Gamification for teaching and learning computer security in higher education

Z. Cliffe Schreuders, *Leeds Beckett University* Emlyn Butterfield, *Leeds Beckett University*

Abstract

In many cases students in higher education are driven by assessments and achievements rather than the "learning journey" that can be achieved through full engagement with provided material. Novel approaches are needed to improve engagement in and out of class time, and to achieve a greater depth of learning. Gamification, "the use of game design elements in non-game contexts", has been applied to higher education to improve engagement, and research also suggests that serious games can be used for games-based learning, providing simulated learning environments and increasing motivation.

This paper presents the design and evaluation of a gamified computer security module, with a unique approach to assessed learning activities. Learning activities (many developed as open educational resources (OER)) and an assessment structure were developed. A new free and open source software (FOSS) virtual learning environment (VLE) was implemented, which enables the use of three types of experience points (XP), and a semi-automated marking scheme for timely, clear, transparent, and feedback-oriented marking.

The course and VLE were updated and evaluated over two years. Qualitative and descriptive results were positive and encouraging. However, ultimately the increased satisfaction was not found to have statistical significance on quantitative measurements of motivation, and the teaching workload of the gamified module was noteworthy.

1. Introduction

Many students take a strategic approach to study, and focus on tasks that are formally assessed, often to the detriment of other aspects of their education, such as engagement with learning tasks that are not assessed and engagement with readings that provide further scope and context to lecture topics. This predicament has been well discussed in the literature [1], and is supported by the author's experience with a cohort of ten students studying computer security, who in a focus group stated that most of them did not do any of the weekly readings that were allocated (despite digital and, in many cases, hard copies being available to them). A few of these students did some of the readings; however, they estimated to have spent approximately ten minutes in total doing so. Another issue that was identified was that the allocated lab work was not completed; although the students engaged well in the assessed tasks. It has been suggested that an effective approach to an engaging assessment structure is to implement regular assessment tasks [2, p. 154]. However, this approach has its own considerations, such as ensuring that marking criteria remain clear and transparent, marked consistently, feedback is constructive and timely, and all managed within the constraints of staff availability.

In this study gamification was investigated as a method of motivating students to engage in a range of learning tasks with clear and timely assessment and feedback.

Gamification is defined as the application of game mechanisms to non-game contexts, and is becoming widely used across a range of domains, including within higher education, to increase motivation and engagement [3]. A gamified assessment structure and assessment tasks (referred to as 'quests') were developed for a final year undergraduate computer security module, in an attempt to motivate students to engage in a range of learning activities.

Despite the availability of a number of online gamification web apps, scripts, and content management systems (CMS), none of these systems fit the requirements for our intended approach to gamification of education, which is discussed in the Results section. Therefore, a new VLE was developed, which integrated with the University's existing VLE (Blackboard), and provided a unique gamified experience, with quest descriptions, criteria, and real-time feedback capabilities, based on a semi-automated assisted marking back-end.

In this paper, we describe our approach to gamified assessment tasks and structure for the module 'Incident Response and Investigation', a module covering incident response topics such as information security management, log management, integrity and network monitoring, intrusion detection, and live and dead disk analysis. We also present My XP, a novel free and open source software (FOSS) gamification VLE, along with the open educational resources (OER) teaching materials we developed. Although these were developed in tandem and to complement each other, these could be used independently: for example, the labs can be used to teach computer security topics without the gamification assessment aspect.

2. Aims

The primary aims of our approach was to:

Improve student engagement and motivation: As discussed in the next section, it is generally accepted in the literature that gamification has the potential to improve motivation. In particular, we aimed to improve engagement with out-of-class activities, such as completing lab

work and engaging with the literature surrounding the taught topics.

Provide a positive student experience: Gamification has also been shown to have the potential to be enjoyable, which we aimed to apply to our class.

Content coverage: Continue to cover and assess the intended learning outcomes and academic content. The module covered many practical aspects and theoretical concepts of information security and incident response. This included understanding intrusion detection systems (IDS) and writing Snort rules for detecting various kinds of network activity; monitoring and investigating logs and implementing networked Syslog logging and various kinds of alerts; understanding approaches to integrity management including custom scripts for monitoring file integrity, and using tools for monitoring and comparing hash digests; creating and analysing disk images for incident response to determine causes of compromise and subsequent actions of the attackers; methods for backup, redundancy, and recovery; and information security management including risk management, contingency planning, and incident response. The specific learning outcomes for the module were: describe various methods for detecting security breaches and identifying the cause; identify and analyse business needs in terms of incident response and the relevant managerial and technical procedures; effectively respond to an incident and undertake an investigation to discover the specifics of the incident; and, describe techniques and procedures that can be employed to recover data and services after an incident.

In order to achieve the aims of the project, our objectives were to: create a VLE for gamification that provides students (with real-time information about their progress and engagement within the module; transparent and consistent criteria; and, detailed and constructive feedback); create assessment tasks (including lab work and other hands-on applied activities; reflective tasks; and, research and self-guided literature searches); and evaluate the effectiveness of this approach to gamification to computer security education.

3. Background and Related Work

3.1 Innovative methods of teaching computer security

The literature contains discussions of various approaches to teaching computer security. An important skill for computer security professionals is the ability to reason about security by questioning assumptions and looking for vulnerabilities [4]. This could be considered a 'wicked competency': that is, an important real-life skill that is hard to assess [5]. Puzzles have been applied to increase engagement and teach technical security concepts via non-technical means, by drawing from real-life examples, current news stories and having students reflect on the security principles at play and how incidents could be responded to [6]. Science fiction prototyping has been applied to teaching security and encouraging the security mindset, by requiring students to consider societal issues and drafting a plot to a science fiction story that considers possible future scenarios around security issues [7]. Other innovative techniques have also been applied, such as requiring students to cheat at a test, and later reporting how they did it [8], and in an informal setting, Bruce Schneier runs an annual movie plot competition [9], where competitors write short story synopses based on security threats that are very specific and illogical to defend against (such as the banning of baby carriers, in case they are used in an attack by filling them with explosives).

Constructivist approaches to teaching, such as problem-based learning [10], discovery learning [11], and experiential learning [12], suggest that students learn best by "learning through doing". Various methods of student/tutor interaction and information presentation for computer security have been suggested to encourage active learning though discussion, such as focusing on seminars and hands-on work [13].

One form of experiential learning, is via games-based learning. Statistics (and anecdotal evidence) suggests that many of our students choose to play computer games recreationally [14]. The current generation(s) of students have been referred to as "digital natives", and it has been argued that serious games can (and should) be used for digital games-based learning (DGBL) [15]. Learning materials developed in this way allow students to engage with material in a 'known' and enjoyable format; although there is also a risk of disengaging those students who have no interest in games. DGBL has been linked to constructivist learning theories [16], and to a state of "blissful productivity" of engagement loops [17]. Games have been shown to be capable of promoting intrinsic and extrinsic motivation [18]. DGBL has successfully been applied to many educational settings, including the military [19], engineering [20], and computer science [21]. CyberCIEGE is a simulation game that teaches information security and assurance topics, by simulating the management of the security for an office environment [22]. Players make security, cost, productivity, and user satisfaction trade-offs in order to achieve business objectives. CyberCIEGE has been the subject of a number of research projects [23], [24]. In 2012 a presentation was given at the Blackhat security conference, presenting a computer security themed card game, Control-Alt-Hack, which was promoted to educators [25], [26]. Another application of games for teaching computer security is CounterMeasures, which presents security tasks via shell access within a game interface [27].

3.2 Gamification, education, and security

Gamification typically involves applying game mechanics such as presenting tasks as quests to be completed, rewarding completion of quests in the form of experi-

ence points (XP), and providing a clear path to progression, often in the form of "levelling up" through player levels. Other common aspects include rewarding certain achievements with virtual badges, and leader boards, which can foster competition between users and give an indication of how their progress compares to that of others.

Gamification has recently seen a wide range of applications, including use in marketing [28], social media and website engagement [29], fitness and health [30], employee motivation [31], and retail and customer motivation [32]. Gamification typically aims to apply the experience from human-computer interaction (HCI), psychology, and game development to improve engagement and motivation in order to promote desirable behaviour.

Gamification is gaining momentum and acceptance in a growing number of fields, and has been argued to be well suited to educational use [33, p. 22] Although, it has also been argued that gamification can lead to a pure points based focus. Some have claimed that education is already in some sense 'gamified', in that students complete tasks to earn marks ('points'), which results in grades ('levels'), and ultimately the 'badge' of having completed classes and degrees. However, explicitly and pro-actively applying gamification to education can potentially provide improvements [34], and is a current area of widespread research activity. For example, gamification has been applied to higher education as activities that were not assessed, such as the gamification of PeerSpace an online learning environment for computer science students, to encourage them to participate in more social and learning activities [35] to increase voluntary homework completion by psychology students [36] and to increase participation in class discussions [37].

Examples of gamification used as the assessment structure in higher education includes modules run by Professor Cliff Lampe at University of Mitchigan, where XP-based assessments are delivered as quests for students to complete, with many learning tasks for students to choose between [38]. Members of staff sometimes even dress up to deliver quests in character. Another example of gamification in higher education is work by Professor Penny de Byl at Bond University, where the modules "Game Design and Logic" and "Animation" have been gamified, and are also graded based on XP [39]. Both modules are designed to incorporate a VLE containing a chart, referred as a leader board, which was developed in PHP with a Google Docs Spreadsheet back-end. The leader board presents students with their progress using a bar chart with grade boundaries indicated, showing the student's XP, and the class minimum, average, and maximum. XP are rewarded for compulsory and non-compulsory activities. Non-compulsory activities include class participation in the form of the game JustJeopardy, and theoretical and practical tasks; each marked on a pass/fail basis, and capped at a maximum value. Compulsory activities consist of assignments and exams. A survey questionnaire was conducted of the student participants, and showed positive outcomes. Exploratory factor analysis suggested dimensions contributing to student responsiveness to a gamified curriculum, a major dimension being playfulness. De Byl [39] concludes: "Gamification affords the transparency and rapid feedback required to keep students motivated. It is the new token economy worthy of further investigation."

Gamification has previously been applied to increase engagement and enjoyment in security education and training. Capture the Flag events are popular amongst security enthusiasts and prevalent at conferences, such as at the annual DEFCON conference [40], the online CTF365 platform [41], and many other security events [42]. These competitions often gamify security tasks by assigning points to defensive and offensive tasks. Researchers have also applied gamification principles to the usability of CAPTCHAs (via quizzes on altered animations [43], and to evaluate the effectiveness of existing CAPTCHA systems [44]) , for encouraging the use of strong passwords (with competitive avatar development [45]), raising awareness of computer security [46], and have considered uses of gamification in security training [47]. As mentioned, our approach aimed to apply games-based learning and gamification to teach computer security topics in the context of higher education.

4. Methods

The approach to this work was that of design research [48]: an issue was identified (as described in the introduction) and requirements were identified (as listed in the aims section). Consequently, as detailed throughout the remainder of the paper, a solution was designed and an artefact was implemented, which was then evaluated. The implementation resulted in learning activities, assessment, and an interactive website VLE for a module delivered at a UK university, over two years: 10 students in 'year 1', then 22 students 'year 2'.

In year 1 evaluation was conducted using online questionnaires (completed via the university's VLE) and a student focus group, and by monitoring the students' progress, results, and engagement with the module. The focus group was conducted towards the end of the module, and was an opportunity for qualitative data collection. The following questionnaires were used to gather more detailed evaluation:

A survey was adapted with permission from de Byl [39], to evaluate the effects and satisfaction of the gamification and games-based learning that had been implemented. Some changes were made from the original questionnaire, such as changes to use UK terminology.

Questions that were specific to the original author's approach were altered or removed. Additional questions were added to evaluate features of our own approach (such as having multiple types of points, as described later in section 5.1). Each question was presented as a five-point Likert scale. Due to the small sample size, during analysis 'strongly agree' and 'mostly agree' were both considered to indicate agreement; similarly 'strongly disagree' and 'mostly disagree' were both considered to indicate disagreement.

The system usability scale (SUS) [49] was used to evaluate the usability of the My XP site. SUS is made up of ten five-point Likert scale questions, and produces a non-linear usability score out of 100. SUS is a well established and thoroughly validated within the literature to be a reliable measure for satisfaction and usability [50].

In year 2, further quantitative analysis was conduced to compare motivation levels with other modules, measured using the Instructional Material Motivational Survey (IMMS), which contains 36 Likert-scale statements, widely used as a measure of the ARCS model of motivation (Attention, Relevance, Confidence, and Satisfaction) [51].

5. Results

In this section the results are presented, including details of the assessment structure, learning activities, and VLE that were developed, this is followed by the results of evaluation, including quantitative and qualitative feedback.

5.1 Assessment structure

Assessment was based on three types of XP associated with varying learning activities. **Skill XP (sXP)** was earned by completing applied tasks such as lab work and games-based learning. **Knowledge XP (kXP)** was earned by completing research or demonstrating knowledge such as finding and critiquing readings or videos or completing multiple choice questions. **Wisdom XP (wXP)** was earned by completing reflective tasks, such as writing short essays and attack trees [52].

As detailed in the assessment brief, in the module guide, and during lectures, the formula for converting XP to final grades was:

$$\text{Marks} = (sXP + kXP + wXP) / 3000$$

$$\text{If } (sXP < 100 \text{ OR } kXP < 100 \text{ OR } wXP < 100)$$

$$\text{Marks are caped at } 35$$

As a general observation, marks tended towards a natural bell curve, without any need to apply scaling.

5.2 Learning activities and assessment tasks ("quests")

In keeping with a gamified approach, an attempt was made to have all assigned learning activities (other than attendance of lectures) defined in terms of quests with XP rewards.

In year 1, a game of Ctrl-Alt-Hack was played during the first lab session, as an icebreaker exercise with a small sXP reward for having participated. While it did raise awareness of security concepts, it was not directed at any of our other specific aims or learning objectives, and subsequently dropped for year 2.

A large component of the available marks for learning activities was for the lab work, which applies the theory covered in lectures to practical technical tasks and challenges. The lab work required students to demonstrate each of the four learning outcomes, and in each case was marked based on the level of accomplishment. Each lab document consists of guided tasks, which have supporting information and instructions to follow, with some problem solving involved, and then a number of much more open-ended components, which involve considerable problem-based and discovery learning.

In each case the lab document identified at various points what the student needed to save (often screenshots and/or a written solutions), with general requirements specified and in each case students could find more detailed criteria for sXP rewards via My XP.

A number of relevant CyberCIEGE scenarios were provided to students as quests, with sXP rewards for completing the scenarios. One lab session was dedicated to introducing CyberCIEGE, then students were encouraged to work through the scenarios outside of the timetabled sessions. CyberCIEGE scenarios were chosen based on their relevance to learning outcome #2; with an emphasis on the management of information security, which the simulations suited well, and required students to put the management topics from the module into practice. The sXP rewards were assigned based on the estimated completion times provided by the CyberCIEGE developers.

Students earned kXP by finding and reviewing readings and online videos related to each of the module topics.

Short reflective tasks were available to earn wXP: each of these was related to a topic from the module, and required students to demonstrate their understanding and ability to utilise the "security mindset". One of the quests was based on Bruce Schneier's annual movie plot competition: students had to describe a situation where mitigation against an unlikely, yet possible, threat was unrealistic. Unlike Schneier's original version, the students had to describe an approach to responding to the incident after the fact. These activities involved students engaging with each of the module topics, requiring them to synthesise information and demonstrate knowledge relating to each of the learning outcomes.

5.3 My XP

To support students in understanding their progress and allowing immersion into gamification a new VLE, known as My XP, was implemented as a Basic Learning Tools Interoperability (Basic LTI) tool.

The server-side code was developed using the PHP programming language, and made use of the Zend framework for communication with Google Docs, and IMS Global Basic LTI sample implementation code, for providing a secure way of being automatically redirected from the university's VLE to My XP (this is achieved via OAuth). The back-end data storage and processing is handled via a Google Docs Spreadsheet, which can be accessed directly by the tutor, from devices including the mobile phone/tablet used for marking during classes.

The My XP site makes use of JQuery and jqPlot to render the client-side website. The result is a website interface that presents students with their current progress within the module, represented as a progress bar towards "leveling up" to their next grade. For example, at the start of the semester they are "not yet passed" working their way towards a 3rd, following that they work their way towards a 2:2, 2:1, then a 1st (as per the UK HE grading scheme). At any point in the semester they could visit My XP, and see exactly what is required to obtain the next grade, and if they wished to do so based on the module outline they could calculate how far to any particular grade they are aiming for. My XP also displays the total amount of XP they have earned, and this is further broken down to the amount of each of three types of XP they have, which relates to three different types of tasks they can complete to earn XP. They are also shown how their progress compares to the class averages. Figure 1 shows an example of the landing page.

After year 1, MyXP was updated to enable work to be submitted directly via file or form upload.

Once a quest had been marked, the student could immediately reload My XP to view their new current progress.

From the tutor's perspective, the marking was performed directly in the Google Docs Spreadsheet, either via a Web browser or via the Google Drive app. The spreadsheet contained all of the data regarding quests, and marking was a matter of selecting from the list of feedback items, and copying into the student's corresponding feedback cell. This was used to automatically assign the appropriate XP reward, thereby providing a fair and transparent marking process that ensured confidence in the consistency of the results provided. If an appropriate feedback item did not exist, one was created, and was consequently included in the list of potential feedback for the quest.

5.4 Evaluation results

Questionnaire results (year 1)

100% of responses indicated that they prefer having access to their progress on a daily basis. One student did not like to see their position in relation to the rest of the class, while approximately 63% (n=5) preferred to. The XP-based assessment was reported to increase the enjoyment of 75% (n=6) of the class, while the remaining 25% remained neutral. None of the students found the XP-based assessment condescending. None of the students indicated that they prefer the way grades are calculated in other classes; 75% of students preferred the XP point based approach.

The question "I prefer having my grade based entirely on assignments and/or exams" received the most mixed responses, with 50% agreeing and 50% disagreeing. One student indicated that the assessment structure was distracting, while 50% disagreed. Similarly, one student indicated that having three types of XP added unnecessary complexity, while 50% disagreed. However, 75% of students found that having three types of XP helped them to understand the type of work that was available, and no one disagreed. 100% of responses indicated that they prefer being able to pick-and-choose which tasks to complete to earn their grades. Approximately 63% indicated that the marking scheme used was clearer to them than those used in other classes, and no one indicated that other marking schemes were clearer.

The questions related to games-based learning indicated mixed responses: three students (approximately 38%) stated that the use of games made them do more out-of-class work, while another three disagreed. The use of games were reported to increase the understanding of security concepts for 50%, while approximately 38% disagreed. 75% of students indicated that the use of games increased their enjoyment of the class, while 25% disagreed.

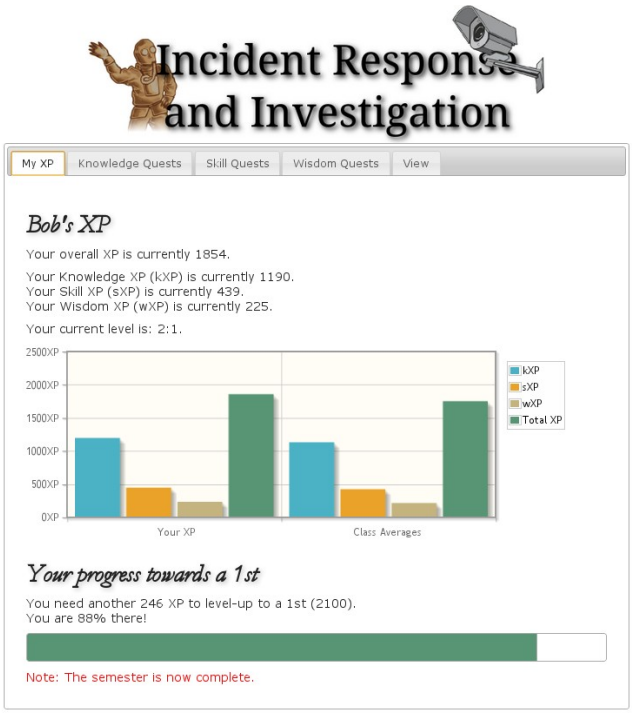

Figure 1: My XP landing page.

In terms of engagement, approximately 88% (n=7) stated that they checked their grades more often than in other classes. For 75% of students, it made them turn up to class more regularly, one disagreed. Approximately 88% of responses state that having XP rewards for lab work made them complete more than they do when it is not marked directly, no one disagreed. 100% of students agreed that getting XP for readings and videos made them do more out-of-class self-directed study. 100% also stated that they did more out-of-class work in general as a consequence. Finally, 100% also agreed that the structure of the assessment made them research and learn about related content that they would not have otherwise explored.

System usability scale (SUS) results (years 1 and 2)

In year 1, the system usability scale (SUS) score for My XP, was a mean of 75.36 out of a possible maximum of 100 (M=75.36, SD=19.33). In year 2 (after software updates), the SUS score for MyXP was a mean of 90.19 (M=90.19, SD=13.29, N=13), compared to the institution VLE as deployed on a similar module, with a mean of 88.75 (M=88.75, SD=13.92, N=12). Cronbach's Alpha for the 10 item scale was .85 and .81 for the two VLEs respectively, indicating the scale was highly reliable. A within-subjects Wilcoxon Signed-Ranks Test indicated that the effect was not statistically significant between the usability of MyXP and the university VLE, $Z=-0.169$, $p < 0.87$.

The Instructional Material Motivational Survey (IMMS) results (year 2)

The Instructional Material Motivational Survey (IMMS) total score mean for the gamified module was 152.32 (M=152.32, SD=18.13, N=12), compared to the score for a similar non-gamified module of 146.76 (M=146.76, SD=21.54, N=12). Cronbach's Alpha for the 36 item scale was 0.89 and 0.92 for the two modules respectively, indicating the scale was highly reliable. A Paired Samples T-Test indicated that the effect on motivation was not statistically significant (95% CI, -11.13 to 22.24); $t(11)=.733$, $p = 0.48$. Post-hoc power calculation indicates that the sample size (N=12) has Power of 0.811, for large effect size (dz=0.8). That is, there may have been sufficient sample size if the effect had been large (as hypothesized).

Qualitative results

The general sense of the feedback from the class was positive. The qualitative results from the focus group and the open-ended survey questions included many positive comments. For instance, this survey feedback: "The gamification made the module a lot more enjoyable for me. It is a different approach to learning that hasn't been the same thing constantly throughout my entire education. I honestly wish all modules would follow the same kind of grading path."

Five students were present for the focus group. The above sentiment was repeated by students during the focus group. There was also consensus within the focus group that they wished more modules broke down assessment to a similar extent. Survey feedback also included the comment: "I would like to see the game process implemented onto more modules." Focus group participants stated that they liked the chart that shows their position in relation to the class averages, and the progress bar showing progress towards grades. They stated that it is very clear how to progress within the module. Marks are further broken down than in other modules. This approach also reportedly helped students with time management.

The requirement to find their own readings and resources for the wiki was "better" than when they were provided with readings to do, and they stated that it resulted in them doing more reading around the module topics. All of the students present agreed that they spent on average two hours each week on readings and videos. They also reported, that this process instigated even further (non-assessed) self-directed reading. This was noted as a significant improvement over the engagement of the same students in a previous module.

The negative comments and constructive feedback included the general consensus that CyberCIEGE was quite challenging, and some students thought too much so, or at least too much effort compared to the available XP rewards. Similarly, others stated that readings and video reviews were seen as the easiest way to earn XP, and perhaps lab work was under-rewarded for the required time and effort. The fact that for a large percentage of the semester students had "not yet passed" was also distressing to some.

6. Discussion

Despite the small sample/class size, we contend that our results support the literature that asserts positive outcomes *can* result from the gamification of education, specifically in relation to computer security in higher education. On one level, the application of gamification resulted in achieving each of our aims: it caused a number of improvements to student engagement, such as improving time spent on independent research, completing lab work, and engaging in out-of-class activities, it provided a framework for reflective tasks designed to engage students in the security mindset, while covering the learning outcomes and content we intended, and did so while increasing the apparent enjoyment of the class, resulting in a positive student experience. However, when compared quantitatively with other similar teaching approaches, the effects are inconclusive.

Our first aim, improving student engagement, was somewhat successful. Year 1 questionnaire responses indicated that a consequence of the gamification was an increase in the amount of completed lab work (for 7 out

of 8 students), and for all students an increase in online research, readings, videos and self-directed study, time spent on out-of-class work in general, and they all reported researching and learning more about related content as a consequence.

However, in year 2 measuring and comparing motivation via IMMS was inconclusive, despite Power to potentially detect large effects. Although non-significant results do not confirm the null hypothesis is true (that there is no difference), it does raise questions about the underlying effect size of the gamification's effect on motivation, and whether the enthusiasm for gamification as a panacea for student motivation is warranted.

The second aim, student experience, could be considered a success. From review of the feedback and questionnaires conducted, students indicated that in many ways they preferred this approach, with a number of students commenting that they thought it would be a good idea for more modules to take a gamified approach, and use assessment that breaks marks down similarly.

Our final aim, that of content coverage, can be considered a success. Although the gamification of the module had an affect on the way that tasks were presented to students and marked, the gamification had no affect on the content that the module covers.

As reported in the results section, the usability evaluations of My XP, resulted in SUS scores of approximately 75 in year 1 and 90 in year 2 (out of 100). Bangor et al. [50, p. 592] provides guidance on interpreting SUS results, based on the analysis of an extensive number of usability studies. They propose that "products which are at least passable have scores above 70". No statistically significant difference was found compared to the university VLE. Based on these results we conclude that the site is reasonably usable and acceptable to students, and that satisfaction was good.

Our results seem to indicate that the games-based learning (as implemented) was less compelling than the gamification of the module. The games-based learning received far more mixed responses from the questionnaire. CyberCIEGE was disliked by some of the students; however, a number of positive comments were received throughout the semester, including the statement that having to repeat tasks (such as setting firewall rules) until correct, helped to solidify security concepts that they had previously learned. In hindsight the educational value of Control-Alt-Hack was arguably too indirect for use in a final year lab session.

Our experience suggests that gamification of education need not be that different to other approaches with highly regular assessment tasks. Many of gamification features (such as regular assessment, and self-direction) could be considered to be consistent with a student-centred approach to education [53]. Although we chose to make the gamification aspect explicit to students in the terminology and description of the assessment structure, many of these characteristics could be applied in less explict ways.

In our experience, some of the challenges and apparent limitations of gamified education include:

Finding the right balance of XP rewards so that students choose to spend their time appropriately and also feel that their time is valued and fairly rewarded is a challenge. Assigning XP to tasks, each with a spread of marks based on the quality of work, while having the final overall number add up to a maximum amount and having levels of achievement that reflect meeting LOs required careful planning, and yearly adjustments.

The gamification approach seems to work well with a module that does not have very large assessment tasks, and which suit having smaller assessed tasks. Gamification would perhaps not be as suitable for modules with exams or large projects with an assessed final state, since these would not suit the "progress bar" interface.

Per-student, the marking workload was substantial, which is a noteworthy consideration given the inconclusive comparative quantitative results. Despite a positive experience, it was our personal judgment that the increased workload did not justify continuing to gamify the module in this way; we are currently investigating ways of retaining noted benefits, while reducing the associated burdens.

Conclusion

A novel approach to teaching computer security topics has been presented, using gamification and games-based learning. The assessment structure was based on a unique approach with three types of XP corresponding to different kinds of activities. A VLE was developed, My XP, which presented students with their current status and progress towards "leveling up" grades, along with quest details. Each quest was displayed along with feedback possibilities with corresponding XP rewards, which is used by tutors to mark the work. This mechanism constitutes a unique approach to marking and feedback for gamified assessment. Our use of gamification achieved: positive student engagement, positive student experience, and content coverage. However, statistical comparisons on effects on motivation were inconclusive.

The resulting VLE and lab exercise sheets are a product of this work, and are available under free and open licenses. My XP is free open source software (FOSS), and the exercises are open educational resources (OER).

References

[1] K. Starcher and D. Proffitt, "Encouraging Students to Read: What Professors are (and Aren't) Doing about It.," Int. J. Teach. Learn. High. Educ., vol. 23, no. 3, pp. 396–407, 2011.

[2] C. Rust, "The Impact of Assessment on Student Learning How Can the Research Literature Practically Help to Inform the Development of Departmental

Assessment Strategies and Learner-Centred Assessment Practices?," Act. Learn. High. Educ., vol. 3, no. 2, pp. 145–158, Jul. 2002.
[3] S. Deterding, D. Dixon, R. Khaled, and L. Nacke, "From game design elements to gamefulness: defining 'gamification,'" in Proceedings of the 15th International Academic MindTrek Conference: Envisioning Future Media Environments, New York, NY, USA, 2011, pp. 9–15.
[4] B. Schneier, "Inside the Twisted Mind of the Security Professional," Wired March, vol. 20, no. 08, 2008.
[5] P. Knight, "Fostering and assessing 'wicked'competences," Milton Keynes Open Univ. McCabe DL Treviño LK 1993 Acad. Dishonesty Honor Codes Context. Influ. J. High. Educ., vol. 64, pp. 522–538, 2007.
[6] M. Bishop, "Teaching context in information security," J Educ Resour Comput, vol. 6, no. 3, Sep. 2006.
[7] T. Kohno and B. D. Johnson, "Science fiction prototyping and security education: cultivating contextual and societal thinking in computer security education and beyond," in Proceedings of the 42nd ACM technical symposium on Computer science education, New York, NY, USA, 2011, pp. 9–14.
[8] G. Conti and J. Caroland, "Embracing the Kobayashi Maru: Why You Should Teach Your Students to Cheat," IEEE Secur. Priv., vol. 9, no. 4, pp. 48–51, 2011.
[9] B. Schneier, "Announcing: Movie-Plot Threat Contest," Schneier on Security, 2006. .
[10] A. J. Neville, "Problem-based learning and medical education forty years on. A review of its effects on knowledge and clinical performance," Med. Princ. Pract. Int. J. Kuwait Univ. Health Sci. Cent., vol. 18, no. 1, pp. 1–9, 2009.
[11] J. S. Bruner, "The act of discovery," Harv. Educ. Rev., vol. 31, no. 1, pp. 21–32, 1961.
[12] D. A. Kolb and R. E. Fry, "Toward an applied theory of experiential learning," Theor. Group Process, 1975.
[13] J. Li, Y. Zhao, and L. Shi, "Interactive teaching methods in information security course," in Proceedings of the 2009 International Conference on Scalable Computing and Communications; 8th International Conference on Embedded Computing, Washington, DC, USA, 2009, pp. 489–493.
[14] TNS/Newzoo/Gamesindustry.com, "United Kingdom National Gamers Survey 2009: Summary report on Basic Topics," 2009.
[15] M. Prensky, "Digital game-based learning," Comput Entertain, vol. 1, no. 1, pp. 21–21, Oct. 2003.
[16] K. Kiili, "Digital game-based learning: Towards an experiential gaming model," Internet High. Educ., vol. 8, no. 1, pp. 13–24, 2005.
[17] J. McGonigal, Reality is broken: Why games make us better and how they can change the world, vol. 169. Penguin Press, 2011.
[18] E. E. Mattheiss, M. D. Kickmeier-Rust, C. M. Steiner, D. Albert, and others, "Motivation in Game-Based Learning: It's More than'Flow'.," in DeLFI Workshops, 2009, pp. 77–84.
[19] M. Prensky, "True believers: Digital game-based learning in the military," Digit. Game-Based Learn., 2001.
[20] M. Ebner and A. Holzinger, "Successful implementation of user-centered game based learning in higher education: An example from civil engineering," Comput. Educ., vol. 49, no. 3, pp. 873–890, Nov. 2007.
[21] M. Papastergiou, "Digital Game-Based Learning in high school Computer Science education: Impact on educational effectiveness and student motivation," Comput. Educ., vol. 52, no. 1, pp. 1–12, Jan. 2009.
[22] C. E. Irvine, M. F. Thompson, and K. Allen, "CyberCIEGE: Gaming for information assurance," IEEE Secur. Priv., vol. 3, no. 3, pp. 61 – 64, Jun. 2005.
[23] C. C. Fung, V. Khera, A. Depickere, P. Tantatsanawong, and P. Boonbrahm, "Raising information security awareness in digital ecosystem with games - a pilot study in Thailand," in 2nd IEEE International Conference on Digital Ecosystems and Technologies, 2008. DEST 2008, 2008, pp. 375 –380.
[24] B. D. Cone, C. E. Irvine, M. F. Thompson, and T. D. Nguyen, "A video game for cyber security training and awareness," Comput. Secur., vol. 26, no. 1, pp. 63–72, Feb. 2007.
[25] T. Denning, T. Kohno, and A. Shostack, "Control-Alt-Hack: A Card Game for Computer Security Outreach, Education, and Fun," Department of Computer Science and Engineering, University of Washington, Technical Report UW-CSE-12-07-01, 2012.
[26] Tadayoshi Kohno, T. Denning, and A. Shostack, "Presentation: Control-Alt-Hack(TM): White hat hacking for fun and profit (A computer security card game)," in Black Hat USA, Las Vegas, NV, USA, 2012.
[27] C. Jordan, M. Knapp, D. Mitchell, M. Claypool, and K. Fisler, "Counter-Measures: a game for teaching computer security," in Proceedings of the 10th Annual Workshop on Network and Systems Support for Games, Piscataway, NJ, USA, 2011, pp. 7:1–7:6.
[28] K. Huotari and J. Hamari, "Defining gamification: a service marketing perspective," in Proceeding of the 16th International Academic MindTrek Conference, New York, NY, USA, 2012, pp. 17–22.
[29] G. Zichermann and C. Cunningham, Gamification by Design: Implementing Game Mechanics in Web and Mobile Apps. O'Reilly Media, Inc., 2011.
[30] M. N. K. Boulos and S. P. Yang, "Exergames for health and fitness: the roles of GPS and geosocial apps," Int. J. Health Geogr., vol. 12, no. 1, pp. 1–7, Dec. 2013.
[31] J. Kumar, "Gamification at Work: Designing Engaging Business Software," in Design, User Experience, and Usability. Health, Learning, Playing, Cultural, and Cross-Cultural User Experience, A. Marcus, Ed. Springer Berlin Heidelberg, 2013, pp. 528–537.
[32] S. Lounis, X. Neratzouli, and K. Pramatari, "Can Gamification Increase Consumer Engagement? A Qualitative Approach on a Green Case," in Collaborative, Trusted and Privacy-Aware e/m-Services, C. Douligeris, N. Polemi, A. Karantjias, and W. Lamersdorf, Eds. Springer Berlin Heidelberg, 2013, pp. 200–212.
[33] K. M. Kapp, The Gamification of Learning and Instruction: Game-based Methods and Strategies for Training and Education. John Wiley & Sons, 2012.
[34] S. Smith-Robbins, "This game sucks": How to improve the gamification of education," Educ. Rev., vol. 46, no. 1, pp. 58–59, 2011.
[35] C. Li, Z. Dong, R. H. Untch, and M. Chasteen, "Engaging Computer Science Students through Gamification in an Online Social Network Based Collaborative Learning Environment," Int. J. Inf. Educ. Technol., vol. 3, no. 1, pp. 72–77, 2013.
[36] R. N. Landers and R. C. Callan, "Casual Social Games as Serious Games: The Psychology of Gamification in Undergraduate Education and Employee Training," in Serious Games and Edutainment Applications, M. Ma, A. Oikonomou, and L. C. Jain, Eds. Springer London, 2011, pp. 399–423.
[37] M. Cronk, "Using Gamification to Increase Student Engagement and Participation in Class Discussion," World Conf. Educ. Multimed. Hypermedia Telecommun. 2012, vol. 2012, no. 1, pp. 311–315, 2012.
[38] H. W. Mak, "The Gamification of College Lectures at the University of Michigan," http://www.gamification.co/2013/02/08/the-gamification-of-college-lectures-at-the-university-of-michigan/, 2013. [Online]. Available: http://www.gamification.co/2013/02/08/the-gamification-of-college-lectures-at-the-university-of-michigan/. [Accessed: 22-Aug-2013].
[39] P. de Byl, "Can Digital Natives Level-Up in a Gamified Curriculum?," in 29th annual ascilite conference, Wellington, New Zealand, 2012, pp. 256–266.
[40] DEF CON Communications, Inc., "DEF CON® Hacking Conference - Capture the Flag Archive," https://www.defcon.org/html/links/dc-ctf.html, 2013. [Online]. Available: https://www.defcon.org/html/links/dc-ctf.html. [Accessed: 17-Dec-2013].
[41] CTF365, "CTF365 Alpha," http://ctf365.com/, 2013. [Online]. Available: http://ctf365.com/.
[42] A. Keane, "Presentation: Better Network Security Through Gamification," presented at the HEAnet National Conference 2013, Athlone, Ireland, 2013.
[43] J. Kani and M. Nishigaki, "Gamified CAPTCHA," in Human Aspects of Information Security, Privacy, and Trust, L. Marinos and I. Askoxylakis, Eds. Springer Berlin Heidelberg, 2013, pp. 39–48.
[44] R. Saha, R. Manna, and G. Geetha, "CAPTCHINO - A Gamification of Image-Based CAPTCHAs to Evaluate Usability Issues," in 2012 International Conference on Computing Sciences (ICCS), 2012, pp. 95–99.
[45] C. Kroeze and M. S. Olivier, "Gamifying authentication," in Information Security for South Africa (ISSA), 2012, 2012, pp. 1–8.
[46] J. Pufahl, "Presentation: HuskyHunt – The Gamification of Security Awareness for Students," presented at the Social Media Strategies for Client Services, Massachusetts, USA, 2013.
[47] J. A. Amorim, M. Hendrix, S. F. Andler, and P. M. Gustavsson, "Gamified Training for Cyber Defence: Methods and Automated Tools for Situation and Threat Assessment," in NATO Modelling and Simulation Group (MSG) Annual Conference 2013 (MSG-111), 2013.
[48] V. Vaishnavi and W. Kuechler, "Design Research in Information Systems," Jan. 2004.
[49] J. Brooke, "SUS-A quick and dirty usability scale," Usability Eval. Ind., vol. 189, p. 194, 1996.
[50] A. Bangor, P. T. Kortum, and J. T. Miller, "An Empirical Evaluation of the System Usability Scale," Int. J. Hum.-Comput. Interact., vol. 24, no. 6, pp. 574–594, 2008.
[51] D. A. Cook, T. J. Beckman, K. G. Thomas, and W. G. Thompson, "Measuring motivational characteristics of courses: applying Keller's instructional materials motivation survey to a web-based course," Acad. Med. J. Assoc. Am. Med. Coll., vol. 84, no. 11, pp. 1505–1509, Nov. 2009.
[52] B. Schneier, "Attack trees," Dr Dobb's J., vol. 24, no. 12, pp. 21–29, 1999.
[53] G. O'Neill and T. McMahon, "Student-centred learning: What does it mean for students and lecturers?," AISHE Emerg. Issues Pract. Univ. Learn. Teach., p. 27, 2005.