Portant – Protecting Sensitive Data from Multiple Sources

COMP3850 – Computing Industry Project

Group 37 – Bradley Anderson, Jarrod Adair, Socheat Chhun, Md Mehedy Hasan, Arshita Jaryal, Edward Morris

Contents

1. Introduction 4

1.1. Problem Identification 4
1.2. Assumptions 4
1.3. Opportunities 5
1.4. Mandates 5

2. Success Factors 5

3. Current Situation 6

4. Benefits 7

4.1. Tangible Benefits 7
4.2. Intangible Benefits 7

5. Alternative Solutions 8

5.1. Alternative 1 – No Action 8
5.1.1. Advantages 8
5.1.2. Disadvantages 8
5.2. Alternative 2 - Virtual Private Network 8
5.2.1. Advantages 8
5.2.2. Disadvantages 8
5.3. Alternative 3 – 3rd Party Mail Encryption (MIMECAST, etc.) 9
5.3.1. Advantages 9
5.3.2. Disadvantages 9
5.4. Alternative 4 – Google Forms for Information Collection 9
5.4.1. Advantages 9
5.4.2. Disadvantages 9
5.5. Alternative 5 – Custom HTML Forms with Extra Layer of Encryption 9
5.5.1. Advantages 9
5.5.2. Disadvantages 10

6. Recommended Solution 10

7. References 11

Table of Abbreviations

Abbreviation	Meaning
API	Application Programming Interface
GDPR	General Data Protection Regulation
IEC	International Electronics Commission
IPSec	Internet Protocol Security
ISO	International Standards Organizations
HTML	Hypertext Markup Language
MVP	Minimum Viable Product
NIST	National Institute of Standards and Technology
SQL	Structured Query Language
SRS	Software Requirements Specification
VPN	Virtual Private Network

1. Introduction

Our team has been tasked with the development of an application that deals with the collection, transfer and collation of information securely at all stages of transfer and storage.

The team consists of 6 people, each with their own roles and responsibilities. These are as follows:

Arshita Jaryal: Project Manager

Bradley Anderson: Documentation Manager

Jarrod Adair: Developer

Socheat Chhun: Developer

Md Mehedy Hasan: Cyber Security Analyst

Edward Morris: Cyber Security Analyst

1.1. Problem Identification

The problem falls under Cyber Security/Cryptography since it is concerned with the development of an application with cyber security protocols as the forefront of our solution.

Portant, the company sponsoring the project is looking to become a communications layer service for organizations to exchange information between individuals, departments, or other organizations.

One major issue that arises with communications is the security of stored and transferred information. Organizational information can be vital to the operations of said organization, hijacked or leaked information can cause monetary and reputational damages to companies that can take years to fully recover from, if at all.

Depending on the nature of the organization, data breaches can also include sensitive information concerning groups of people such as medical records, bank information, etc.

With sensitive information being exchanged, there needs to be a way to ensure that only the sender and the intended recipient/s will be able to see the information being sent if it is intercepted.

1.2. Assumptions

- That the developed application will be a Google Chrome/Drive extension since it utilizes Google APIs and Portant's existing product is a Google Docs extension.
- Once the data/information has progressed to the Google APIs we assume that the existing google APIs have their own security measures in place.
-

1.3. Opportunities

Portant currently offers an application that allows for the streamlining of documentation processes such as formatting, data entry and transfer. With these functions being offered, Portant is good for smaller projects and companies that would be passing data between an internal network with a smaller risk of being exposed to anyone that is not the intended party.

The major benefit of Portant is that their product is easy to use and code-free, meaning that no prior knowledge of coding or programming is needed to efficiently use the application. Where previously something like SQL would be needed to move large amounts of information between spreadsheets or tables.

With the implementation of data encryption of stored and transferred data, the product can then be marketed to larger organizations as a communications and documentation automations platform. The security measures in place for communications would encourage larger organizations that would want secure communications to protect data to use the application. With a larger customer base available to Portant, they could then build up demand for expanded functionality which can be facilitated through the monetization of their application.

1.4. Mandates

The security and communications protocols must adhere to international standards of security as outlined by organizations like the ISO/IEC and NIST. This is also in addition to complying with many regulatory standards of data privacy and security set out by governments around the world such as Europe's GDPR, Australia's Privacy Act 1988 and the United States Privacy Act 1974 to name a few.

In addition to this, to be able to integrate the application with G Suite products like Drive and Gmail, Google API credentials would need to be obtained through Portant for company use.

2. Success Factors

For the project to be successful, an application needs to be delivered with the following features and functionality.

- Users can request data from one or more sources by email or a HTML form.
- Users can specify data sources to draw from by email.
- Any data sent via email or forms must be both secure and verifiable.
    - Secure in that only the sender and intended recipients can view it regardless of if it is intercepted at any stage of transit or storage.

    - Verifiable in that the information is provided exactly as it was sent and it was sent by the person that was expected to provide the information.
- Any information that is collated into a Google Doc in an easy to view format.
- Lightweight enough to be used in a browser and have quick response times.
- Can automate repetitive and often used procedures such as requesting information at regular intervals automatically.

To accomplish the above, the cyber security team will design security measures for end-to-end encryption and storage. The developers will implement security measures designed by the cyber security team as well as creating data transfer and writing protocols via Google's API. Any documentation to accompany this product such as user manuals and software design and development documentation are to be done by the product and documentation managers.

The timeline of which to accomplish this task is as follows:

- Weeks 3 – 8: The initial development of security protocols as well as the information gathering method for the first MVP deliverable in Week 8, emphasis is focused on getting secure transfer implemented in a simple form or email format.
- Week 8 – 11: Work and edit existing prototypes for deliverable 3. Refine our Project plan and SRS. Organise a demonstration of our plan and prototype with our client.
- Week 11 – 12: Finish all editing and create the final Project Presentation.
- Week 12 – 16: Form Group meetings to create and rehearse the final presentation and discuss feedback to create a concise and consistent presentation.

3. Current Situation

As stated before, Portant has a product that enables the streamlining of documentation processes and the transparency of information. They are aiming their product at modern organizations that rely on the flow of information between stakeholders, departments, and other organizations.

Portant wants to see this security functionality as a 'proof of concept' of what kind of security features and functionality can be incorporated as a part of their existing Portant product. The idea is that when transforming the documents, information is kept private. Examples of this is not only for privacy of general users but for the privacy of the business, security measures need to be taken in layers which even existing employees have restricted access to. This ideology envelopes the businesses data from all potential security threats.

4. Benefits

4.1. Tangible Benefits

1. Cost Savings
    a. Clients that use the application can cut labour costs that would otherwise be spent managing documentation and communications.
    b. Revenue can be increased as more manpower can be dedicated to developing their products/services.
2. Time Savings
    a. Time can be saved that would be spent working on menial documentation tasks and put towards product development.
3. New Products and Services
    a. The streamlined and secure communications and information flow can benefit companies of all sizes as the benefits allow a company to focus on developing their product/service.

4.2. Intangible Benefits

1. Increased Worker Morale
    a. With the documentation and information gathering/transfer process made much easier, morale is improved since workers are spending less time being bogged down by menial documentation tasks and more time on productive work.
2. Improved Communication
    a. With the finished solution, communication channels between the user and the data source will include encryption services which can enforce industry benchmarks of Confidentiality and Integrity. This security will increase trust for the end user, providing clarity and confidence during communication.
    b. Communication processes will also be faster since with automated forms that can collate information, people will not need to manually chase up information via email or spend longer than is necessary sending or entering information into spreadsheets/documents.
3. Increased Worker Experience
    a. As workers improve their communication and their morale is increased, workers gain experience in the project environment, this allows for future projects and processes to run much smoother as they are them accustomed so these specific work environments.

5. Alternative Solutions

5.1. Alternative 1 – No Action

5.1.1. Advantages

- Time and money saved on development and thus can be spent elsewhere.

5.1.2. Disadvantages

- Existing security concerns will still be present.
- Risk matrix for cost-benefit analysis would be necessary to determine the viability of no action.
- Potential loss of existing consumer base and limiting the appeal of Portant's application to companies that are not as security conscious, this will result in limiting or loss of income.

5.2. Alternative 2 - Virtual Private Network

5.2.1. Advantages

- VPN's provide overall security with high performance and remote access. Using tunnel IPSec, data can flow securely through the cloud without being visible to malicious actors.
- Compared to different paid services, VPNs are a cost-effective method of implementing network security.

5.2.2. Disadvantages

- Whilst the previously stated cost-effective benefits provide an advantage over other paid services, VPNs are still a paid alternative to an otherwise cost-free solution.
- VPNs may also impose an internet connection and bandwidth deficit whilst using the service.

5.3. Alternative 3 – 3rd Party Mail Encryption (MIMECAST, etc.)

5.3.1. Advantages

- Third party mail encryption services already exist and only require its implementation into the Portant dataflow. This can be a cost-effective method of introducing a high level of security with maintenance outside of the company's capacity.

5.3.2. Disadvantages

- Depending on the service, a third-party mail encryption service has limited customisability.
    - Requires constant communication with third-party service team for maintenance.
- There is an associated cost to each third-party service; each having different price ranges.

5.4. Alternative 4 – Google Forms for Information Collection

5.4.1. Advantages

- Existing form system that does not require development, saving time and money.
- Easier to integrate with other G Suite services like Gmail and Drive for the purpose of mail and data collation.
- Do not need to worry about maintenance after development.

5.4.2. Disadvantages

- Relies on Google's security measures which is unknown in the type of security and to what degree it is implemented.
- Limits the implementation to using a pre-made form system, which limits features that can be added.

5.5. Alternative 5 – Custom HTML Forms with Extra Layer of Encryption

5.5.1. Advantages

- More flexibility with implementation and functionality.

- Allows for third-party security and transfer protocols which further adds flexibility with implementation.
- Since the inner workings will be known through development it will be easier to maintain and further develop as opposed to using third party forms.

5.5.2. Disadvantages

- Money and time will need to be put forth to designing and developing the security measures and forms.
- Since it is a custom-made system, thorough testing will need to be done to ensure transfer and security protocols are implemented properly.
- The project will need to be properly planned to ensure all targets are hit on time and to an acceptable standard.

6. Recommended Solution

Our Sponsor wants us to build a web application that will encrypt the form that we send to our users. Even though VPN is the option that will be the most secure out of our alternative solution, this option is out of the way because we need to build our own web application that does all this without the help of VPN servers.

For the Google Form Alternative, we do not have any control over the form. Which contradicts what our sponsor wants us to do. Google Form does not encrypt our form and send it to the user, it is just a tool for us to easily build forms and get respond from our user. What we are looking for in this Project is to send the form from our Python server and receive it back from the users in a secure way. Which is why we decided to go with the last alternative solution.

Our recommended solution is Custom HTML Forms with Extra Layer of Encryption which is mentioned in Section 5.5. It has much flexibility with implementation and functionality than other solutions. Using a Python third party library will provide the requested form with extra layers of security.

If we are using Google Form to send to our client, we do not have full control of what we are sending and receiving. Instead, we are building our own custom HTML form with an extra layer of encryption with the help of a third-party Python library which is called Virtru. With the Help of Virtru, we can create our own form and encrypt it and send it to the user. After the user has completed the form, we can decrypt the form in our Python server and send it to the Google Docs API or Google Drive API.

Once any information passes from email or forms through Google’s API then the security measures in place are that of Google’s which we have no control over as to the security in place.

7. References

Virtru Developer Hub. 2021. *Quick Start: Python*. [online] Available at: <https://developer.virtru.com/docs/getting-started-python> [Accessed 10 March 2021].

Sigler, C., 2021. *A Simple Approach to Securing Web Forms*. [online] Medium. Available at: <https://medium.com/virtru/a-simple-approach-to-securing-web-forms-801cd5af405e> [Accessed 10 March 2021].