to our digital identities, we most often lack the necessary technical skills, which prevents us to autonomously manage our digital security. In fact, in this field, we often consider technology as a black-box lurking on the background of our lives, rarely being aware of the various ways it can be used for securing our digital identities.

In our 60 minutes workshop, the theoretical principles set out above will be combined with an hands-on approach, proposing a playful activity to the participants, with the goal of explaining the basics of encryption and the fundamental role it plays in today's digital presence. First, a few generic principles will be presented, demonstrating how a simple encryption algorithm, called the Caesar's Cipher, can be used to encrypt short sentences. The Caesar Cipher is a very simple mono-alphabetic cipher that consists in shifting the letters of the plain text. The shift order and direction form the secret or encryption key. This algorithm can be implemented using a very simple hand-made cardboard artefact: the Cipher Wheel, which consists of two concentric circles, each one with a

printed alphabet, that can be manually rotated and assume all the possible 25 different positions/secrets. The Cipher Wheel, has been used in similar activities in the context of the "Games for Media and Information Literacy Learning" research project (GAMILearning - UTAP-ICDT/IVC-ESCT/0020/2014), which addresses the need for student awareness in managing their digital identities with game play and production. The project explores the way that the game analysis and production supports a wide range of media literacy and learning skills.

In the proposed workshop, several Cipher Wheels will be distributed to the participants. who will then be invited to organize themselves into two groups, the messengers and the intruders. The messengers will be divided between senders and receivers, which will sit at opposite parts of the room, with intruders sitting in between. Senders and receivers will then privately agree on a secret number, which will be the key for the Cipher Wheel encoding and, obviously, never to be disclosed to the intruders. The main goal of this activity will be to exchange encrypted messages between senders and receivers, using the agreed secret and the Cipher Wheel. These messages will be forwarded through the intruders, who will try to sneak into the conversation, exploring various possible secrets with their Cipher Wheels, or using whatever other strategies they can imagine to break the secret code. Overall, this playing part of the workshop is planned to take approximately 45mn.

At the end, an interactive reflection of approximately 15mn will be held, analysing the flaws of the encryption utilised, how it can be improved and explaining how more complex algorithms are used by networked systems to promote digital security in real life scenarios. The situations depicted in the activity will be linked to actual threats to which individuals' digital identities are exposed on the Internet, highlighting the essential role that encryption plays on their protection. The heuristics of the approach followed by the participants during the playful experience will also be discussed

following an action research approach, in order to evaluate if and how it promoted their awareness on digital security.

At the end of this workshop the participants will have acquired a good experience on the pedagogical capabilities of games, and the way they can promote their digital identity management literacy.

Keywords: Game-based learning; Encryption; Digital Security; Digital Identity.