



INITIAL PLAN

Animating security concepts

Lara Ashford
1718561

Supervisor: George Theodorakopoulos
Moderator: Parisa Eslambolchilar
Module Number: CM3203
Module Title: One Semester Individual Project
Credits: 40

Table of Contents

ETHICS	1
1. PROJECT BACKGROUND AND DESCRIPTION	2
1.1 PROJECT BACKGROUND	2
1.2 PROJECT DESCRIPTION	2
2. PROJECT AIMS AND OBJECTIVES	3
2.1 PROJECT AIMS	3
2.2 PROJECT OBJECTIVES	3
3. WORK PLAN	4
3.1 WEEKLY PLAN	4
3.2 GANTT CHART	0
REFERENCES	0

Ethics

As a part of this project, I will be requiring human participation as a part of my testing and evaluation stage and from reading the Computer Science and Informatics Ethics information (Computer Science and Informatics Resource)ⁱ and consulting with my supervisor I believe my project will require ethical approval. Therefore, I will make sure to ensure I have completed the necessary Research Integrity online training programme and complete an ethical approval form with the university at least two weeks in advance of collecting any data from participants as advised by the university.

1. Project Background and Description

1.1 Project Background

Modern society has dramatically changed in a variety of aspects since the developments of technology. From the transformation of how people do their jobs, to developments of phones, the use of IOT devices and driverless cars. Most aspects of life have been, or are being, changed by technology, both positively and negatively. This project endeavours to build on these developments in technology to inspire student learning and education, creating a positive use of technology. Specifically, this project aims to solve one of the negative effects of technology that has been generated, namely a skills gap in cyber security.

Research has shown that 653,000 businesses (48%) have a basic skills gap and 408,000 (30%) have a more advanced skills gap. (GOV.UK, n.d.)ⁱⁱ. This shows the current lack of knowledge in existing staff members but also there is difficulty recruiting people into the field where the most desired roles that are in high demand are security engineers (18%), security analysts (13%), security architects (10%), security managers (9%) and security consultants (8%) (GOV.UK, n.d.)ⁱⁱⁱ.

Fundamentally, knowledge in security is more important today than ever before as more and more of companies and individuals' systems and data are online, creating vulnerability to security attacks. This has resulted in a growing demand for increased awareness and understanding of security concepts and cryptography, as well as getting more people into the industry sector to combat the security vulnerabilities generated through the use of technology. This creates a clear need for more education in security both before people embark on their careers into the working world and to encourage more people to work in security. This can be achieved by making the learning process more enjoyable with the aim of encouraging people to pursue a career in cyber security.

How humans learn and educate themselves has drastically evolved from solely the use of textbooks and libraries to having a wealth of resources online since the creation of the world wide web. Overtime these developments have allowed for higher availability in software, in particular coding languages to create visual learning tools. The use of interactive animations is becoming more prevalent in education, as they are useful in keeping those learning engaged in the learning process and giving immediate feedback about the subject matter being taught. By creating an interactive animation tool user learning can be enhanced and potentially improved in an area that is a priority.

1.2 Project Description

In this project, I will design and develop an educational web-based interactive animation for cryptographic or more general security concepts and processes. This will include, for example, the use of stream ciphers, block ciphers, modes of operation, hash functions or RSA.

This project is important as it will help students to enhance their education through understanding and enhancing their knowledge of security concepts by having interactive elements to the animation. This will enable them to experience the concepts by creating an experience that will promote the enjoyment of learning and stimulating an interest in the subject area. This project will utilise the developments of technology to create this tool for educational purposes therefore addressing the growing need to educate people on both how security concepts work and the need for them discussed in the previous section.

After creation of the web-based animation, I will carry out experiments with users to determine if the animation enhanced their understanding of the concepts, increased their learning enjoyment and if it made them more likely to consider a career in cyber security. This will be compared to answers to the same questions after learning the same content on a control source such as written information, to ascertain if visual and interactive learning has a benefit to education within the realms of cryptographic or security concepts.

2. Project Aims and Objectives

2.1 Project Aims

This project aims to create an interactive educational animation that will actively engage the learner and aid their education of cyber security knowledge.

Aims
<ul style="list-style-type: none">• Expand my technical knowledge on security concepts and encryption methods
<ul style="list-style-type: none">• Understand what enhances a user's learning and understanding of concepts in regard to visual aids and why this improves learning
<ul style="list-style-type: none">• Produce a web-based animation of security concepts for the intended target audience of university students who have a security module or element in their degree.
<ul style="list-style-type: none">• Identify the impact of the users understanding of the subject area before and after using the projects animation to ascertain if it enhanced their understanding
<ul style="list-style-type: none">• Enhance students understanding of the chosen security concept
<ul style="list-style-type: none">• Detail and evaluate my findings in the final document of my individual project

Table 1 - Project aims

2.2 Project Objectives

1. Research
I. Carry out research into different security concepts and encryption methods and decide on which to animate for this educational tool
II. Learn about the benefits of visual learning and what requirements are needed to be satisfied to generate better learning through animations
III. Explore the different programming languages, libraries and platforms are available to create an animation
2. Design
I. Research and determine a design methodology to use and establish if there are any proven design requirements/frameworks of visual tools that have proven to enhance a user's learning experience
II. Design the animation, including the look, how much the user can interact with the animation and the order of events the user will go through using the animation.
3. Implement the animation
I. Create the web-based animation using the chosen design methodology and programming languages
4. Testing
I. Use alpha testing initially and make any changes necessary from failed tests
II. Conduct functionality beta testing (user testing) to determine ease of use of the animation, navigation flow and other functionality conditions.
III. Carry out experiment testing to establish whether the tool enhanced their understanding of the subject area. This could involve giving the user a control piece of knowledge on the subject area and conducting questions and then asking the same questions after they have used the animation, to ascertain if their knowledge improved.
5. Evaluate and document
I. Collate all work and results into a final document
II. Analyse and evaluate the project's findings and determine a conclusion
III. Complete final report

Table 2 - Project Objectives

3. Work Plan

Supervisor meetings

I have arranged with my supervisor to have fortnightly one to one meeting during this time to discuss project progress as well as seek any advice or guidance, in addition a group meeting is also to occur fortnightly, alternating with the individual meetings for the same purpose. This is to allow for any similar project questions and answers to be shared amongst my supervisor's other students.

Project timeline

This individual project is due to take place from the 1st February to the 14th of May, with a 3-week term time break after week 8. This allows for a total of 12 weeks for the project to be carried out and delivered by the 14th of May. I have detailed, beneath, the weekly schedule for this project, including work to be carried out and significant milestones. This process is likely to be iterative in nature rather than linear, therefore I may need to revisit previous tasks in later weeks, for example in the design and implementation stage these weeks are likely to be iterative in nature. Additionally, it is likely I will face some unforeseen challenges that I'm not aware of at this moment in time. Therefore, if these occur, I will adjust my project schedule accordingly and aim to overcome any challenges quickly and effectively to keep the project on schedule.

3.1 Weekly Plan

Week 1: Initial Plan 01/02/2021 – 05/02/2021 (1 Week)

1. Create an initial plan

Milestone: Submit initial plan. **Completed date:** 08/02/2021

Week 2-3: Literature Review/Background Research 08/02/2021 – 19/02/2021 (2 Weeks)

1. Research the benefits of using animations and visual aids for the use of learning. Understand what elements specifically promote better understanding and retention of the subject. Make notes on findings to be later written up in the report.
2. Research different security concepts that would benefit from being taught in the format of an animation. After developing an understanding of a variety of different security concepts, evaluate which one/group would be best to undertake for this project. Possible options include:
 - a. Block cipher with different modes of operation applied such as CBC, EBC, CTR
 - b. Diffie-Hellman Key Exchange
 - c. Hash functions
 - d. RSA cryptosystem

After taking time to research different options I will discuss my findings with my supervisor and decide which is best for this project.

3. I will investigate the different available programming libraries and platforms that are available to code an interactive animation tool and choose what I will use. From an early discussion with my supervisor, we have discussed using JavaScript for the majority of the code of this project, therefore I will look into whether to use this or if there is a better alternative.

Week 4: Design Stage 22/02/2021 – 26/02/2021 (1 Week)

1. I will first research different design methodologies and evaluate which will be best to use for this project
2. I will then investigate if there are any design principles/requirements that are standard practice to follow, especially for the purposes of enhancing someone's learning.
3. From the two stages above I will use these to then create design templates of the front end of this interactive animation.
4. Additionally, I will create UML/class diagrams showing how the core functionality of the code will work.

Milestone: 1st Review meeting with supervisor. Presenting all my intentions for the animation and taking into consideration any feedback before moving onto the implementation stage.

Week 5-8: Implementation 01/03/2021 – 26/03/2021 (4 weeks)

1. Firstly, I will begin coding the core functionality of the chosen security concept, for example getting an encryption algorithm to successfully encrypt and decrypt a given message
2. After I have the core fundamentals of my code working, I will move onto creating the front end of the application. The application will be editable, for example changing initialisation vector or by changing the mode of operation
3. In week 7 I will then turn my attention to creating and coding all the design and styling elements to fulfil the design methodology and requirements discussed in week 4 above.
4. Lastly In week 8 I plan to use this week to finish off any remaining coding elements that may remain due to challenges or over running and then complete alpha testing. This will entail myself testing the system to ensure its core functionality are being adhered to and working successfully.

Milestone: 2nd Review meeting with supervisor. Showing my finished animation and getting feedback. If any significant changes are needed after this meeting, I will use the easter break as an opportunity to rectify these.

Easter Recess

1. There is a three-week easter recess which I have not planned to do any work in as the university recommends having a break. I am very aware it is possible for projects to overrun due to unforeseen problems, especially in the coding stage. Therefore, if the implementation stage takes longer than expected I will use this easter period to finish the implementation of the animation in order for week 9's work to go ahead on time.

Week 9 Evaluation: 19/04/2021 – 23/04/2021 (1 Week)

1. In this week I will conduct beta testing (with users). I intend to have university students use the animation created and give feedback on its ease of use and functionality.
2. In addition, I will be carrying out experimental testing to establish whether the tool enhanced the users understanding of the subject area. This could involve giving the user a control document of information on the subject area and conducting questions and then asking the same questions after they have used the animation, to ascertain if their knowledge improved.
3. Then I will summarise my findings into both numerical statistics and charts to use in the final report as a way of showing my findings.

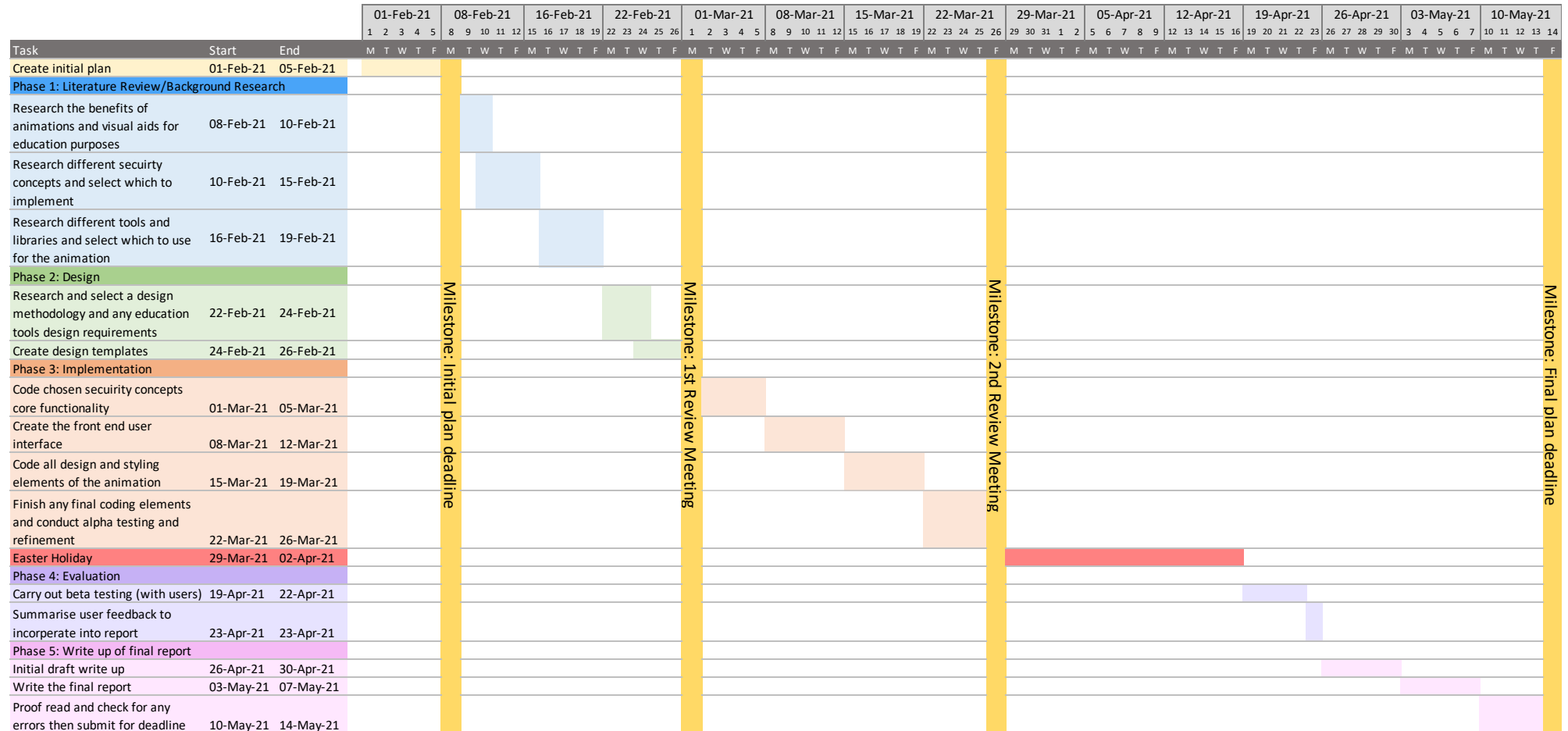
Week 10-12 Write up of final report: 26/04/2021 – 14/05/2021 (3 weeks)

1. Week 10 will be used to write a complete draft report, collating all the research notes on background of the problem and designing, implementation and results stages listed above. Each of which will be written in brief as each stage of the project is carried out.
2. Week 11 will be used to rewrite this report into a final polished document
3. Week 12 will be for final proofreads, checking for errors and making any necessary changes before submission.

Milestone: Submit final report. **Completed date:** 14/05/2021

3.2 Gantt chart

Below is a Gantt chart which shows the project schedule, highlighting the key milestones as well as the week-by-week schedule for all the tasks discussed above.



References

ⁱ Computer Science and Informatics Resource. [online] Available at: <https://www.cs.cf.ac.uk/ethics/> [Accessed 4 Feb. 2021].

ⁱⁱ GOV.UK. Cyber security skills in the UK labour market 2020. [online] Available at: <https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2020/cyber-security-skills-in-the-uk-labour-market-2020?fbclid=IwAR0mAdta1NZtAfjFaGUCWcQQsqjNY58ZTfATOSAXC65aG5Y6d2FTVOpPbSQ>

ⁱⁱⁱ GOV.UK. Cyber security skills in the UK labour market 2020. [online] Available at: <https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2020/cyber-security-skills-in-the-uk-labour-market-2020?fbclid=IwAR0mAdta1NZtAfjFaGUCWcQQsqjNY58ZTfATOSAXC65aG5Y6d2FTVOpPbSQ>