Provocative Games to Encourage Critical Reflection

Daisy Abbott, Olga Chatzifoti and Sandy Louchart
The Glasgow School of Art, Glasgow, UK
d.abbott@gsa.ac.uk
o.chatzifoti@gsa.ac.uk
s.louchart@gsa.ac.uk

Abstract: The SECRIOUS project takes a game-based approach to improving knowledge and attitudes in cybersecurity practices. Our methodology includes interdisciplinary Serious Game co-design with coders and aims to produce critical reflection on participants' own coding practice. To encourage this we created a series of Small Provoking Games (SPGs) about the project's three overarching topics (Code Security; API Security; Security Lifecycle) and five co-produced themes (Coder Practices; Code Motivation; Morality; Resources; Communication). Games and play are well-suited for creating both reflection-in-action and reflection-on-action. Provoking a lasting change in attitudes towards secure coding practice requires dialogic or inquiry-based reflection leading to transformative reflection We define a 'provoking game' as one that uses the techniques of reflective game design to produce cognitive and affective challenge – a eudaimonic appreciation of the player experience. This emphasises a player's sense of purpose and aims to create exo-transformation (change in attitudes and/or practice outside the game.) SPG design foregrounded Khaled's principles of reflective game design and was led by serious game experts, a cybersecurity expert, and a playwright, and included input from the entire SECRIOUS team to define each game's specific focus. Two SPGs were produced: Protection (which challenges the assumption of 'absolute' cybersecurity protection) and Collaboration (which highlights communication in cybersecurity developer teams.) A third game is in development. SPGs feature highly exploratory gameplay, expected failure, and focus on metaphor (of both game objects and player actions) to create doubt, contradicting existing mental models and encouraging the players to question the game rules and underlying concepts. The games were used within game-jams to provoke critical discussion, a creative mindset, and group reflection. This paper analyses the design process of these two SPGs and reflects on our contribution to reflective game design.

Keywords: Serious Games, reflective game design, critical thinking, cybersecurity, reflection

1. Introduction

The overall goal of the SECRIOUS project is to engage coders in cybersecurity issues as both players and designers of serious games. The main problem was defined not as a lack of knowledge resources but as a need to shift attitudes towards attaining and effectively using knowledge about cybersecurity. To achieve this, our methods needed to 1) encourage critical reflection leading to attitudinal and behavioural change and 2) elicit the nature of cybersecurity practice. Provoking a lasting change in attitudes towards secure coding practice requires dialogic or inquiry-based reflection leading to transformative reflection (Baumer, 2015; Mekler, Iacovides and Bopp, 2018). Small, provoking games (SPGs) are proposed as an effective method for interventions that aim to challenge learners' (false) preconceptions and create revised understandings. We define a 'provoking game' as one that uses the techniques of reflective game design to produce cognitive and affective challenge and aims to create exo-transformation (change in attitudes and/or practice outside the game) (Mekler, Iacovides and Bopp, 2018). In this sense, SPGs are about players' self-awareness and attitude shift with regards to their subject matter.

As well as functioning as standalone games, our SPGs were specifically designed to enmesh with our cybersecurity game jams to provoke reflection and contribute to the co-design process of new serious games arising out of the game jam. As such, the SPGs play a part in wider methodological development for the co-design of serious games. This paper covers the context of using serious games to provoke critical reflection, our methodology and methods, an analysis of the games themselves (both available at SECRIOUS, 2022), and our reflections on this process.

2. Research background

The concept of 'reflection' has been defined in numerous ways and there is no single, widely-accepted definition. However, literature reviews (Atkins and Murphy, 2018; Reflection Toolkit, 2020) note that despite the range, complexity, and abstraction of scholarly writing on reflection, differences are typically around terminology and the structure of the metacognitive process. Definitions tend to share three main elements which can be summarised simply as: reflection is a *conscious exploration* of the *self* to *construct new insights*. Furthermore, the literature tends to agree on three key stages of reflection: Breakdown (also called discomfort, surprise,

conflict, or dissonance); followed by Inquiry (analysis); which may lead to Transformation (new perspective, affective and/or cognitive change) (Schön, 1992; Baumer, 2015; Atkins and Murphy, 2018).

The depth of reflection is defined in different ways and using different terminology. Depth is typically structured as a hierarchy from superficial observations, through intentional inquiry and/or dialogic reflection which constructs links to one's own experiences and/or wider social and ethical constructs, to truly transformative and/or critical reflection that results in a meaningful shift in beliefs, approach, or behaviour and that extends into the future. Critical reflection specifically includes "bringing unconscious aspects of experience to conscious awareness" (Sengers *et al.*, 2005, p. 50).

Existing literature on reflection within serious games notes that many games' purposes go beyond knowledge acquisition and aim for attitudinal or behavioural change, for which reflection at least at the level of constructing relationships between a game and real life is required (Khaled, 2018; Mekler, Iacovides and Bopp, 2018; Whitby, Deterding and Iacovides, 2019). Khaled notes that simulations of real life processes afford reflection as they "explicitly represent systems of beliefs, propositions and processes [...] enabling interrogations of validity" (2018, p. 5), a characteristic shared by games. However, "Unlike simulations, games are inextricably linked with the notion of designed challenge and often also with difficulty. [...] Non-trivial challenge, analysis and problem solving, key parts of the reflective process, are already present in how we generally understand games." (pp.5-6). Mekler, Iacovides and Bopp also state that games are particularly suitable for supporting reflection as they "confront players with puzzling or surprising situations, which invite them to plan, experiment and look for new solutions" (2018, p. 315) , matching the three key stages of reflection. Schön (1992) distinguishes reflection-in-action as synchronous with practice and reflection-on-action, which occurs after the activity has taken place. Reflection-on-action can (but does not necessarily) result in behavioural/attitudinal change and can also feed back into reflection-in-action. In the context of serious games, a combination of both types of reflection can result in-game reflective processes (e.g. developing your conceptualisation of the game or altering your play style) and out-of-game changes in, for example, self-image or behaviours (Whitby, Deterding and Iacovides, 2019). Games' potential clearly reaches beyond reflection-in-game as the fictionalised challenges both provoke curiosity and grant agency, which supports reflection in out-of-game contexts (cf. Khaled, 2018, p. 22), demonstrating again the real potential for games as a medium to support transformative reflection.

Various principles for reflective game design have been proposed, although there is no unified approach (Kitson *et al.*, 2019). It is important to begin by challenging the assumption of 'fun' that is still common in research on serious games. Serious games can, of course, be fun however, a more important concept is that of the 'serious experience' (Mekler, Iacovides and Bopp, 2018), where negative emotions can lead to positive experiences, producing eudamonic appreciation (i.e. contentment from having purpose in life). In other words, games can be *rewarding*, whether or not they are also *enjoyable*. This concept is particularly important when considering reflective game design and it is noted that greater cognitive and affective challenge tend to lead to greater appreciation (Whitby, Deterding and Iacovides, 2019 p.340). Kitson *et al.* note that "although we can use technology to design for transformative experiences, we do not design the experiences themselves but rather create the conditions to invite them" (2019, p. 2). Useful analyses of design qualities that inhibit or encourage reflection in game design (Sengers *et al.*, 2005; Khaled, 2018; Mekler, Iacovides and Bopp, 2018; Whitby, Deterding and Iacovides, 2019) have been synthesised into our recommendations for reflective game design:

- Provide for interpretive flexibility (Sengers *et al.*, 2005) to encourage the active construction of meaning crucial for reflection and meaningful 'questions over answers' (Khaled, 2018, p. 23).
- Expose unconscious aspects through challenging player expectations (of game systems, narrative, content, and external assumptions) (Sengers *et al.*, 2005; Khaled, 2018; Mekler, Iacovides and Bopp, 2018); explicitly designing to "engage, problematise, and potentially conflict with cultural and social norms" (Whitby, Deterding and Iacovides, 2019, p. 339); and making learning clear and conscious (Khaled, 2018, p. 23).
- Create player actions/decisions that are emotionally or cognitively meaningful to increase eudaimonia and extended reflection (Whitby, Deterding and Iacovides, 2019, p. 345).
- Provoke the player. Khaled calls this "Disruption over comfort" and notes that "Games that are designed to disrupt can create opportunities for players to be thoughtful, creative and innovative"(2018, p. 23). It includes techniques of distancing, surprise, and failure to help trigger the critical analysis necessary to contradict an existing mental model. However, it is also crucial that provocation needs to be well-balanced for player engagement.

3. Provoking game design

Drawing on the recommendations for reflective game design above, our main emphasis (in both design process and SPG product) was on: *interpretive flexibility*; *disruption of/subverting* expectations; *expected failure/frustration* during construction of meaning; explicit *out-of-game reflection*; and *rigour*. Our aim was to focus players' attention on critically examining the game object's behaviours and the rules governing their interactions. Therefore, the majority of player responses should take place at the meta level - outside of the game. To maximise critical reflection, we defined overall principles for designing the SPGs.

1. Abstraction of the content entities to their essential properties and methods, and re-rendition in a fictional, unconventional metaphor.
2. Integration with out-of-game activity to re-contextualise game content and experience within the domain of cybersecurity.
3. Use of metaphor to "mask" familiar content and create the distance conducive to critical reflection.

3.1 Interdisciplinary co-design

SPG design was in the context of a highly interdisciplinary research project and it was crucial to maximise the different types of expertise within this team. This paper's authors (all serious game specialists) worked closely with a cybersecurity expert and a playwright. This collaboration was particularly fruitful as it allowed thorough and nuanced investigations of the problem area, focussing on the most important intended outcomes. This laid rigorous groundwork for a well-scoped serious game intervention. The cybersecurity expert ensured the validity of the content and its modelling, whilst the playwright was crucial in producing a creative, unconventional metaphor, as well as designing an engaging overall narrative and story beats for the games. Furthermore, the entire SECRIOUS research team was involved in ideation for each game's subject, and contributed feedback, validation, and oversight throughout the design and development process. We consider this interdisciplinary approach to have been absolutely crucial for rigour.

3.2 Design and implementation of two provoking games for cybersecurity

3.2.1 Triadic Game Design

Triadic Game Design (TGD) is well-established as a rigorous serious game design method and can also be used for documentation and evaluation (Harteveld, 2011). TGD breaks serious game design into three aspects: Reality (where the investigation of the problem area and the associated subject matter takes place); Meaning (where the intervention strategy to generate change is designed) and Play (where the gameplay to best achieve this change is designed.)

The Reality aspect was analysed in interdisciplinary meetings with the support of data gathered in user-centred workshops that SECRIOUS held for this purpose, cross-referenced with related literature to clearly define each problem area and establish priorities. An ideation phase focussed on creating questions inspired by the project's three overarching topics (Code Security; API Security; Security Lifecycle) and five co-produced themes (Coder Practices; Code Motivation; Morality; Resources; Communication). These questions were used to identify an overall concept for three SPGs which together cover these topics and themes. (This paper considers the first two games; the third is currently in development.) Each SPG design process started with the preconceptions that we aimed to target in each game's audience. Led by cybersecurity experts, we composed a set of entities/concepts essential to the specific subject in question and defined key messages that the game should convey.

For the Meaning phase, we drew explicitly on the principles of design-for-reflection to produce an intervention strategy with a list of associated learning mechanics. Using guidance for serious game workflows (Abbott, 2020) we defined: 1) intended outcomes; 2) learning context; 3) learning behaviours (using Bloom's Taxonomy (Anderson and Krathwohl, 2001)); and 4) emotional design. We then used this information to select appropriate Learning Mechanics (LMs) from the Learning Mechanic Game Mechanic (LM-GM) Framework (Lim *et al.*, 2013). We also considered the LMs for the post-play activity as these 'out of game' reflections were core to our strategy.

For the Play phase, we worked with the playwright to devise a premise for a comprehensive metaphor and a loose narrative plot to cover the intended outcomes arising from the Reality and Meaning phases. Working with the cybersecurity expert, we translated subject matter entities into in-game objects and the subject matter principles into game rules. LMs were mapped directly to appropriate Game Mechanics (GMs). We shortlisted a set of genres and play-styles appropriate to the LM-GM mappings and content, formulated player actions, and

designed the serious gameplay loops. We also specified in-game performance assessments, win/lose conditions and concluded with level design, which was directed to stage in-game events inspired by real-life conditions. These activities all drew directly from the LM-GM mapping that arose from the TGD process. It is important to note that this is not a fully linear process and iterative design cycles clarified and reinforced elements in all three phases. Lastly, game designers specified the content for the post-play activity. The specific design of each SPG is summarised below.

3.2.2 SPG#1: Protection

The first SPG, named Protection, was designed to address the following preconceptions:

- Coders think cybersecurity is an optional and obscure feature that is the domain of dedicated experts, rather than an essential aspect of any application.
- Coders think that cybersecurity is binary, instead of thinking in terms of a fluid and changing landscape of risk that is in constant need of re-assessment.
- Coders not appreciating the diverse range of mitigation strategies and their suitability towards certain threats, or compatibility to each other.
- Coders thinking of cybersecurity as an independent layer with a view of "the more the better", whereas it is an integral part that should be balanced with functionality.

This led to the definition of the following learning outcomes. After playing players should:

- Perceive cybersecurity as a crucial component of any system
- Reflect on their own coding practice.
- Understand that absolute security is not possible.
- Understand that risk assessment is contextual and can fluctuate over time.
- Grasp the concepts of risk, threat and countermeasures and figure out that threats and defences have multiple (1-many) relationships.
- Acknowledge that security features may have functionality trade-offs.

The most relevant Learning Mechanics were the *Simulation* of a fictional yet recognisable situation which allows players to *Explore* and use *Experimentation* with *Feedback* to reverse-engineer the rules of the game which in turn allows them to *Analyse* and *Plan* how to succeed. We explicitly excluded *Instruction* and *Guidance*, however, implicitly in the meta-game and explicitly in the post-play activity, the player is prompted to compare how these rules reflect or contradict their own mental model of their cybersecurity practices. To serve these LMs, we selected the core Game Mechanics of *Movement* (to explore and avoid threats), *Collection* (of defences/mitigations), *Design/Editing* (of a defence strategy), and *Strategy/Planning* (to adapt to changing contexts). Figure 1 shows the gameplay loop with associated Learning and Game Mechanics.

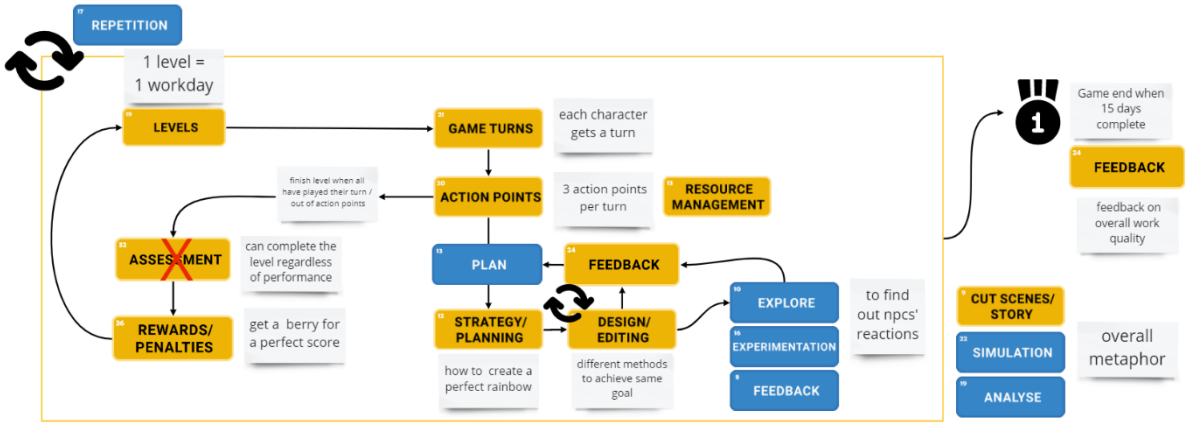

Figure 1: gameplay loop showing mapping of Learning and Game Mechanics for Protection

We then designed the core metaphors for game objects and game rules. These are summarised in Table 1, Figure 2, and Figure 3.

Table 1: each game object with its justification for Protection

Game object	Justification
Main character	A hybrid biological/electronic entity to convey the universality of the concept of security.
Digital rainforest	An ecosystem of software applications with a changing context (day-night cycle represents abundance vs scarcity).
Plants	Data suppliers.
Berries	Data that the character can process: beneficial orange berries give power (juice) to the main character; harmful purple berries (poison) have a delayed corruption effect (as from malware) and blue berries stick the main character's mouth shut, mimicking a distributed denial of service attack.
Malicious agents	Hackers. Each predator has a different movement pattern (patrol, hunt, spring-trap) and damage effects representing common attack methods, such as control hijacking, process shut down, asset theft, etc.
System parts	Cybersecurity defence strategies that negate or mitigate negative effects and increase main character's functionality and ability to avoid threats.

Figure 2: Protection game objects

Game rules, reflecting the principles laid down during the Reality phase, are:

- A character starts unable to defend themselves and needs to collect and install system parts for defence. Installing defence modules takes time and resources.
- Some threats can be rendered obsolete by installing the proper defence modules, some can only be mitigated, while for others there are no defences and the player needs to avoid those threats.
- Some threats can become more or less dangerous based on other conditions. For example, blood sucking mosquitos become more dangerous if the player is paralyzed by a spider and cannot escape.
- Some defence modules render others useless, while some defence modules complement each other. E.g. a filter module at the I/O port (prevention mechanic) makes the database compartmentalization module (contingency mechanic) redundant.
- Installing the most impervious defence module significantly increases resource consumption and limits functionality.
- Installing too many defence modules causes system overload and triggers a non-responsive state until upgrades are uninstalled.

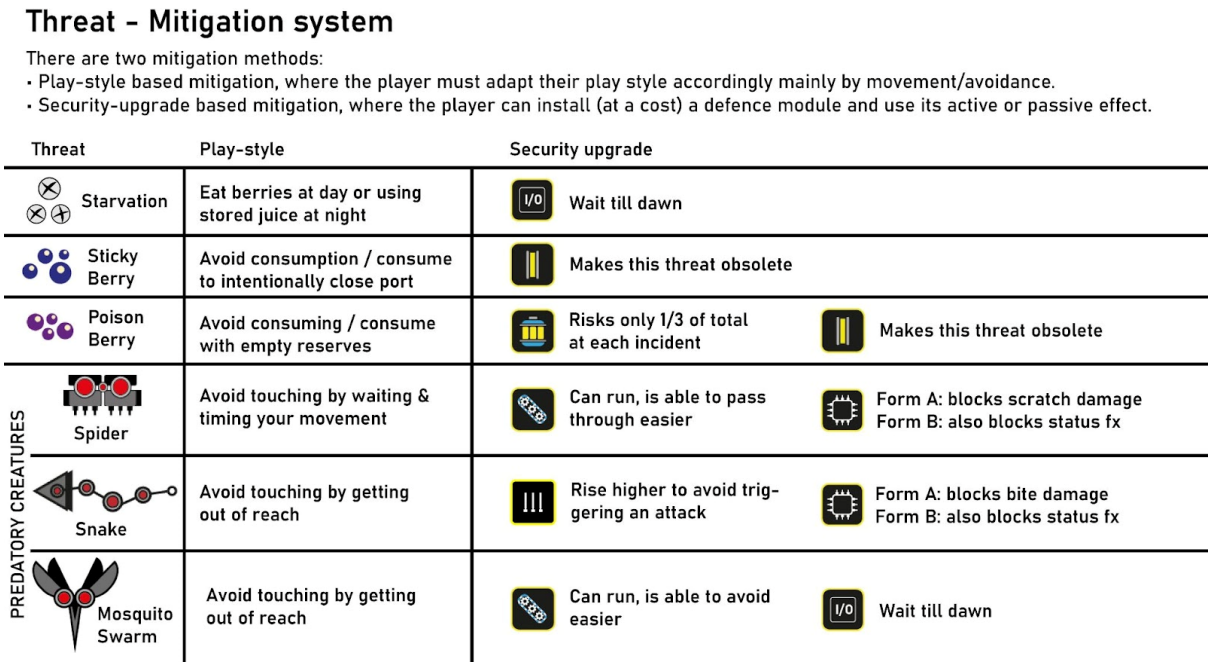

Figure 3 – Summary of Threat-Mitigation interactions in Protection

In terms of gameplay, Protection is a short, 2D, side-scrolling, real-time, single-player game with genre elements from action (move/avoid/collect), strategy (manage resources/select) and puzzle (choose/combine). The player must navigate a risky landscape, trying to survive against various threats using diverse defence systems. Our design avoided common tropes associated with these genres (e.g. score, time pressure, lifecount), allowing instead the exploratory approach conducive to critical thinking. Productive failure is a core concept and the player is expected to 'die' at least once as they gather information. The player must analyse feedback loops to discern the game's rules and create defence responses. Feedback is frequently counterintuitive or surprising, subverting players' expectations. The three main in-game actions are moving, collecting, and installing/uninstalling defence systems (the main educational player action, mirroring the process of risk assessment and defensive planning). This requires the player to first find the respective module (which represents gaining and updating knowledge in real life.) Protection is single-player to serve our goal of inquiry-based reflection on an individual's own practice.

The story takes the protagonist on a journey of natural evolution and intentional change, starting with the protagonist becoming aware of their own existence and expanding into developing movement and a metabolic cycle (input/output). Intentional change is ensuring survival by installing combinations of defence systems. The character has no explicit purpose other than surviving in its harsh, native environment. The story concludes with the protagonist symbolically mastering these conditions and flying away. In the post-play activity, players were asked to interpret in cybersecurity terms what they thought the entities represented and what they deduced from the story.

3.2.3 SPG#2: Collaboration

The second SPG, Collaboration, was designed to address these problem areas:

- Developers (or teams) working on different parts of the code tend to operate in an isolated way and cybersecurity issues can creep in due to a lack of overview and/or communication.
- Developers may not treat communication as an important part of their job and consequently may not be willing to devote time and energy to it.
- Human/"soft" skills are an undervalued and frequently untrained skill set in highly technical work environments but are crucial for successful project delivery and good work conditions.

This led to the following core learning outcomes. After playing players should:

- Understand that the security of the product is only as good as the security of the weakest link.
- Understand that the quality of communication across teams can affect the quality of the end-product.

- Appreciate that the human side of communication is as important, energy consuming and skilled as the technical content.
- Grasp that security needs to be implemented in multiple aspects and stages, therefore overview and communication throughout the development pipeline is necessary.
- Reflect on their own communication skills and cybersecurity contexts.

Learning Mechanics were identical to Protection, however, this time they were mapped to *Levels* and *Game Turns* (representing time in the Security Lifecycle), *Action Points* (representing worker time/resources), and the same *Planning*, *Design*, *Resource Management*, *Feedback* cycle as in Protection. See Figure 4.

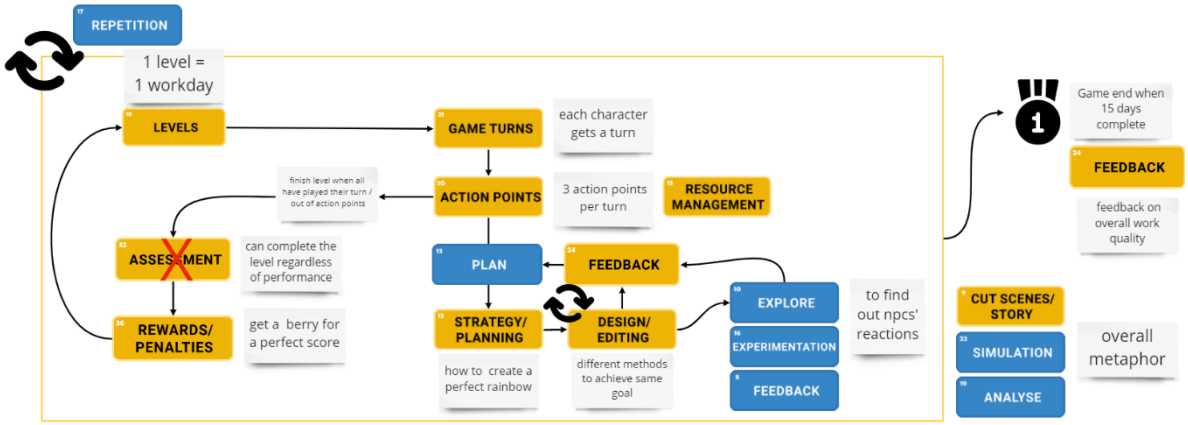

Figure 4: gameplay loop showing mapping of Learning and Game Mechanics for Collaboration

We then designed the core metaphors for game objects and game rules. Collaboration adopts the same fictional universe with its light-hearted tone and colourful iconography as Protection, but expands the list of in-game entities, summarised in Table 2 and Figure 5.

Table 2: each game object with its justification for Collaboration

Game object	Justification
The Rainbow	An infrastructure that outputs 'rain' into the digital rainforest, representing a publicly-used software application with its seven coloured lanes representing the dimensions of the cybersecurity requirements.
Rain	Data flow that can become corrupted without secure infrastructure.
Trees	The user community that relies on the infrastructure to serve a vital need, and the variable health of the ecosystem.
Monsoon season	Represents the duration of the team project: 15 days (15 game levels.)
Main character	The same main character as Protection.
Other characters	Various colleagues, similar but distinct creatures with their own personalities (expressed by face) and expertises (expressed by colour).

Collaboration game rules are:

- Each co-worker can construct lanes in their own colour/expertise. Some roles can combine their efforts to construct lanes in a composite colour. Some roles are unique and impossible to substitute.
- Each co-worker has their own personality and default mood/behaviour ranging from highly motivated through indifferent to opposed to the project's goal.
- Talking to NPC co-workers influences their mood and behaviour. Each personality responds differently to various communication styles.
- At the end of a work day, the Rainbow should have all 7 coloured lanes. Each missing or incorrect lane reduces the cybersecurity quality of the Rainbow and contributes to Rain acidification.
- Acid rain impacts the health of the ecosystem. Damage accumulates over the duration of the monsoon season.
- There is no personal reward or penalty for the team members for the quality of their work. The only feedback that exists is the observed health of the ecosystem.

- There is no fail threshold for each level, or for the game overall. A player is allowed to complete a level (commit code) no matter what cybersecurity quality the Rainbow has
- Damage done to the ecosystem can be ameliorated to a small degree using berries, which are generated if a level is completed with a perfect score.

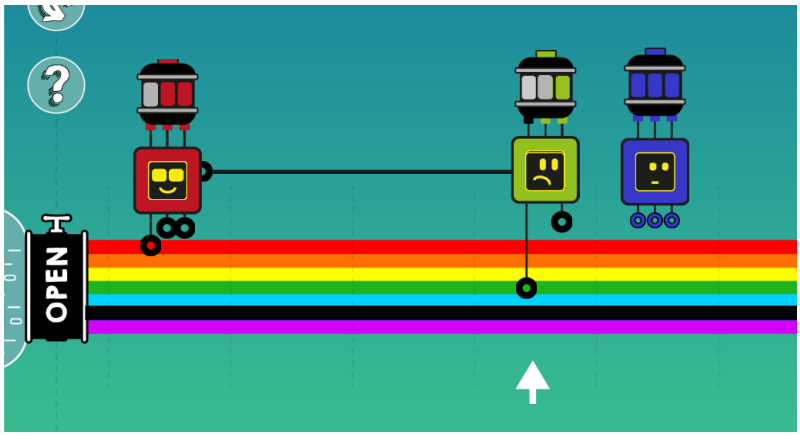

Figure 5: cropped screenshot from Collaboration showing communication and different moods

Collaboration is a turn-based, puzzle game, with each level representing a work day and a whole game run representing a software project. Collaboration is single-player with AI agents to model specific behaviours. The puzzle for each level is to find the appropriate actions to take in order to make the safest Rainbow possible. This requires players to learn/recall the order of colours in the Rainbow (an abstraction of technical skills), and also observe and understand their colleagues' personalities (the human aspect). The challenges are designed to be not always feasible or perfectible. Furthermore, the challenges frequently have more than one solution representing different approaches to problem-solving. In Collaboration, time was quantified in work shifts and had a sense of chronological order which led us to adopt the turn-based approach. Space was irrelevant as a concept which led to a single, static level design where all actions took place. Main variables for each level were the team composition and the Rainbow puzzle, allowing for levels to be procedurally generated. Action points were an essential mechanic to signify units of energy/time during a work shift. The player can choose to spend their action points constructing a rainbow lane (writing code) or communicating with their co-workers. This is a direct translation of the key message that communicating is as essential and time consuming as coding, but also equally an integral part of development work.

As in Protection, players were asked to undertake a post-game activity and describe in cybersecurity terms what (they thought) the entities reflected, but this time players were also asked to directly reflect on how they manage their real-life work relationships and compare that to in-game events.

4. Discussion

These two SPGs appear, on some level, to be quite different. In Collaboration, players have a clear premise, identity, and objective and the game rules are highly scaffolded with a tutorial and reference manual. On the contrary, in Protection, players have ambiguity and freedom with instructions limited to the game controls and absolutely everything else open to interpretation. However, both games were designed with the fundamental concept of provocation through both the subverting of player expectations and of withholding information about the game rules which forces players to experiment, explore, and actively construct their own meanings and mental models. Game differences are to focus the player's attention to best achieve each game's intended outcomes. An evaluation of the SPGs in terms of their effectiveness in achieving reflection is outside the scope of this paper (detailed evaluation is forthcoming). However, we can comment on preliminary results from using Protection and Collaboration within Serious Game Jams on the SECRIOUS project.

Firstly, the abstraction of technical detail and focus on visualising concepts and processes through a friendly metaphor made our SPGs an ideal medium for introducing cybersecurity to a novice audience. Cybersecurity is not often depicted in such a playful manner and this could help to promote engagement. Player feedback on the graphical style was very positive, whilst noting that the game setting was "difficult to interpret". The adoption of metaphor makes the post-play activity essential to a complete SPG experience as, whilst the games in isolation could create critical reflection, our overall purpose was reflection as part of co-design activities. Post-play

reflection is an established technique in simulation-based training where an 'after-action review' helps players to receive extrinsic feedback, gain an overview, and analyse their performance (Meliza, Goldberg and Lampton, 2007). Our goal was rather to create dialogue as players compared and contrasted different interpretations of the metaphor and, by doing so, deepen their understanding of and relationship to cybersecurity concepts. Recontextualization during the post-play activity actively prompted players to compare their in-game experience with their real-life practices and note any new observations arising and their potential implications in real world terms. Post-play reflections demonstrated a variety of interpretations of character identity and which threat-defence combination was the most useful, implying different critical judgements (or at least different play styles). Furthermore, players effectively analysed and re-mapped the in-game content to SECRIOUS Cybersecurity Concept Cards (a forthcoming SECRIOUS output), with some very insightful responses. Therefore, we consider the ambiguity in asset design and gameplay to be successful.

Our SPGs excluded mechanics that promote 'gamified' engagement, such as competition and rewards. Protection also eschewed any instructions to orient the player. Furthermore, the games had a hybrid genre style, for example, Protection looked and felt like a platformer but control mastery was not the way to win, it was instead strategic thinking. It could be argued that this unfamiliar gameplay encourages reflection, however they may also have decreased engagement. In Protection players were initially confused (one asked "Are were supposed to know how to do this?"), however, continued experimentation allowed players to construct meaningful connections between game events and cybersecurity concepts. Players did express surprise (and sometimes frustration) during gameplay, especially at points that had been designed to challenge expectations or provoke 'out of the box' thinking, for example, the realisation in Collaboration that it was not possible to always get a perfect score, or the narrative twist in Protection that too many upgrades causes an overload.

Finally, it is important to note that our SPGs were designed as a single (or limited) user experience. Replayability was not a design goal and the focus was firmly on their place within a wider educational and creative methodology. This implies that SPGs for similar purposes could be made even shorter to improve completion whilst still providing the basis for critical reflection.

5. Conclusion

We have presented the rigorous design process of two Small Provoking Games which feature highly exploratory gameplay, expected failure, and focus on metaphor. We integrated gameplay experience with a range of post-game activities designed to create doubt, contradict existing mental models, and encourage players to reflect on underlying concepts and make links with real-world practice. Whilst evaluation is still in progress, it can be seen that these provoking games have been successful in creating ambiguity, meaningful connections, and an accessible introduction to cybersecurity concepts. A formal evaluation will follow to analyse if these characteristics have been successful in our core goals of 1) creating inquiry-based reflection, and 2) supporting players in the move from consumers of cybersecurity-themed games to co-designers.

Acknowledgements

The authors thank our collaborators at Civic Digits, a company that works at the intersection of games, performance and technology. Civic Digits' director, Dr Clare Duffy is a playwright and theatre director and Rupert Goodwins is a technical Journalist with a specialism is cyber security.

The SECRIOUS project work is supported by the Engineering and Physical Research Council (Grant ID: EP/T017511/1).

References

Abbott, D. (2020) 'Intentional Learning Design for Educational Games : A Workflow Supporting Novices and Experts', in Schmidt, M. et al. (eds) *Learner and User Experience Research: An Introduction for the Field of Learning Design & Technology*. EdTech Books. Available at: https://edtechbooks.org/ux/11_intentional_learn.

Anderson, L. and Krathwohl, D. (2001) *A taxonomy for learning, teaching, and assessing: A revision of Bloom's taxonomy of educational objectives*. Boston, MA: Allyn & Bacon.

Atkins, S. and Murphy, K. (2018) 'Reflection: a review of the literature', *Journal of Advanced Nursing*, 18(8), pp. 1188–1192. doi: https://doi.org/10.1046/j.1365-2648.1993.18081188.x.

Baumer, E. P. S. (2015) 'Reflective Informatics', pp. 585–594. doi: 10.1145/2702123.2702234.

Harteveld, C. (2011) *Triadic game design: Balancing reality, meaning and play*. 1st edn. London: Springer. doi: https://doi.org/10.1007/978-1-84996-157-8.

Khaled, R. (2018) 'Questions Over Answers: Reflective Game Design', in Media, P. D. of D. (ed.) *Playful Disruption of Digital Media*. Singapore: Springer, pp. 3–27. doi: 10.1007/978-981-10-1891-6_1.

Kitson, A. *et al.* (2019) 'Transformative experience design: Designing with interactive technologies to support transformative experiences', *Conference on Human Factors in Computing Systems - Proceedings*, pp. 1–5. doi: 10.1145/3290607.3311762.

Lim, T. *et al.* (2013) 'Strategies for Effective Digital Games Development and Implementation', in Baek, Y. and Whitton, N. (eds) *Cases on Digital Game-Based Learning: Methods, Models, and Strategies*. Hershey, PA: IGI Global, pp. 168–198. doi: 10.4018/978-1-4666-2848-9.ch010.

Mekler, E. D., Iacovides, I. and Bopp, J. A. (2018) '"A Game That Makes You Question...": Exploring the Role of Reflection for the Player Experience', in *Proceedings of the 2018 Annual Symposium on Computer-Human Interaction in Play*. New York, NY, USA: Association for Computing Machinery (CHI PLAY '18), pp. 315–327. doi: 10.1145/3242671.3242691.

Meliza, L. L., Goldberg, S. L. and Lampton, D. R. (2007) *After Action Review in Simulation-Based Training*. Florida. Available at: https://apps.dtic.mil/sti/citations/ADA474305.

Reflection Toolkit, T. (2020) *Reflection Literature Review*. Edinburgh. Available at: https://www.ed.ac.uk/sites/default/files/atoms/files/reflection_literature_review.pdf.

Schön, D. A. (1992) *The Reflective Practitioner: How Professionals Think in Action*. Routledge. doi: https://doi.org/10.4324/9781315237473.

SECRIOUS (2022) *Provoking Games for Cybersecurity*. Available at: https://secrious-research-project.itch.io/ (Accessed: 2 May 2022).

Sengers, P. *et al.* (2005) 'Reflective design', *Critical Computing - Between Sense and Sensibility - Proceedings of the 4th Decennial Aarhus Conference*, pp. 49–58. doi: 10.1145/1094562.1094569.

Whitby, M. A., Deterding, S. and Iacovides, I. (2019) '"One of the Baddies All along": Moments That Challenge a Player's Perspective', in *Proceedings of the Annual Symposium on Computer-Human Interaction in Play*. New York, NY, USA: Association for Computing Machinery (CHI PLAY '19), pp. 339–350. doi: 10.1145/3311350.3347192.