COMP61421 Coursework I – Risk Management

1 Introduction

The assignment has two main parts. The first is based on a case study and guides you towards creating an assured risk treatment plan. The second is based on the guest lectures and elicits your reflections on various aspects of real-world cyber-security.

The assignment is marked as follows:

- 5 points - asset register
- 5 points - attack tree
- 5 points - risk treatment
- 2 points - test plan
- 8 points - reflections (2 per lecture)

Details on requirements for successful completion follow below.

2 Case study – SPYONU

Sections 2.1 and 2.2 present the case study from the customer and vendor side respectively. Note that we are tasked with protecting our customer, whereas the vendor is solely interested in selling their software product. As such, the specification below may sometimes be quite vague.

Always remember that you have the authority to make architectural, technical, and organisation assumptions and decisions. Indeed, software specifications often are full of holes well into the development cycle. This creates the opportunity for you to fill in the blanks with some critical thinking and design in security to the architecture.

See Section 2.3 for the assignment questions.

2.1 Scenario from the customer side

Redfriars School has 300 pupils and 50 staff. Staff include – but are not limited to – administration, building maintenance, catering, a school nurse, and (of course) teachers. Some of the teachers also provide careers advice and social counselling to the pupils. Some have supervisory roles for their subject matter and carry the title, 'Head of subject. The Head Teacher is concerned with the tactical, day-to-day running of the school. The school is managed by a panel comprising three governors, (including a parent governor), a bursar (managing the accounts) and the head teacher who set school policy and strategies to realise those policies.

The school has agreed with AI-City Software Limited, a 'disruptive technology provider', to be an early adopter for a new educational tool that will support teachers, parents, and students to make the most of the learning environment. This tool is called the Student Personal Year Organiser and Notification Unit (or SPYONU for short).

SPYONU has an artificial intelligence core that

- Predicts grades and the path to improve them.
- Detects mood swings that may indicate a student is troubled and needs additional support
- and collates data about the students, teachers, and school management to produce guiding reports for the head-teacher to steer the school in the opposite direction from the dreaded special measures that can be imposed by the Department for Education.

SPYONU looks at what is going on at the school in question, other schools, and the jobs market. It learns from social media and other contemporary sources to direct students to the careers that suit their talents and both students and teachers to the curriculum and support their students need.

Information is collected, processed, and stored about each pupil including attendance records, additional needs including dietary requirements, parent or guardian contact details, marks from school work and examinations, and membership of extra-curricular clubs, behavioural and disciplinary records, and financial records about the payment of school dinners and school trips. SPYONU collates students' data and correlates it with teachers' performance to create Personal Educator Development Review and Plan (PEDRP) for the teachers, administrative staff, and by upwards analysis of those reports too, produces a Personal Head Teacher Development Plan (PHTDP) for the Head Teacher.

The school has an exemplary record in compliance with contemporary data protection principles. Refriars is ever cautious of its responsibilities to safeguard the staff, students, and the families associated with the school. It is because of this dedication that they have asked groups from the MSc in Advanced Computer Science (ACS) at the University of Manchester to carry out a risk assessment and prepare a risk treatment plan for SPYONU to assure that it can cope with historical, contemporary, and emerging threats from the cyber risk landscape.

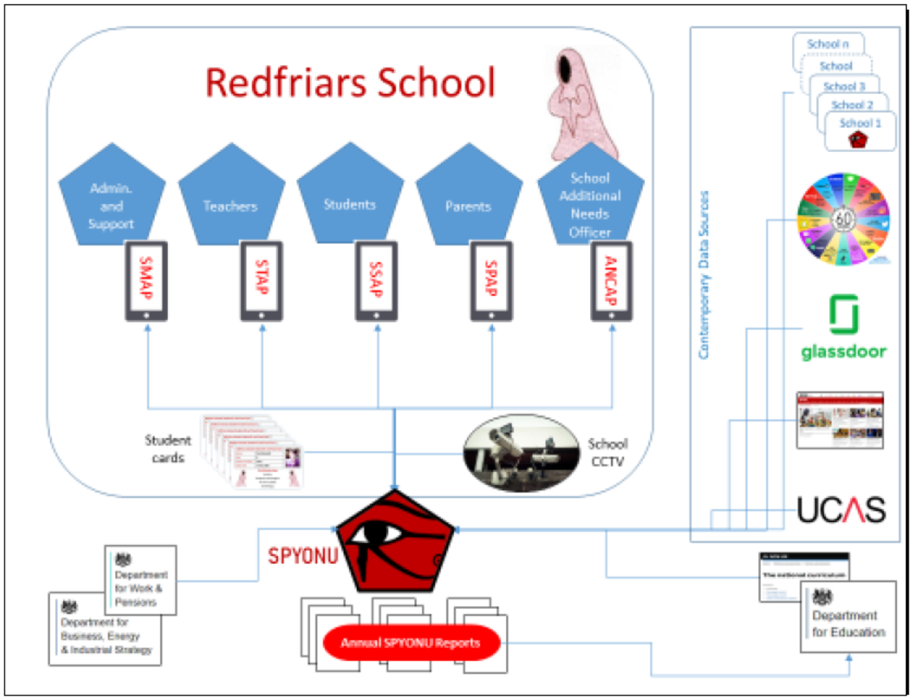

Figure 1: Student Personal Year Organiser and Notification Unit (SPYONU)

2.2 Technical details from the vendor side (see Fig. 1)

Student Personal Year Organiser and Notification Unit (SPYONU) is – according to the brochure – 'the very latest in machine learning and advanced artificial intelligence'. SPYONU collects schooling data from SPYONU schools and cross-references it with multiple interactive contemporary data sources across the world (See Figure 1). SPYONU benchmarks the progress of the school and individual pupils to provide Personal Study Plans (PSP) and Well-being Life Exercises (WBLE) that are 'tailored to an individual student's educational and socio-psychological needs'. These plans set out what to learn and how to learn it (books, videos, practical experience, and so on) and tracks the student's progress, adjusting the plans and exercises according.

SPYONU also monitors teacher's performance with respect to the students and prepares Personal Educator Development Review and Plan (PEDRP) for each teacher which are collated and fed into a the Personal Head Teacher Development Plan (PHTDP) for the Head Teacher and the School Management and Improvement Plan (SMIP) for the school overall.

The SPYONU family of applications comprises:

- SPYONU Students' App – SSAP – including:
  - Assessments, examination, and test results

  - Dinner money and school clubs and outing finances
  - Internal school messaging
  - Personal attendance tracking
  - School reports
  - School rules and behaviour guidance.
  - Timetables

- SPYONU Parents' App – SPAP– including:
  - Assessments, examination, and test results
  - Dinner money and school clubs and outing finances
  - Internal school messaging
  - Parent, carer and multi-agency interaction
  - School reports
  - School rules and behaviour guidance.
  - Student attendance tracking
  - Timetables

- SPYONU Additional Needs Coordination App – ANCAP – including:
  - Additional needs care planning
  - Assessments, examination, and test results
  - Dinner money and school clubs and outing finances
  - Internal school messaging
  - Parent, carer and multi-agency interaction
  - School reports
  - School rules and behaviour guidance.
  - Student attendance tracking
  - Timetables

- SPYONU Teachers' App – STAP – including:
  - Assessments, examination, and test – setting and results
  - Extracurricular activity planning and reporting
  - Internal school messaging
  - Lesson planning
  - Parent, carer and multi-agency interaction
  - Personal Educator Development Review and Plan (PEDRP) or Personal Head Teacher Development Plan (PHTDP) as applicable to the role

  - School report writing
  - School rules and behaviour guidance.
  - Student attendance tracking
  - Timetables

- SPYONU School Management App – SMAP
  - Additional needs care plans for the school
  - Audit and compliance schedules and actions arising
  - Assessments, examination, and test – setting and results schedule
  - Assessments, examination, and test results
  - Dinner money and school clubs and outing finances
  - Extracurricular activity planning and reporting
  - Internal school messaging
  - Parent, carer and multi-agency interaction
  - School report writing management
  - School rules and behaviour guidance
  - Student attendance tracking
  - Timetables

SPYONU also connects teachers, parents, and children together to notify and manage absences ('no more taking in a note into school'), seeing who has what homework to do and when it has to be handed in (and whether it was hand in on time), distributing marks, school reports, logging detentions, paying dinner money and registering for school trips.

Each application feeds live data back to AI-City Software Limited to enhance the real time accuracy of Personal Study Plans (PSP) for students, Well-being Life Exercises (WBLE) for students and their families, and the Personal Educator Development Reviews (PEDR) for teachers.

Data from the above tracking and correlation is used – in conjunction with worldwide sources listed below to prepare (amongst other items mentioned herein):

- Personal Study Plans (PSP) – These contain detailed learning programmes for the students across the school that's subscribed to SPYONU. Each one is specifically created for each student respectively and connected to complementary resources and discounted study materials.

- Well-being Life Exercises (WBLE) – These exercises are calibrated against student moods, like, and dislike to maximise the participation of the respective students

- School Management and Reporting Tool (SMART)[1]
    - Attendance data
    - Behaviour monitoring
    - Data protection information
    - Data Reporting
    - Finance
    - Messaging
    - Mobile access
    - Parent and carer interaction
    - Safeguarding
    - School report writer?
    - Security
    - Support
    - Statutory reporting?
    - Timetables

SPYONU tracks the books purchased by thousands of parents and students and correlates the data with the examination results of students from those families to advise which publications will lead to the best results.

SPYONU follows the Facebook, Instagram, Twitter, YouTube, WeChat, TikTok, Reddit, and similar social network accounts of tens of thousands of young people and correlates the language used by them with sporting achievements, crime reports, and suicides recorded in national and local press to determine which young people might be at risk of harm and alerts officers from the local Multi Agency Safeguarding Hub (MASH).

SPYONU will also ‘scan events and programmes and collate these with information about the attendance records of tens of thousands of students to predict student absences and notify teachers in time for these to be avoided’! Unpreventable ones are reported to the school kitchens to cancel meals and reduce food waste.

2.3 Case study questions (17 points)

Get familiar with the case study above. Specifically, consider how the operational processes will work by looking at the components in the illustration. Then, consider what information assets need protecting. For each asset, ask yourself whether it is transitional or permanent (e.g. temporary files versus a central database), whether it is critical to any of the stakeholders (e.g. financial data), and whether it is legal or falls outside of permitted boundaries (e.g. encourages users to take illegal/non-secure shortcuts).

Then, produce the following:

[1] Designed to comply with the best fit to https://www.gov.uk/government/publications/choosing-a-school-management-information-system-mis

- **Asset Register (5 points)** Catalogue the assets to create an Information Asset Register. Value each asset in terms of confidentiality, integrity, and availability. Use the template shown in class.

- **Attack Tree (5 points)** Identify the threats to the students' personal data throughout the system lifecycle. Create an attack tree for these assets. Use multiple trees if you think there are independent root nodes.

- **Risk Treatment (5 points)** Assess the likelihood of each threat in your tree(s). Propose countermeasures for them. Explicitly state which ones are necessary for business continuity (i.e. the ones that make the system resilient).

- **Test Plan (2 points)** Outline a test plan to assure the effectiveness of your risk treatments (around 100-200 words). Hint: this module has a significant penetration testing component and you might like consider where this fits with red, blue, and purple teaming, vulnerability scanning, and audits although not necessarily in that order.

3 Reflections on guest lectures (8 points)

This is the second part of your assignment: your reflections on what you learnt from the guest lecturers. Reflections are not a detailed summary of the content. Instead, they should contain only the elements that you found particularly noteworthy.

More practically, write one paragraph (around 100-200 words) for each lecture. Focus on content that subverted your expectations, contradicted your prior knowledge on the topic, or surprised you in some interesting way. Alternatively, reflect on how the guest lectures would apply to the case study in this assignment (see Section 2).

Overall, aim to provide more personal answers than AI-generated ones!

Guest	Date	Topic	Points
Paul Vlissidis	7/11 12pm	Red Pill or Blue Pill? (or how to make red teaming useful)	2 points
Avi Shaked	7/11 @ 2pm	Integrating Security into System Design: An Ontology-Driven, Conceptual Modelling Approach	2 points
Jon Noel	14/11 @ 11am	Evolution of Malware	2 points
Ian Thornton-Trump	14/11 @ 2pm	Infosec Management: When You Think You Need a Lawyer. You Probably Do Need a Lawyer	2 points

Note dates and times are subject to change. Listen keenly for alterations to the schedule.

4 Submission instructions

Submit your whole assignment, from asset register to lecture reflections, as a single Adobe PDF file. Make sure your name and student ID is clearly visible on the first page of the file. Failure to do so may result in a mark of 0 for the assignment.

Please include your name clearly in your filenames. For example:

- PaulMetcalfeSecurityReport.pdf
- LiSeng001.pdf
- 06_AliceAdabeo.pdf

Up to 10% of the marks can be forfeit if you don't follow these labelling instructions – they're part of the exercise.