CyberGaTE
A Gamified Virtual Training Environment

Dr. Chitra Balakrishna
Senior Lecturer, Edge Hill University
The CyberGaTE team

• Dr Chitra Balakrishna

• Prof Daniela Romano

• James Coleman

• Michael Banford
Agenda

- Need for Change in Cyber Security education
- CyberGaTE - Project Aims and Objectives
- Why Gamification?
- CyberGaTE – Student as Pro-Sumers
- Work in Progress
- GameJAM
- Results
Motivation

Based on two important studies ISACA (2015) and H M Government (2014).

- There is a clear shortage of cyber security professionals within UK, while the cyber-threats are on an exponential increase.
- Despite the fact that nearly 70% of the 130 Universities in UK offer some form of cyber security courses.
- Fresh graduates lack real-world skills that employers demand.
- Employers value experience more than academic qualifications.
The Need for Change in Cyber-Security Education

• An effective cyber-security training calls for change of behavior that requires more than providing information about risks and reactive behaviors.

• Understanding of how different people perceive risks is critical to effective training

The GAP

• Most cyber-security teaching methods use defensive strategies, in line with the current dominant practice in cybersecurity which is to react, largely, to attacks and not engage in anticipatory or offensive strategies

• There is a general lack of attacker-centricity, the characteristics of attackers are seldom incorporated in training in order to understand these attackers or anticipate their attack
CyberGaTE: Objectives

• Develop a holistic game-based cyber-security training environment

• The environment to incorporate various elements of real-life scenarios that would have learners as active participants

• Gamification enables to balance the offensive and defensive cyber-security training

• Use known characteristics of cyber-attackers to train participants in anticipating an attacker's motivation and behaviour in carrying out certain attack

• The gamified learning resources are to be hosted on a virtual training environment using the innovative concept of ‘Classroom as a Service’
Innovative Pedagogical Practices

CyberGaTE Innovation in Content Creation and Delivery

Content Creation:
• Concepts of Problem-based/Challenge-based Learning
  – drawn from our previous project Cyber Security Knowledge Exchange (CSKE)
• Gamification
  – Tool for student engagement and for effective learning of cyber-security concepts

Delivery:
• A virtualized immersive learning environment is hosted on a cloud based on concepts of Classroom-as-a-Service.
Project Deliverables

• CyberGaTE learning environment
  – A self-directed, virtualized training ground hosting gamified learning resources accessible via the Internet
  – We aim to reach a vast learner-base beyond the scope of the host institution.

• Self-contained gamified learning resources
  – These are aligned with current best practice, IASME, ISO27000 series, PAS555 (ISO, 2013). These will be available as stand-alone learning resources in an open repository along with facilitator guide, hardware and software requirements to deliver the course within a lab environment.
Gamification

• Applying game mechanics in a non-gaming context

• The project aims to address issues of engagement and motivation through the use of game mechanics and gamification techniques

• Some gaming techniques that shall be explored are real-life problem-based storytelling that would form the basis of the training content to keep the learner motivated.
We are not the first!

<table>
<thead>
<tr>
<th>Game</th>
<th>Offensive Training</th>
<th>Defensive Training</th>
<th>Environment</th>
<th>Other features</th>
</tr>
</thead>
<tbody>
<tr>
<td>Counter Measure [5]</td>
<td>Yes</td>
<td>None</td>
<td>Simulated</td>
<td>Limited features and content.</td>
</tr>
<tr>
<td>CyberCeige[6]</td>
<td>None</td>
<td>Yes</td>
<td>Simulated</td>
<td>Proprietary, limited features and content.</td>
</tr>
<tr>
<td>Cyber Nexus[7]</td>
<td>Yes</td>
<td>None</td>
<td>Simulated</td>
<td>Proprietary</td>
</tr>
<tr>
<td>Cyber Protect[8]</td>
<td>None</td>
<td>None</td>
<td>Simulated</td>
<td>Proprietary and limited awareness</td>
</tr>
<tr>
<td>Netwars[9]</td>
<td>Yes</td>
<td>Yes, Limited</td>
<td>Simulated</td>
<td>Proprietary</td>
</tr>
<tr>
<td>Micro Games[10]</td>
<td>None</td>
<td>Yes</td>
<td>Simulated</td>
<td>Proprietary and limited features</td>
</tr>
</tbody>
</table>
Problems with the existing Cyber Games

• Most of them are proprietary and not mostly target industry professionals training for certifications.

• None of them have both offensive-defensive strategy combined.

• Games are built by the companies or institutes and used by the trainees or students. No collaboration.

• All of the games simulate the security features into the game with no access to real-world servers
CyberGaTE Differentiator

- Active collaboration between the content producer and consumer.
- Balance of defensive-offensive strategies within the games
- Free and open source for educational use.
- Most important is the game is not simulated, instead game is hosted in a virtual training environment with access to servers, firewalls at the backend.
Problems with the existing Cyber Games

• Most of them are proprietary and mostly target industry professionals training for certifications.
• None of them have both offensive-defensive strategy combined.
• Games are built by the companies or institutes and used by the trainees or students. No collaboration.
• All of the games simulate the security features into the game with no access to real-world servers.
Student as Pro-Sumers

**Students** engage as co-creators of the content, actively facilitated by industry and academic experts, who collectively identify and capture the cyber security skills gap.

**Students** would be voluntary evaluators of the CybeGATE training environment, when embedded into cyber security modules across year 2, 3 and masters degree program.

**Students** team shall be recruited to deconstruct and gamify and generate interactive TEL versions of the content under the supervision of a gamification academic expert.

**Students** team shall be recruited to design and implement a virtualised training environment based on principles of Classroom-as-a-Service under the supervision of an academic expert.
Interim Progress

**Work package 1: Aim**

- *Identify the top four areas of shortage in cyber-security from the perspective of academics, employers, industry experts and students.*

**How?**
- **Crowdsourcing** - online survey targeting employers, academics and domain experts
- **Workshops** - Group discussion and brain storming with industry partners and domain experts
- **Students** – A Survey conducted as part of MSc project

**Deliverable**
- A course content specification document with clearly identified topics and areas of focus.
The Survey

- **Employers** identified cyber-security skills that were hard to find among fresh cyber security graduates
  - [https://docs.google.com/forms/d/17vLR9OT6CaJmoA-Ev7xhmiy6IS5aAPQl4UgjxOO-XSM/viewanalytics](https://docs.google.com/forms/d/17vLR9OT6CaJmoA-Ev7xhmiy6IS5aAPQl4UgjxOO-XSM/viewanalytics) (20 industry respondents)

- **Academics** identified cyber-security areas that were challenging to teach based on student performance and student learning experience (6 academics on email survey)

- **Students** identified cyber-security areas that were difficult to understand and apply due to the lack of hands-on experience (three groups each at L5, L6, L7)
  - [https://docs.google.com/forms/d/1uwr2Cpj9PWLQcwbiWXd7SF04iXpKOmls9K_7mgg58YI/edit?ts=574d6669#responses](https://docs.google.com/forms/d/1uwr2Cpj9PWLQcwbiWXd7SF04iXpKOmls9K_7mgg58YI/edit?ts=574d6669#responses)
Four common areas of Cyber Security Identified

• *Penetration Tests and Ethical Hacking*

• *Intrusion Detection and Monitoring*

• *Incidence Response and Management*

• *Implementing Secure Systems*
GameJAM

Work Package 2: Gamification

- GameJAM - A Focus-group activity with heterogeneous group of students.

- The students were given a brief talk on cyber-security and a pilot lesson plan and asked to provide idea for possible games that would deliver the learning objectives.

Participant profile

- Level 4, level 5, level 6, level 7 as well as PhD scholars, included gamers as well as non-gamers.
- Both male and female students from various backgrounds, age group between 20-28 years.
- The gamers played different genres of games with varying expertise and frequency.
- The Game JAM was facilitated by the students themselves and the outcome of the barnstorming reported to everyone at the end of the GameJAM.
Pilot Lesson Plan

• A pilot lesson plan was designed with the following learning objective

• At the end of this session the students are expected to be able to
  – Articulate the various cyber-security terminologies and identify them in a given cyber-security scenario
  – Understand the layers of cyber security and articulate the role each layer plays in designing a holistic cyber-security solution.
  – Identify the types of security attacks.
  – Understand and Appraise the goals of security.
Results

The GameJAM recordings were analyzed and the outcome listed

- **Tower defence Strategy** - is a type of strategy game where the goal is to defend a player's territories or possessions by obstructing enemy attackers, usually achieved by placing defensive structures on or along their path of attack *(Learn by Failing)*

- **Attack-Strategy** – is a type of games focus on gameplay requiring careful and skillful thinking and planning in order to achieve victory. *(Think Like a Hacker)*

- **Puzzle** - require the player to solve logic puzzles or challenges to navigate through complex layers of a game *(Problem-Solving)*

- **Role-playing** - Most of these games cast the player in the role of one or more "adventurers" who specialize in specific skill sets (such as melee combat or casting magic spells) while progressing through a predetermined storyline. *(Student Engagement)*
Future Work

• Workpackage 3: Implementation
  – Student project assistants have been recruited and trained to start building the game and the virtual lab environment

• Workpackage 4: Field Trial Evaluation
  – The content will be field trialed across three Modules each at Level 5, Level 6 and Level 7 to evaluate the CyberGaTE the content and training environment.
Conclusion

• CyberGATE aims at using gamification to enhance students engagement with the CyberSecurity material

• The resources will be delivered using the concept of classroom as a service

• A GameJam has been held to allow the students to brainstorm on possible game scenarios to be used for the gamification

• The gamified resources are under development and will be tested in the coming Autumn
References


