Assignment 2: Cybersecurity Essay

Version 1.0
Creative Computing
COMP280

Gareth Lewis

Introduction

In this assignment, you are required to write a report on cybersecurity related issues for a GaaS (games as a service) provider that is looking to launch a new service and is concerned with potential issues relating to hacking, phishing, data security and compliance to the GDPR regulations.

To help with cybersecurity research for writing your report, you will work collaboratively to build a collection of cybersecurity knowledge, as a wiki, that you can all use to provide suitable and appropriate evidence for writing on cybersecurity.

'There are two types of companies: those that have been hacked and those that will be'

-Robert Mueller, FBI Director 2012

'Yesterday, I changed my WiFi name to 'hack if you can'. When I checked it today, it was 'challenge accepted'

-anonymous

XYZ Online Games Cybersecurity report

This is a report from another consultant's visit to XYZ games. She spent a day with the company having an office tour and interviewing people from each department and the company's CEO.

XYZ Online is a relatively new game developer looking to soft launch its exciting new game service 'Trankcraft: Plains of Destruction', an MMO drawing heavily from World of Tanks. Currently, the game will launch on PC with support for mobile and web services to allow players to keep up to date with their tank clans and battle ladders.

The company is organised into four functional areas: development, operations, sales & marketing and customer service, with each area running vertical teams with an overall management team overseeing business operations made up of the heads of each area and the CEO and CFO of the company.

The development team is responsible for on-going game development and consists of a small development team that works in the basement of the company office and is supplemented with remote contractors. All development is managed through Trello and git, with a remote git service through github.com. Typically, development is undertaken on a main branch, tested locally and then pushed to the operations team. Development back-ups are 'managed through git' according to the lead developer.

The operations team is responsible for keeping the game service running. Currently, the game service is hosted on several blade servers in the company office that the company acquired in a liquidation sale from another SaaS company. The servers have no service-level agreements in place, their OS is tied to the original purchaser and there appeared to be little operational redundancy. The operations team share the same git service as the developers, allowing developers to easily 'live patch' issues in the service as they are found.

The sales & marketing team is responsible for bringing customers to the game

and keeping them playing (and paying for) it. Much of the team's work is done through data mining the game's database to up-sell and cross-sell in-game items to players through targeted emailing using player sign-up details.
The team cite that a big advantage of having just one database in the company allows easy access of data for all. Typically, the person responsible for data mining will 'pull' customer details from the database onto a usb stick to run pivot table enquires in Excel, though he has lost several sticks during communing to and from work. This is not regarded as an issue as 'no-one would know what to do with our data'.

The customer service team is responsible for dealing with customer issues, typically issues with login details, credit card and payment issues and issues with in-game purchases, either purchases not going through or requests for refunds. Much of the customer service team's work is centred around updating the game database, given the employee churn in customer service, there is one account that all customer service employees use to update the database and this is used for all customer transactions (password changes, payment details, game data reversals and so on).

When interviewed, the CEO stated that the goal of the company was to 'travel light and break stuff to get things done and make a great game' and stated that they didn't really have time to waste putting pointless processes in place that would just slow them down.

Like the blade servers, much of the company's hardware has been acquired second hand resulting in a wide range of equipment, OS and application versions. The CEO says it's a good thing that the company is using 'all the windows from 7 to 10' as it gives them a lot of scope to do compatibility testing of the game without using an external company and wasting money. Currently, the company has no explicit IT department with programmers from the development and operations filling the roles on an ad hoc basis.

The report required for this assignment consists of the following components:

(A) A section that highlights key potential cybersecurity issues for the company

(B) A discussion on how control strategies can mitigate the issues raised in (A)

(C) A section that outlines major potential GDPR issues for the company based on their current operations.

(D) A section containing a code demonstration comparing the Caesar and XOR ciphers against modern AES standard cryptography as found in Python libraries like `cryptodome`, `fernet` and others, demonstrating why AES is a better approach to cryptograph.

https://www.geeksforgeeks.org/caesar-cipher-in-cryptography/

https://www.geeksforgeeks.org/xor-cipher/

The report should be around 1500 words [+/-10%] with a fairly equal weighting to sections A, B & C. Section D should contain a python project.

To help collect and collate a central knowledge base of cybersecurity issues, you will collaboratively build and use a git-based wiki 'cybersecurity body of knowledge'.

Assignment Setup

This assignment is a combination of data collection and advocacy, reporting writing and programming tasks.

For the data collection and advocacy part, you will use the repository that has been setup on git:

https://github.com/Falmouth-Games-Academy/comp280-cyberworkshop.git

For the report writing part, you are free to use any work processing software you are comfortable using (Word, Google Docs, Latex etc) and any referencing style (IEEE or Falmouth-Harvard) though ensure that you keep to one style of referencing throughout the report

For the programming task, create a project in Python that contains working code samples.

Part A

Part A consists of collaboratively building the group 'cybersecurity body of knowledge'.

To complete Part A:

(A) As a team, divide out the articles between yourselves. They are generally grey literature, so won't be as long or as demanding a read as typical academic papers. You should all have around 4 or 5 articles to read and write notes on.
(B) Read each article and make notes using 5Ws&H and 3As
(C) Upload your articles onto the website
(D) Once you have all read your papers, determine how the articles cluster. There should be some obvious groups around data breaches, state-sponsored cyber terrorism and hacktivism, white hatting and security.
(E) Split your team into subgroups to write a page for each group that will serve as an introduction to the topic and highlight key issues, outcomes and findings.

You will receive **informal feedback** from your **tutor** during the workshop sessions in weeks 2 & 3.

Part B

Part B consists of a **single formative submission**. This work is **individual** and will be assessed on a **criterion** basis.
To complete Part B, write the report using a word processing package of your choice, preferably creating output as a pdf file. For the programming work, use PyCharm and make sure to include the AES encryption libraries, and any other libraries you use, as part of the project. Zip the report and the PyCharm project together and then upload the zip to Learning Space.

You will receive **formal feedback** from your **tutor** within three weeks

Additional Guidance

On the surface, the wiki generation task sounds like a lot of work, but many hands will make light work. As a team, you will need to divide out the work between all of you and then collect your impressions on the papers to work out how they cluster.

The 5Ws&H approach is often referred to as the 'hack's method' as it is commonly cited by journalists to address the who, where, why, what when and how of stories. As each of your articles is a story about cybersecurity there should be those aspects. Again, you can look for interesting groupings; what kind of people and organisations are involved in these cyber articles? Are there any commonalities in what and how things are being done and so on?

The 3As is a similar approach that comes from UML modelling, in particular use-case collaborations. The three As describe the actors, activities and artefacts in a system and you can use this to think about who is involved in cyber article, what is being done (the activities) and what it's being done to (the artefacts).

Both the 5Ws and 3As give you fairly simply frameworks that you can employ to compartmentalise complex situations in order to improve your understanding.

To write up your articles, make sure everyone contributes to the process. I will use a tool to assess your contributions for marking this worksheet so don't leave all the writing to one or two scribes. It's a group writing activity and you will all benefit greatly from the body of knowledge you have created once you turn your attentions to the essay writing part of the assignment.

For many companies, particularly games companies, the challenge of just making and launching a product can become a completely encompassing task with process and long termism slipping under the radar as activities that can just be 'done later'. From our studies in cybersecurity, our 'later' may not fit into a hacker timeline of later allowing hackers to break into systems will the system's owner is concerned with other 'more pressing' activities.

Business reports often reveal as much about a business by what is not said rather than what is said. In this case, it is worth thinking about what has been written concerning issues like control and control strategies, OWASP, GDPR and penetration testing. By thinking about what is missing from the report, you should have a large choice of issues to consider, the challenge is in deciding which ones are the most important for the company.

To address the programming part of the assignment, you will need to write working versions of both naïve and AES cryptography. To perform well at this part of the assignment, you will need to refer to the rubric relating to *comments* and *testing*. Therefore, be sure to layout and comment your code so that its functionality makes sense and be sure to include some form of testing that will show both normal operation and edge cases for the algorithms & approaches you are considering.

FAQ

What is the deadline for this assignment?

Falmouth University policy states that deadlines must only be specified on the MyFalmouth system.

What should I do to seek help?

You can email your tutor for informal clarifications. For informal feedback, make a pull request on GitHub.

Marking Rubric

Learning Outcome Name	Learning Outcome Description	Criteria	Weight	Refer for Resubmission	Adequate	Competent	Very Good	Excellent	Outstanding
Basic Competency Threshold			30%	At least one part is missing or inadequate	The student demonstrates an adequate ability to generate ideas, problem solving, concepts, technical competency and proposals in response to set briefs and/or self-initiated activity. The student's work demonstrates an adequate, ethically informed, real-world experience of industry/business environments and markets. Adequate participation in cybersecurity body of knowledge No breaches of academic integrity				
Code / Process	Implement working and maintainable software components.	Naïve crypto	10%	Samples do not function correctly Code is poorly laid out with few, if any comments No evidence of testing	Samples function sporadically Code is poorly laid out with few, if any comments Some evidence of testing	Samples function with few issues Code laid out is acceptable, comments are somewhat ad hoc and meaningless Some evidence of testing	Samples function correctly Code is generally well laid out and comments are fairly meaningful Some evidence of testing framework	Samples function correctly Code is well laid out and suitably commented Clear evidence of testing framework	Samples function correctly Code is well laid out and suitably commented Significant testing evident
		AES crypto	10%	No evidence of 3rd party AES framework Samples do not function correctly Code is poorly laid out with few, if any comments No evidence of testing	Submission uses 3rd party AES framework Samples function sporadically Code is poorly laid out with few, if any comments Some evidence of testing	Submission uses 3rd party AES framework Samples function with few issues Code laid out is acceptable, comments are somewhat ad hoc and meaningless Some evidence of testing	Submission uses 3rd party AES framework Samples function correctly Code is generally well laid out and comments are fairly meaningful Some evidence of testing framework	Submission uses 3rd party AES framework Samples function correctly Code is well laid out and suitably commented Clear evidence of testing framework	Submission uses multiple 3rd party AES frameworks and compares performance and functionality Samples function correctly Code is well laid out and suitably commented Significant testing evident
Advocate / Industry	Analyse the legal, social, ethical, and professional issues that affect creative projects, with a focus on the role of professional bodies.	Highlighting cyber security issues	15%	few or superficial considerations given	3-6 issues presented Lack of depth / insight / coherence Over-concerned with one or two business functions	3-6 issues presented Reasonable depth / insight / coherence Covers all areas, but not equally	3-6 issues presented Good of depth / insight / coherence Fairly equal coverage across business areas	3-6 issues presented Good coverage with some insight between business areas Fairly equal coverage across business areas	3-6 issues presented Good coverage with significant insight between business areas Fairly equal coverage across business areas
		Control & Control Strategies	15%	few or superficial considerations given	3-6 issues presented Lack of depth / insight / coherence Over-concerned with one or two business functions	3-6 issues presented Reasonable depth / insight / coherence Covers all areas, but not equally	3-6 issues presented Good of depth / insight / coherence Fairly equal coverage across business areas	3-6 issues presented Good coverage with some insight between business areas Fairly equal coverage across business areas	3-6 issues presented Good coverage with significant insight between business areas Fairly equal coverage across business areas

		GDPR considerations	15%	few or superficial considerations given	Lack of depth / insight / coherence Concerned with a single GDPR consideration	Reasonable depth / insight / coherence Concerned with several GDPR considerations	Good of depth / insight / coherence Concerned with most relevant GDPR considerations	Good coverage with some insight between business areas Concerned with most relevant GDPR considerations	Good coverage with significant insight between business areas Concerned with key GDPR considerations
		Quality of Presentation & writing	5%	Report is wall of text with little or no formatting No referencing Significant spell-checking / grammar issues No consideration of diagramming	Report has minimal formatting Some references, not necessarily following reference guides Some spelling / grammar issues Some use of diagramming	Report is reasonably well formatted Referencing generally follows guides but few references Occasional spelling / grammar issues Some relevant use of diagramming	Report is well formatted Referencing (quality & quantity) generally good Very Occasional spelling / grammar issues Good use of diagramming	Report is well formatted Referencing (quality & quantity) is very good No obvious spelling / grammar issues Very good use of diagramming	Report is well formatted Referencing (quality & quantity) is very good No obvious spelling / grammar issues Excellent use of diagramming