The gamification of cybersecurity training

Natalie Coull, Iain Donald, Ian Ferguson, Eamonn Keane, Thomas Mitchell, Oliver V. Smith, Erin Stevenson and Paddy Tomkins

Coull, N., ... et al. 2017. The gamification of cybersecurity training. In: F. Tian, C. Gatzidis, A. El Rhalibi, W. Tang, & F. Charles (eds.) *E-learning and games: 11th International Conference, Edutainment 2017, Bournemouth, UK, June 26 – 28, 2017 : revised selected papers* (pp. 108-111). Cham: Springer.

The Gamification of Cybersecurity Training

Natalie Coull[1], Iain Donald[1], Ian Ferguson[1], Eamonn Keane[3], Thomas Mitchell[1], Oliver V. Smith[1], Erin Stevenson[1], Paddy Tomkins[2]

[1] Abertay University, Bell Street, Dundee DD1 1HG, Scotland
[2] Droman Crime Solutions Ltd, 4.9 Techcube, 1 Summerhall, Edinburgh, EH9 1PL, Scotland
[3] Police Scotland, Scottish Crime Campus, Craignethan Drive, Gartcosh, G69 8AE, Scotland

n.coull@abertay.ac.uk

Abstract. Due to the rapidly and continued evolving nature of technology, there is a constant need to update police officers' training in cyber security to ensure that the UK continues to be a secure place to live and do business. Rather than deliver traditional classroom-based training, our project assesses the effectiveness of the delivery of cyber security through the use of games based learning to simulate cybercrimes and provide training in incident response. The aim of our research is to transform the delivery of first responder training in tackling cybercrime.

Through the use of a Game Jam and subsequent prototype development, we have trialed training materials that are based on serious games technology. The game poses a common incident reported to the police, for example the problem of a virtual person receiving offensive messages via Facebook and the training reflects the dialogue with that person and the technical steps to ensure that a copy of the evidence has been preserved for further investigation. Evaluation has been conducted with local police officers. Overall, this approach to the large-scale provision of training (potentially to a whole force) is shown to offer potential.

Keywords: gamification, serious games, cybersecurity.

1 Introduction

Many of the crimes frequently reported to the Police involve some aspect of digital technology. Cybercrime is no longer limited to describing criminal events where a computer or digital device is the target or tool, e.g. hacking or identity theft. Indeed, technology can play a key part in virtually any criminal investigation. For example, Police Officers responding to reports of a murder may need to investigate the mobile phone of a victim to establish which route they took to their destination, and the browsing history of the murderer could be used to establish intent. Consequently, crime scenes in the 21st century can contain a number of different digital devices, all of which may contain crucial evidence. First responders (those police officers who are the first ones on the scene when dealing with an incident) may be tasked with identifying and seizing those devices and due to the volatile nature of digital evidence, how they interact with those

devices can impact the availability and integrity of evidence. Training police officers in the appropriate handling of digital devices is crucial to ensure that law enforcement can manage crime effectively. Although classroom-based training can be an effective mechanism for delivering cybercrime training, it is expensive and time consuming. There is a clear need to explore alternatives to traditional classroom based training.

2 Gamification of Cybersecurity Training

Computer games afford visually rich, interactive and immersive environments that allow exploration of complex problem spaces, both for entertainment purposes and in serious contexts. Existing research evidences that games can be engaging for a variety of different users [1] and are an effective mechanism for encouraging participation in activities. It is also shown that games enable users to interact with an environment that replicates the real world and have a positive impact on motivation, enjoyment, positive feelings and happiness [2], which consequently can encourage learning and retention of knowledge [3,4].

2.1 Our Solution

Ensuring timely and cost-effective training of cybersecurity to police officers is a key priority for many law enforcement agencies. Serious games is one method that can deliver engaging and measurable training in a relatively cheap manner. A collaboration between academia, industry and law enforcement has led to the completion of a pilot project, described here. We have created a prototype using 3 crime scenarios and conducted an initial evaluation with local law enforcement personnel. Through this project, we have aimed to demonstrate that serious games can provide continually updated training in a way that is engaging for the user, which doesn't take officers off the streets for days at a time to sit in a classroom, and which can be delivered at a fraction of the cost of traditional training techniques. Our project, "First Responder's Guide" is a novel fusion of cybersecurity and computer games technology. The first stage in our research, described here, has led to the creation of a prototype that contains a virtual environment with 3 different crime scenarios. This stage consisted of 3 core activities:1) Game jam, 2) Prototype development, 3) Initial evaluation.

Activity 1: The Game jam
A game jam, typically popular in the gaming community, is an event where a mix of software developers, artists and game designers meet in a physical location to create one or more games over a short period of time (typically 1 to 2 days). These game jams provide an excellent opportunity to focus participants' efforts on developing games around a particular theme and challenge the participants to develop rapid prototypes which can be presented to peers and industry at the end of the game jam.

Our Game Jam was delivered over a 2 day period for the first stage of our prototype development. We used the Game Jam as a mechanism for identifying a broad range of

game ideas and designs that could be utilized in a serious games environment to train Police Officers in responding to cybersecurity incidents. We invited students from across all our digital degree courses to participate in the Game Jam. At the beginning of the game jam, we provided students with a project brief, which outlined the challenges involved in the seizure, acquisition and analysis of digital devices. The students then formed teams to produce their 'asset', i.e. their proposed game to train police officers in cybersecurity. At the end of the 2-day period, each team presented their asset to a team of judges and were scored according to their proposed design, computer graphics, modularity and adaptability. The winning team were then invited to participate in the next stage of the project: Prototype Development.

Activity 2: Prototype Development

The next stage of the project involved developing the winning asset from the game jam into a prototype. The student team worked with representatives from Police Scotland to develop the scenarios which were incorporated into the prototype. The scenarios were developed to simulate the types of crimes involving a digital element that Police Scotland typically encounter. The scenarios can be classified as:

1. A pre-planned operation involving indecent images of children
2. A reactive enquiry in which a complainant has received threatening messages via social media.
3. A spontaneous enquiry involving an attempted fraud of a business via spear-phishing.

Each scenario is built around a virtual environment, which the player can explore using either a 2d or 3d navigation mode. Within the environment are various different objects, depending on the particular scenario. Objects include laptops, mobile phones, credit cards, smart televisions etc. The user is able to inspect the objects and is presented with various different options for interacting with the objects, for example the user can chose to switch off a mobile phone, place it in a faraday cage or seize it for further investigation. For each level of game play, the user is presented with a description of the particular scenario, prior to entering the virtual property. After inspecting the virtual crime scene, the user can choose to leave the property and is then presented with their scores and feedback as to the appropriate course of action.

Activity 3: Evaluation

A short, qualitative evaluation was conducted with a small group of ten police officers to gather feedback on the appropriateness of the prototype. The purpose of the evaluation was to establish police officers current knowledge of cybercrime and incident response and their attitude towards using games for training. Each participating officer was interviewed using hypothetical scenarios, prior to playing the game. Scores for each participant were recorded during game play, before completing a questionnaire on game play and usability.

Results

Although all participants had received some form of training in cybersecurity prior to playing the game, there was some disparity between the interview answers and game play answers. Analysis of the questionnaire responses indicated that some participants found the wording of the questions vague. The navigation controls were also challenging for some participants. This feedback will be invaluable for the next stage of the game development, which will focus on refining the scenarios and in-game text, and removing the joy-stick navigation option so that the controls are more typical of a normal smart 'phone application. Overall, participants were overwhelmingly positive about using games for training purposes.

3 Conclusion

Cyber security is a rapidly developing field with increasing impact on society and attracting the challenges of large and complex data sets on networked computing devices. This impact is reflected in patterns in crime: most of the crimes that Police Scotland investigate now involve computer technology to some extent and so training in this area is imperative. Typical classroom based training can be expensive and time consuming. Using serious game to train police officers in cybersecurity is a viable option. The prototype developed as part of our project is a novel fusion of cyber security and computer games technology to provide a new training tool that harnesses the interactivity of serious games. Importantly, this tool has demonstrated the potential for more effective training to be delivered at a significantly reduced cost, to more staff and without the need for lengthy and expensive classroom-based sessions. Improving the cybersecurity skills of law enforcement personnel will lead to improved response to cybercrime and better preservation of digital evidence.

References

1. Zelinski EM, Reyes R. Cognitive benefits of computer games for older adults. Gerontechnology : international journal on the fundamental aspects of technology to serve the ageing society. 8(4):220-235. (2009).
2. Glover, I. Play as you learn: gamification as a technique for motivating learners. In: Proceedings of World Conference on Educational Multimedia, Hypermedia and Telecommunications 2013. Chesapeake, VA, AACE. (2013).
3. Kumar, J. Gamification at work: Designing engaging business software. In International Conference of Design, User Experience, and Usability (pp. 528-537). Springer Berlin Heidelberg. (2013).
4. Mekler, E.D., Brühlmann, F., Opwis, K. and Tuch, A.N. Do points, levels and leaderboards harm intrinsic motivation?: an empirical analysis of common gamification elements. In Proceedings of the First International Conference on gameful design, research, and applications (pp. 66-73). ACM (2013).