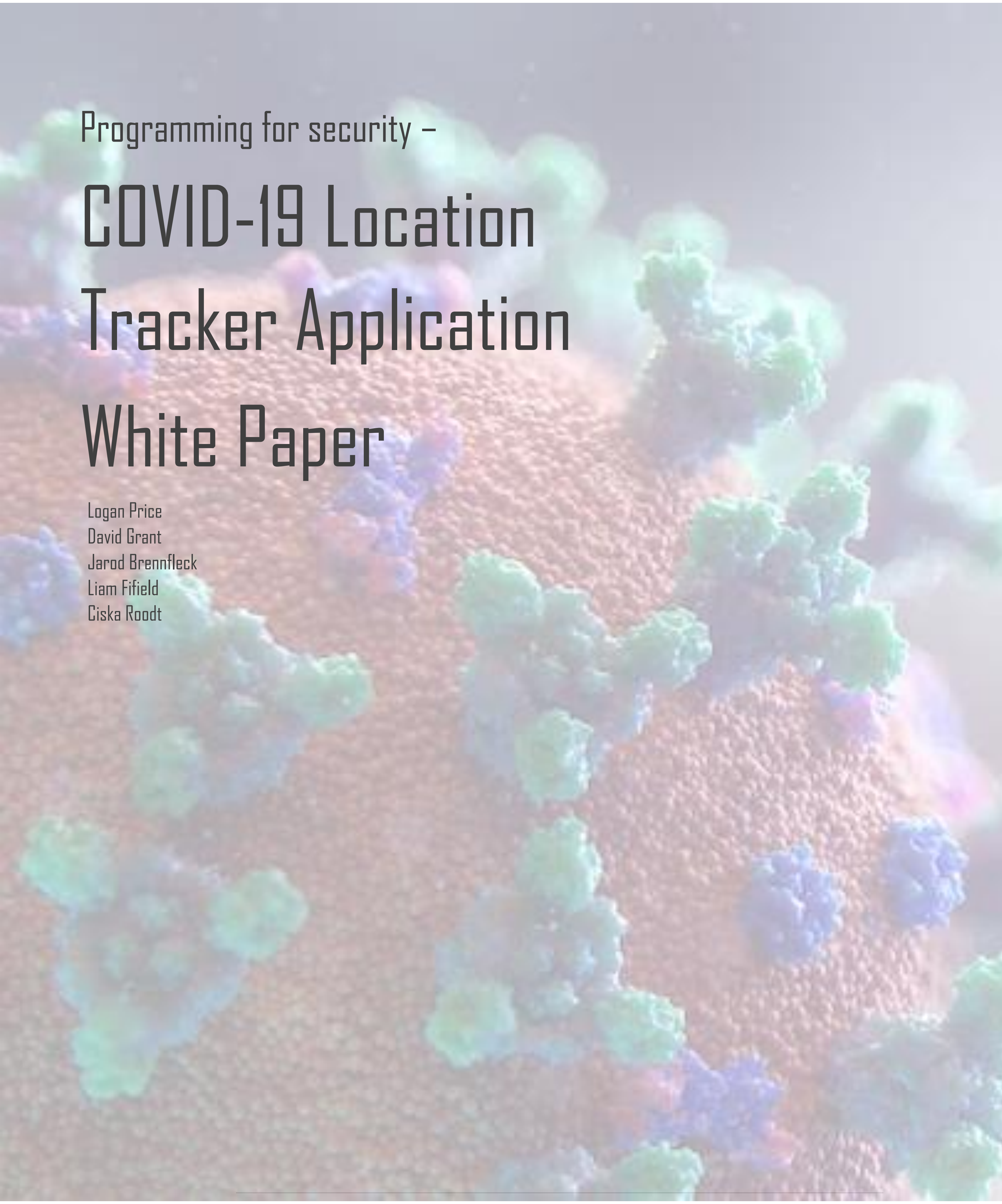

Programming for security –

COVID-19 Location Tracker Application White Paper

Logan Price
David Grant
Jarod Brennfleck
Liam Fifield
Ciska Roodt

Abstract

With the continued spread of COVID-19 within the community, it is paramount that effective methods are in place to monitor and slow progression. Due to the highly infectious nature of the virus, it is vital that an effective location tracker is utilised. This tracker must also be protected against attack from malicious parties. As it will be storing sensitive data relating to individuals and their movement, the application must consider security as a top priority. Programming for Security Team have created an application that addresses the importance of having secure data transmission, stores log in information effectively and works to prevent against injection attacks.

Problem

Location trackers such as a one being designed for Covid contact tracing, is storing the sensitive data of individuals all over the world. If a malicious actor was able to access the stored data, they would be able to retrieve individuals names, birthdates, emails, locations and the sale of sensitive information on the dark web. Additionally, incorrect, or malicious data can be inserted. This makes the legitimate stored data invalid, as none of it can be trusted if there is enough false data in the database. For this reason, it is vital that a location tracker is fitted with the ability to protect the information of its users.

Background

Covid-19

The spread of COVID-19, while it has slowed down, has not fully stopped in the 14+ months that it has existed. There have been several, repeated outbreaks in several cities around Australia, even after border restrictions have been implemented. This has resulted in repeated lockdowns, as which has resulted it social and economic hardships.

Why a location tracker?

Location trackers are allowing the public to against move freely by allowing for an accurate log of locations to be maintained. By doing so it allows for accurate contact tracing if a case is to be discovered, and hot spot mapping to be conducted.

Solution

“PFS group” has created an application that integrates the necessary security requirements of an effective covid tracker. This application is utilizing a python run back end with a web developed front end. Within both of these sides considerations have been made to target Password protection, securing the data link and input filtering.

Considerations

Password Protection

To ensure the security of the information contained within the Database all passwords will be salted and hashed. By doing so it helps mitigate the risk of compromise through hash table attacks.

Hashing –

A users password is run through a specific one way algorithm in order to generate an encrypted hash of a fixed length. In this application SHA256 was utilised as a one way function.

This hash is then stored within the internal database instead of the plain text password. By doing so it ensures in the event of a breach a hacker does not have easy access to account passwords. To further ensure the confidentiality of the information salting can be added to the passwords.

Salting –

Salting ensures that there is no collusions between different users password hashes. The addition of a unique salt to every users passwords ensures that the same hash function can be used without the risk of collusion. It also means that if a hacker is able to crack a single users hash, they will be unable to gain access to other accounts. It helps to ensure the security of users accounts and information without requiring the user to create a unique password.

According to McAfee Security, ideally the length for a salt should be at least 32bytes representing the same as the length of the output of a hash

Data Protection & Functionality

To ensure the data contained within the application is secure while allowing access to authorised persons, the data must be encrypted. A symmetric key encryption cipher, AES128 was utilised within the application. It ensures the data is secure, while allowing nurses using a specialised login to enter hot spot locations and return the individuals who may need to be contacted.

Secure data link

To ensure that data is secure while passing between user and server on the transport layer, the stream can be encrypted through TLS. Transport layer security or TLS is the cryptographic protocol that uses a combination of symmetric and asymmetric encryption in order to encrypt the data that passes. TLS assists in the protection against man in the middle attacks and can assist in the assurance of integrity of transmitted data. It is important to note that it does not ensure the integrity of data on either end, only protects it as it passes through the network.

Input filtering

In order to effectively mitigate against an injection attack, input received from the client side must be filtered. This can be done in both the Server Side and Client side. Server Side filtering takes a clients input and ensures that it is valid before returning a result, while client side filters operate on the browser side and ensure input is valid before sending it to the server. One of the mechanisms used to prevent against an injection attack is removal of user input. Information such as location is gathered through phone GPS location as opposed to user text input.

Conclusion

The applications used to tract the spread of the covid-19 have an obligation to protect our sensitive information. Programming for Security Group has created an effective application that works ensure secure data transfer, effective password protection and prevents input filtering. With the use of this application, location can be effectively tracked and information can be securely stored.