Assessment cover

**STUDENTS, PLEASE COPY THIS PAGE AND USE AS THE COVER PAGE FOR YOUR SUBMISSION**

|  |  |  |  |
| --- | --- | --- | --- |
| Module No: | **COMP5020** | Module title: | **Foundations of Security** |

**Coursework**

Assessment title :

**01/03/2024 14:00**

Due date and time**:**

40 hours per student

Estimated total time to be spent on assignment:

# LEARNING OUTCOMES

|  |
| --- |
| **On successful completion of this module, students will be able to achieve the module following learning outcomes (LOs):** *LO numbers and text copied and pasted from the module descriptor* |
| * Demonstrate a thorough understanding of the fundamentals of computer and information security, and design. |
| * Demonstrate and apply a thorough understanding of the fundamentals of computer and information security in terms of threats and attacks, secure coding theory, cryptography, and security analysis. |
| * Evaluate the security of existing software and systems architecture and produce a report on the   analysis of them for both technical and non-technical readerships. |
| * Identify and utilise trustworthy information sources and evaluate the trustworthiness of unrated sources. |
| * Apply self-awareness in evaluating their impact in team-based work and utilise appropriate communication and problem resolution strategies. |

|  |  |
| --- | --- |
| **Engineering Council AHEP4 LOs assessed (from S1 2022-23)**  *LOs copied and pasted from the AHEP4 matrix* | |
|  |  |
|  |  |
|  |  |
|  |  |

**STUDENT NAMES (ONLY IF GROUP ASSIGNMENT, OTHERWISE ANONYMOUS)**

|  |  |  |
| --- | --- | --- |
| **Student No:** | **Student Name:** | **Group Name and Number:** |
| **1.** | Penri Jones | 19238681 |

**Statement of Compliance *(please tick to sign)***

Y

I declare that the work submitted is my own and that the work I submit is fully in accordance with the University regulations regarding assessments

*(*[*www.brookes.ac.uk/uniregulations/current*](http://www.brookes.ac.uk/uniregulations/current)*)*

**Github Repo:** https://github.com/19238681/COMP5020resit

**Abstract:**

This document presents my background research, as well as the proposed system for the Passport Office business. In this document, I consider the threats and vulnerabilities of the system, as well as proposing alternate methods to secure and protect the service from threats. I will then detail a threat and risk analysis, using multiple methods, including SD3, STRIDE, a Risk Severity Matrix and DREAD. Finally, a secure design specification will be included, in order to further patch possible vulnerabilities that may be present within the system.

The passport office is an institution that is inextricably linked with the systems of our government. Their role is to gather information about people, whether that be provided by the customer, or information gathered through other governmental departments. They then analyse this information, determining if it is both accurate and also meets the requirements for a valid passport. If so, they are in charge of printing and issuing said passport to the customer in question, and securely storing all the information for future use and verification purposes.

They hold many different types of data, most of which are counted as personal identifiable information (PII). Some of this data is considered ‘sensitive PII’, such as biometric information (photo ID, fingerprints, iris scan, facial recognition data) or information regarding racial origin or ethnicity. *(European Commission, no date)*

According to background research, to process said sensitive information, the organisation is required to have “Reasons of substantial public interest (with a basis in law)”. An example of a substantial public interest reason would be for any “Statutory and government purposes”, for which the passport office would apply. *(Information Commissioner’s Office, no date)*

While the other types of data are still PII, they are not sensitive, and the processing and security requirements are somewhat lessened, although strict privacy rights must still be enforced. Other types of data include but are not limited to: Full name, address, gender, date of birth, place of birth, contact details, payment information, documentary data (such as supporting documents like a driver’s license) and application history (regarding previous passport applications).

While it is unknown the exact processes and protocols that the Passport Office maintains, due to secrecy and privacy reasons (not to mention proprietary technologies), we can make some educated and accurate assumptions as to what types of systems would be required.

Firstly, our proposed service would require a Database Management System (DMS) to store all the data discussed above. Due to the size, but also privacy and security concerns, access to such a system would need to be privileged and highly vetted. A DMS system like this would also heighten CIA concerns (Confidentiality, Data Integrity and Availability) – as efficient addressing would allow for high-rate availability, while the principle of service separation and elevated privilege levelled access requirement would maintain Confidentiality. In addition, our proposed DMS system would require several backups, both due to its large size, but also the importance of the data stored therein. These backups would be both online and offline, cloud and local. Based on the UK Passport Office’s own numbers, they issue around 6 million passports per year, while servicing over that amount of passport validation service requests. *(Home Office, 2022)* As such, it would be prudent to have the system backup modifications to the files daily, with additional complete backups taken at various times. This would ensure Data Integrity, as any lost or corrupted data could be retrieved from one of the several backups available.

Our proposed system would require a way of intaking, processing and generating payment information, to interface with banks, generate invoices and receipts, and process payments for the services rendered.

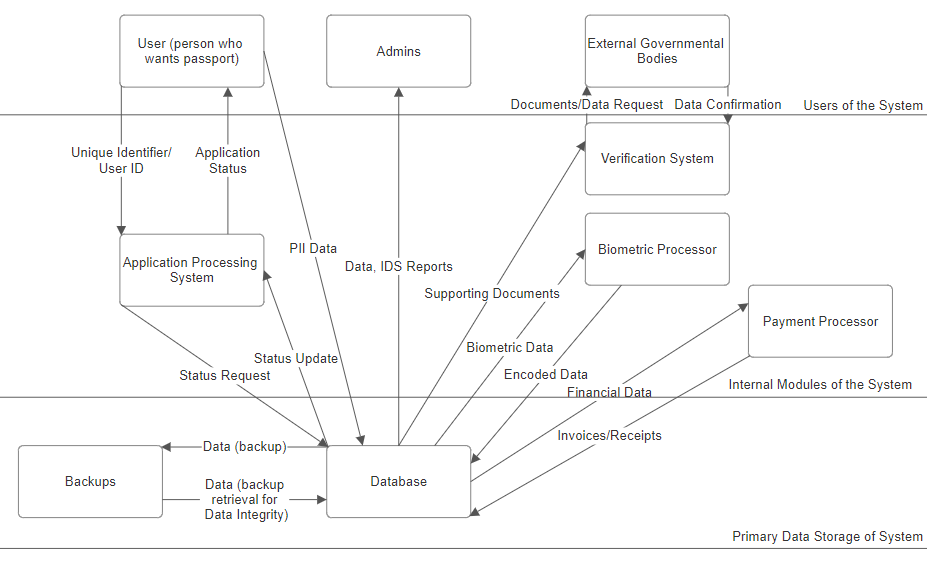
We would require Biometric data systems, for the generation and confirmation of biometric information, such as iris scans, fingerprint, and facial recognition data. Given the updated biometric passports provided in the UK since 2010 *(Post Office, 2024)*, this information needs to be accessible in order to be applied to the requisite passports.

A front-end passport application processing system would be needed, in order to track, verify and process the status of applications throughout the entire work-process. In addition, audit and logging systems would be essential, in order to provide Repudiation should something go awry.

Finally, a verification system would be required, in order to verify authenticity of supporting documents (such as driver’s licenses and birth certificates). Based on information provided by the Passport Office, they “may also pass the information you give us to UK law enforcement agencies or government departments involved in preventing fraud to help prevent or detect identity theft, fraud or other criminal activity.” *(HM Passport Office, 09/22).* It would be this system that is capable of sending automated requests to other governmental bodies, in order to verify the authenticity of the provided information, and gather other sensitive PII. This system would require an Optical Character Recognition system (OCR’s) in order to automate the process, and detect issues with the provided documents.

**Threat Analysis:**

I have decomposed my proposed system in a data flow diagram in order to better determine all possible avenues of attack.



|  |  |
| --- | --- |
| Item | Software |
| Title | Spoofing User Identity |
| Application | Software/Web Protocol |
| Threat Target | Server |
| Threat Type(s) | Spoofing Identity |
| Risk | **Damage:** The user’s private and personal information could be gathered without their knowledge or consent (from the Application Processing System). That being said, this method would only provide a singular person’s PII at once, which while something that must be prevented, wouldn’t grant access to the entire system. **(6)**  **Reproducibility:** To reproduce this event, the hacker would either need to brute force the password of the user, or instead use a man-in the middle attack. Both options would need to be repeated for each individual user, and as such, isn’t that repeatable **(3)**  **Exploitability:** Either a pre-existing user-side vulnerability would be required, or a lot of time and already gathered personal knowledge would be needed **(5)**  **Affected Users:** Only the current user would be affected, although theoretically, with enough time, this could be repeated on all users **(1)**  **Discoverability:** It would be difficult to discover, especially due to requiring knowledge of the safety measures put in place to counteract this very action **(5)** |
| Total Risk Rating | **4** |
| Mitigation techniques/Secure Design Recommendations | Have restrictions on the amount of attempts in a timeframe, with additional verification required upon reaching said amount.  Have a strong password and data encryption protocol, with strong password length and difficulty requirements |

|  |  |
| --- | --- |
| Item | Hardware |
| Title | Hackers gain physical access to database servers |
| Application | Database |
| Threat Target | Servers |
| Threat Type(s) | Tampering with data |
| Risk | **Damage Potential:** could lead to the entire server (all data not stored in a backup) being corrupted, tampered with, altered or deleted **(10)**  **Reproducibility:** would be near impossible to reproduce, since not only would you need to sneak into a governmental building, but also, do it after security has already been heightened by a previous attempt **(1)**  **Exploitability:** To succeed, you would require not only knowledge of specific governmental building layouts, you would need access codes, as well as some form of social engineering **(2)**  **Affected Users:** Would affect all the users, data tampered with could be restored from a backup, but PII would have been accessed and possible stolen **(10)**  **Discoverability:** This vulnerability is present in every system. No matter how secure the software and hardware are, the people maintaining it are always present and vulnerable. That being said, the amount of knowledge and resources (as previously stated) is quite enormous **(2)** |
| Total Risk Rating | **5** |
| Mitigation techniques/Secure Design Recommendations | Have a security system present, not only in the building, but also separately preventing access to the server rooms.  Use SD3 – Secure by Default by using the principle of least privilege by allowing only a few people to have access to the server room, but also Secure in Deployment by educating employees about social engineering, and training them to report suspicious activity and the like. |

|  |  |
| --- | --- |
| Item | Network |
| Title | Shut down the online service |
| Application | Wireless Connection |
| Threat Target | Server (Application Processing) |
| Threat Type(s) | Denial of service |
| Risk | **Damage Potential:** It would prevent users from submitting, checking on the progress of, or receiving updates on their passport application process. It would not reveal private information, nor cause it to be lost – only a temporary ceasing in productivity, which could cause minor damage to user’s lives **(2)**  **Reproducibility:** Should the vulnerabilities in the anti-DDOS system not be patched, or changes not made to the server architecture to prevent similar attacks in the future, it is likely such attacks would continue to work **(7)**  **Exploitability:** The attempt would require not only some information on the wireless architecture of the system, but also a great amount of machines to perform a DDOS attack **(5)**  **Affected Users:** This would affect all users at the time of the attack **(10)**  **Discoverability:** As previously mentioned, some knowledge of the architecture would be crucial to performing a successful Denial of Service Threat **(6)** |
| Total Risk Rating | **6** |
| Mitigation techniques/Secure Design Recommendations | Apply robust and strong anti-DDOS protections, with backup wireless and web servers should the main connection go down  Rate limit incoming connections, so as to reduce the amount of incoming traffic  Set in place filters to ignore obviously harmful or misconfigured packets |

|  |  |
| --- | --- |
| Item | Staff |
| Title | Stealing Admin data |
| Application | Database |
| Threat Target | Servers |
| Threat Type(s) | Elevation of Privilege/Information Disclosure |
| Risk | **Damage Potential:** It would allow (depending on the admin’s privilege level) for complete server and system access **(10)**  **Reproducibility:** It would require very specific series of events and gathered information without arousing suspicion, and such information would become useless immediately after the event **(1)**  **Exploitability:** This would require not only trained and professional attackers, but also luck, time and deep knowledge about the building, and the people working there **(2)**  **Affected Users:** Every user would be affected, in addition to the admin users **(10)**  **Discoverability:** It should be nearly impossible to gain access to this information normally, hence social engineering, dumpster diving e.c.t **(2)** |
| Total Risk Rating | **5** |
| Mitigation techniques/Secure Design Recommendations | Secure in Deployment:  Implement routine password and username changes by system policy  Implement policies to shred and dispose of crucial and confidential information safely and discretely  Secure by Default:  Utilise the Principle of Least Privilege – allow the least amount of people required to have access to the information, and implement more restrictions and safety measures in correlation with that user’s access level.  Use 2-factor authentication to log in  Utilise company VPN’s, and limit BUOD |

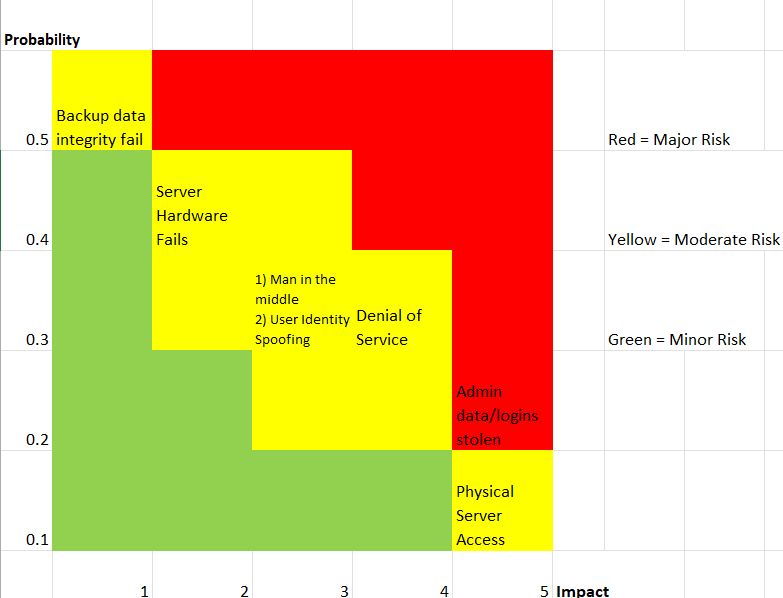
**Risk Analysis:**

In the upcoming Risk Assessment Form and Risk Severity Matrix, I have discussed, labelled and analysed the possible threats and associated risks of this proposed system.

**Risk Assessment Form:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Risk Event** | **Probability** | **Impact** | **Detection Difficulty** | **When** |
| Denial of Service attack | 0.3 | 4 | 5 | Anytime Application Processing System is online |
| Physical Server Access | 0.1 | 5 | 2 | Anytime |
| Man in the middle attack | 0.3 | 3 | 1 | During data transfer between server and user |
| Server Hardware Fails | 0.4 | 2 | 5 | Anytime service is active |
| Admin data/logins stolen | 0.2 | 5 | 2 | Anytime |
| User Identity Spoofing | 0.3 | 3 | 1 | Anytime Application Processing System is online |
| Backup data integrity fail | 0.5 | 1 | 4 | Anytime service is active |

**Risk Severity Matrix:**



**Secure Design Specification**

SD3 should be present in all aspects of this project, and it should be built with security in mind since the start. Within the actual system architecture, as mentioned before, the principle of least privilege should apply, not just to the operations and programs of the system itself, but to the administrative users interacting with said system. The ‘sensitive’ PII should have stricter access controls, since not only is it more privileged information, but also, more damaging should it be accessed.

Due the importance of security in this system specifically, documentation and training for the staff (Secure in Deployment) will be crucial. Training on Phishing, how to protect your internet presence, two-factor authentication, and possibly an Intranet VPN are all options that should be implemented, to both decrease the vectors of attack, but also limit possible information spread regarding the internal workings of the system. Intrusion Detection systems should be used, and consulted regularly, with the security team taking time to go through and update/patch critical issues found. Credentials should be changed and updated regularly, with systems in place to prevent repeats or passwords too weak, in order to decrease the likelihood of logins being stolen or guessed. Defence in depth is a key component here, due to the multiple sub-systems being used, with the higher-levelled ones being used to protect the lower-level aspects, given the lack of exterior user interaction with them. (layered security).

**Risk Response Matrix:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Risk Event** | **Mitigation Plan** | **Contingency Plan** | **Trigger** | **Responsibility** |
| Denial of Service attack | Mitigate: Prior testing, rate limit incoming connections, robust filters updated regularly | Backup servers should be utilised if mitigation plans fail, temporarily maintaining Availability while team mitigates issue | User connectivity not restored after 5 mins | People responsible for the Application Processing System, Cyber Security Team |
| Physical Server Access | Mitigate: Physical security in place, badges, employee training, principle of least privilege | Should the physical server be un-operational, and unlikely to improve quickly, utilise a backup server (perhaps one of the onsite backups) in place of the main temporarily | Suspicious activity, physical hardware failure with signs of tampering, intruders found on cameras or in person | Security Team, receptionists, employee who’s credentials were used/stolen |
| Man in the middle attack | Mitigate: Use more secure transmission protocols, encrypt data transfers, use sophisticated handshake protocols | If this type of attack is suspected to be occurring, or suspicious activity is detected, then prevent further traffic to that user for a period of time, before attempting to reattempt | Automated systems detect errors in communication protocols, incorrect packets being returned, failure to confirm arrival at destination | Same as first |
| Server Hardware Fails | Mitigate: Rigorous testing, multiple backups, automated restart protocols | Same as physical server access, in addition to forcing a hard-reset | Server not rebooting within 5 mins of downtime, repeated failures to load/reboot | Hardware team, person who chose the brand of hardware |
| Admin data/logins stolen | Mitigate: educate all internal users on proper etiquette, mandatory password changes every couple months, vpn’s, internal system portals, 2-factor authentication | Have a system for resetting users passwords, not accessible through any outside source, purely onsite.  Have the ability to disable accounts for periods of time – the ability to do so protected by enhanced passwords. Automated programs searching for strange/unusual behaviour and flagging it | Automated programs flag activity of an admin as fraudulent, account begins to undertake flagged actions un-associated with their normal role, alerts of massive database changes | Cyber security team, admin who’s data was stolen |
| User Identity Spoofing | Same as man in the middle, plus having secure and complicated hashing and encryption | Same as man in the middle attack | Same as man in the middle attack | Same as first |
| Backup data integrity fail | Mitigate: Test thoroughly beforehand, have multiple backups, have automated system to try again when backup failed | Have multiple backups, and additional systems for both automated and manual restorations and backups of database. End of the day confirmation by team that backups have occurred – alerts when multiple have failed | Backup failed multiple times, automated alert message being received, end of day manual checking found error | Internal IT team, Cyber Security Team, Admins |

**Conclusion:**

Based on all the data presented above, I believe my modelled system could be considered properly secure, if all suggestions and Secure Design Specifications were followed, and updated, when further unforeseen events were to occur. The security of this system, with the PII and governmental nature, is paramount, and I think that goal has been achieved here, and will assist millions of people in streamlining their passport application processes. I believe my quotations and citations were done in a clear format, and while I had some issues with the hypothetical nature of the proposed system, and the difficulty in finding information regarding specific internal tools and systems, I believe I have done a good job in determining which would be necessary and needed for the system to function as required.

**Bibliography:**

* European Commission (no date) What personal data is considered sensitive?. Available at: <https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_en> (Accessed: 07/03/2024).
* Information Commissioner’s Office (no date) Special category data. Available at: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/lawful-basis-for-processing/special-category-data/> (Accessed: 07/03/2024).
* Home Office (2022) His Majesty’s Passport Office. Available at: <https://careers.homeoffice.gov.uk/role/frontline-and-operational/hm-passport-office> (Accessed: 14/03/2024).
* Post Office (2024) What are biometric passports?. Available at: <https://www.postoffice.co.uk/identity/biometric-passports> (Accessed: 07/03/2024).
* HM Passport Office (09/22) Guidance for paper passport applications. Available at: <https://assets.publishing.service.gov.uk/media/636e1326e90e07618e6ae553/09.22_Guidance_Booklet_IND.pdf> (Accessed: 07/03/2004).