Project Proposal

Client profile

The client of the project is the 7th Signal Regiment a unit of the Australian army. This unit of the Australian army is a signal intelligence unit and therefore is interested in the study and practical implications of signals in national defence and warfare. This includes "*electronic signals and systems such as communications systems, radars, and weapons systems*" (Commonwealth of Australia, 2021).

The 7th Signal Regiment units place in army and the 6th Combat Support Brigade is as described above and is therefore imperative that is continuously evolves their capabilities to the most up to date implications of electronic signals. This is because it is important that ground forces can communicate without hostiles having the ability to derived information for a tactical advantage over them. This means that the regiment must keep up with or surpass technical capabilities of other nations.

The project aims to assist team managers and their personnel to track ongoing work projects and co-ordinate personnel all using their personal devices, phones for example.

The impact of the project is aimed to increase the effectiveness and efficiency of teams by allowing them to use widely available technology to assist them in conception, initiation, planning, execution, monitoring of their work projects. This will increase the rate at which work projects are able to be completed.

The project will contribute to the 7th Signal Regiment as due to security concerns the available technology that allow for communication and planning of work projects is limited with current widely available solution all having the flaw that information is controlled by a 3rd party that is not controlled by defence and software source code cannot be access by them therefore defence is unable to verify security measures are in place.

Problem definitions

Client Project description

The projects finished capability as described by the client is an application accessible on PED's (personal electronic device) designed for co-ordinating/collaboration of teams, tasks and projects that is approved for security classification of up to official. Currently teams use outlook calendars, excel spreadsheets vera teams or a "defence diary" on the DRN (Defence restricted network) to organise their projects, the issue with the current methods are information is split between many different applications or by individuals which can cause team managers to lose track of ongoing work due to difficulty finding where information is stored. Documenting task completion can be difficult for personnel as DRN access is not always easy on a job and their competed task are document long after it has been done (end of the day for example). This can cause needless delays or even outright forgetting to document task completion. With the current system used for organising projects there are many points where confusion can be caused, and information can go missing or undocumented.

Client Needs

The intent behind this project seems to be to create one easy to access application for both team managers and there personal to track day to day projects in real time as well as standardising a communication method for projects while keeping a detailed record of both communication and

task progress (likely to aid with accountability and mistake finding). This will likely be most accessible as a downloadable application on an individual's phone or app.

The main problem with current options in the market seem to be the security risk associated with using applications where direct control of information, servers and source code are not controlled by defence Australia. These risks include uncertainty of encryption levels of information being send over networks and server hosting location (application database access not controlled by defence). These seem to be the main reasons why a dedicated app made and controlled by defence is needed. Even through not directly stated being able to time maintenance and server down time to prevent needless confusion for personal is also a reason on why defence would prefer to use their own personal servers. Also, from my own personal experience with using the DRN (current solution used DRN access) I have found that having to access program through the DRN entail going through a virtual machine which causes all application usage to come with lag or a delay causing user experience to be slow when performing any actions. To have a highly responsive product for end users the application will need to be separate from the DRN to prevent the issues associated with virtual machines.

High level objectives

The project can be defined by 2 high level objectives the product or application must be designed to meet. These being official+ level encryption and application capability.

- official+ level security (HL-1)

The application will need to be clear by defence to have access to information at official at minimum or higher securities levels. This will mean data send over any network will need to be encrypted, users will need to be authenticated and data stored will also need to be encrypted. Any other possible security vulnerability will also need to be addressed, eliminated, or minimised to a reasonable degree. These will include but not limited to cross website scripting, sql injection, PED's loss (device password storage and loss of access), key loggers, remote access to device and shoulder surfing.

- Application Capability (HL-2)

The application must be capable of organising, sorting, and tracking on going work projects from wherever a user is.

Low Levels objectives

The high-level objectives can be converted to the following low-level objectives.

- RSA encryption (HL-1)
  RSA encryption is an asymmetric encryption method approved for information with the classification TOP SECRET. The RSA will need a 3072-bit key to be approved for this level of classification. RSA encryption stated will need to be used to exchange AES keys. (Australian Signals Directorate, 2021)
- AES encryption (HL-1)
  AES will be used to send information across a network at minimum AES-256 will need to be used for information of up to TOP SECRET (Australian Signals Directorate, 2021). AES will be used for general information exchange as RSA will likely be far too slow to both encrypt and decrypt data causing end users to have an unresponsive user experience (Priyadarshini Patil, 2015).

- Password hashing (HL-1)
  To prevent storing passwords in plain text in the database hashing will need to be used. SHA-2-384 will be used and is clear of TOP SECRET classified information. (Australian Signals Directorate, 2021)
- Ability to create team/project and create/track, update tasks (HL-2)
  The application will need to capable of assisting team leaders and personal in managing tasks. Therefore, the application will need features and functionality to create team/project and create/track, update tasks.
- Ability to communicate to team or individuals (HL-2)
  Project management no matter the job will require a way for individual assigned to teams to communicate in a quick and easy manner. This will entail the ability to send messages to groups and individuals in teams as well as push notifications to alert users of messages.
- Easy to understand UI design (HL-2)
  Projects can become quickly overwhelming with the sheer number of tasks required to be done. The user interface for clients will need to be easy to navigate to important information as well as ways to view only important information to prevent screen cluttering as most users will be using the application on small screens.

Project Constraints

The constraints on this project's solution revolve around security.

The most impactful security issues are with iOS kill codes installed on all apple devices using iOS 9 onwards. Mobile device management (MDM) administrator can remotely enable lost mode and from there remotely lock and wipe devices. (2021 Apple Inc, 2021) It should be noted that this can be done without any agreement with user if desired from apple (from an technical perspective). This is an issue as if apple desired, they could wipe all apple devices used by Australian defence personnel. As the app aims to be used to coordinate defence personnel having a 3rd party with the power to disrupt communication would be a major security concern. To avoid this the app will not be designed for apple devices forcing users to have PED's with operating systems that do not have iOS installed.

There are many security issues with using webs-apps that include but are not limited to cross website scripting, sql injection and key loggers for example. Due to the limited time and developers on the project it will not be feasible to develop an application that is able to handle all these security issues. To complete this project in the timeframe a mobile app will be developed as they are fully executable programs with far less security issues to handle which will therefore save time.

Finish State

A finish project will produce an application accessible on PED's designed for co-ordinating/collaboration of teams, tasks and projects that is approved for security classification of up to official.

Organisation Standards

As this project is an army commissioned contract it will therefore fall under the organisational standards outlined by the department of defence.

The intellectual property of the project will fall under the ownership and licensing under contracts for the acquisition of Defence capability. The 7th signal regiment will own the copyright of the project. Copyright is the exclusive right to reproduce or copy an original work in a material form, to

publish the work and to communicate the work to the public. The IP of this project will include programs, Source code, databases, and designs documentation. (Commonwealth of Australia , 2018).

The data and documents generated within this project will need to be stored in defence's environment or the contractors. Data will need to be easily identified to allow users to readily search for, located, and access the data when needed. (Commonwealth of Australia , 2019)

As a QUT student working on this project I must comply to the Student Code of Conduct. Most notably this will include academic misconduct. The sections that apply to this project will be Plagiarism, Self-Plagiarism and Collusion (Queensland University of Technology, 2021).

External Standards

There is no governing body for app development standards. Platforms such as apple and android do require developers to submit privacy policies entailing how and why information is being collected to allow apps to be publish on their platforms. This may be needed to allow easy access to app for users.

As the client is apart of defence and therefore an Australian government organisation the app will need to conform to the Australian privacy act of 1988. Most notably its 13 principles (Commonwealth of Australia, 2021).

Focused Examination of Literature

The Australian Signals Directorate (ASD) has approved the cryptographic algorithms of RSA with 3072 bit key, AES-256 and SHA-2-384 for information classified up to TOP SECRET. (Australian Signals Directorate, 2021). Due to defences high security standards these algorithms will need to be implemented to allow for secure communication between user apps and defence servers in this project.

RSA is a widely used encryption and decryption algorithm but also an asymmetric algorithm meaning it has different keys for encryption and decryption allowing for safe key exchanges between parties. (A. A. Hasib and A. A. M. M. Haque, 2008)

An example of using RSA to secure connections for Secure e-learning web-based application has been implemented and shown capability to prevent data theft, data modification, data fabrication of an unauthorized user and prevents files from being readable both in storage and transmission through the encryption process. The RSA algorithm also had the benefit of authentication data to a specific user (Baihaqi, 2017). This example shows that the RSA algorithm is an effective algorithm to establish secure connection between parties and is an acceptable method to establish security keys and encrypt data over a network.

As stated, the RSA is an effective algorithm however there are disadvantages to using it. These being the time it takes to encrypt/decrypt data as well as the avalanche effect. The avalanche effect is simply how much the data will change once encrypted due to a small change in the original text. Out of the most used encryption algorithms (DES, 3DES, AES, Blowfish) RSA performed the worst having the least amount of change. Note that AES performed the best (Priyadarshini Patil, 2015). The RSA algorithm also is easily the worst algorithm to choose from when comparing encryption and decryption times as it will grow with the size of the data (over 2 seconds for 3MB of data) where other algorithms will not grow due to these circumstances such as AES for example (Priyadarshini Patil, 2015). This shows that using AES algorithm will allow for a far more responsive app as well as

shown far greater changes from the original plaintext when encrypting data. For the project using AES will be a better choice over RSA however AES is a symmetrical algorithm creating a problem with secret key exchange between communicating parties.

To solve the issue with key exchange an implementation of using a combination of RSA and AES was used to secure electronic health record application. This method used the RSA algorithm to send the AES secret key over a network encrypted. This allowed a secure connection between party to be form using the AES algorithm without risk of the disclosure of the secret key (Wardhani, 2016). A similar method will be used in this project to create a connection between a server and client apps.

RSA and AES will be used to establish an encrypted communication between the server and user apps however authenticating users will be done using knowledge possessed by the user in the form of passwords. To prevent users' passwords or other identifying knowledge being possessed by the server to be disclosed a hashing algorithm will needed to be used on user's data. Approved hashing algorithms include SHA-2 with 384-to-512-bit outputs may be used for information with the classification of TOP SECRET (Australian Signals Directorate, 2021).

SHA-2 can protect user's data as it transforms an input message into a 256 bits message. This transformation is one way, and the original message cannot be recreated from the resulting transformation (R. V. Mankar, 2013). The SHA-2 has shown a high level for randomness in tests being able to completely remove the original input and compress it down to the specified bits (Z. Al-Odat, 2019). These tests have shown that the SHA-2 hashing algorithm is a highly effective algorithm with no noticeable issues and is therefore the algorithm that will be used to secure passwords in the sever database for the project.

In the java standard libraries or API provided by Oracle for the Java platform includes built-in many of the most used cryptographic algorithms, including the RSA and AES encryption algorithm as well as the SHA message digest algorithm and key agreement algorithms (2021 Oracle, 2021). These libraries will allow the security required by defence to be implemented using the programming language java therefore java will be used to develop the project.

Milestones and deliverables

The app will be made using an agile development methodology by separating app features and capabilities into separate subsystems which will each be designed and implemented independently. In practice this will be done by using an object-oriented programming approach to separate each feature or capability into individual objects. Using an object-oriented approach will also keep the project very modular as well as allow related source code to be easily identified to its function.

The project will be tested throughout development using a range of phone emulators and running severs and databases on the developers own system/devices. Testing will be done by designing test cases that will run on the development version of the app and server which will require a certain result to continue program execution or will throw an exception and print it to a terminal/log.

Significant milestones and deliverables of project can be seen in the table below.

Milestones / deliverables	**Description**
Reports and Presentations	
Project Proposal	Initial project proposal document
Progress Report	Semester 1 progress report

Progress oral	Semester 1 oral presentation on progress
Project update	Report to highlight progress and changes to initial project proposal
Final report	Final report on project
Final Oral	Final oral presentation on project
Development Milestones	
Client to Server Database encrypted communication	Demonstrate the ability to send information using AES and RES encryption over a network from the clients PED to a server and store/extract information onto/from the server. Must be capable of handling multiple client connections.
User authentication / login	Demonstrate the ability to login from a client app using all necessary security measures. Including AES encryption, RES encryption, hashing of stored password.
User registration	Demonstrate the ability to create new users over a network. No information on user can be sent unencrypted over the network and data must be stored in database
Home ui design / app navigation design	Designed general look and navigation of the application. This will include UI design and home UI will be implemented and navigation to app features will be implemented.
Feature 1 – team organiser	The application ability to create a team and create/track/assign tasks is complete. This will also include the ability from personal to complete tasks.
Feature 2 – group and individual messaging	The application ability to create message rooms for teams and send messages to and from individual users is implemented.
Feature 3 – personalised check list	The application ability to create a personalised check list of jobs needed to be completed by individual users.
Feature 4 – team message board	The application ability to create a team message board to store important information – sort of a news board or like a GitHub read me file

Tasks

The tasks needed to complete the milestones above will include creating 2 separate application a server and a client app which will communicated using TCP over the internet. The server will be a command line application and will require access to a database. The client app will be design for a mobile device and therefore will require a GUI and will be the interface for users to interact with the server database. Tasks can be seen dot pointed below.

- Programming language / ide selection
  There are many ide's and potential programming languages that could be selected to complete this project all with advantages and disadvantages. This task entails researching the possible options and deciding on which options to choose.
- App testing methodology
  This task entails having a way to test the application during development and deciding on the application build process methodology (method to convert code to usable application or compiling code).
- Set up GitHub.

A GitHub repository is important for a project as it allows for an external backup of files as well to revert project back to usable states if problems are encountered that cannot be solved with current project state. It is also a way to keep a log of individuals contribution if more developers are added to the project.

- Set up client / server sockets.
  The socket connections are the backbone of the project as it is the method that allows communication over the internet or network (connecting client to server) will likely be done by TCP.
- Set up encryption protocol (AES or RES 256)
  This task is used to set up the encryption of messages over socket connections and establishing key exchange procedures.
- Set up/design database on server.
  The server of this project will need a secure method of storing data. This task entails creating a database connection between the server program and database. Preliminary database design will also be needed to complete this task.
- Initial login page creation and functionality
  With all the previous tasks complete development of the client application can start with a login page to authenticate users before granting access to the rest of the app and database queries.
- Registration page creation and functionality
  Once authentication of users is implemented the ability to add new users to the database will need to be added.
- Home UI creation and page navigation
  Before application features can be implemented general user navigation will be required. This will mean design of a home page as well as having a way to navigate to application features.
- Feature 1 design.
- Feature 1 development.
- Feature 2 design.
- Feature 2 development.
- Feature 3 design.
- Feature 3 development.
- Feature 4 design.
- Feature 4 development.
  The above tasks (features 1 -4) will be the tasks that related to implementing features of the application (application ability to assist in organising teams). Features are yet to be fully designed however currently plan features include messaging between groups and individuals, interactive Gantt chart, personalised checklist of tasks and personal diaries.

The resources needed to complete the project are minimal as the project will only requires open-source software to complete and testing will only require a few different sized phones which I can source independently, or emulators could be used instead. The main resources needed to complete the project will be time and expertise's.

In the 2 semesters given to complete the project (if done independently) I can reasonably expect to have completed a useable app with minimal features (expecting 2 major features).

For Gantt chart of project refer to appendix 1

Communication

Weekly check-ins

Too update my supervisor on my progress I plan to attend open office hours or email to give updates on my project progression and address issues and concerns weekly. If unable to attend office hours an email will be sent to update the project supervisor on the project and to explain missed attendance.

In the below table are the submitted items.

Submittable	**Date**	**To**
Project proposal Draft	Semester break Semester 1	Marked by Supervisor
Project proposal	Week 7 Semester 1	Marked by Supervisor
Progress report draft	Week 11 Semester 1	Marked by Supervisor
Progress report	Week 14 Semester 1	Marked by Supervisor
Progress oral	Week 14 Semester 1	Marked by Supervisor
Project update draft	Week 3 Semester 2	Marked by Supervisor
Project update	Week 5 Semester 2	Marked by Supervisor
Final report draft	Week 11 Semester 2	Marked by Supervisor
Final report	Week 14 Semester 2	Marked by Independent Academic
Final Oral	Week 14 Semester 2	Marked by Supervisor & Marked by Independent Academic

Communication Matrix

Tool	**Purpose**	**Expected response time**
Meet with Supervisor during office hours	General discussion about project. This includes basic questions about assessments, the technical content, and resources.	n/a
Email Supervisor	Notify if unable to attend office hours or if question cannot wait for office hours meeting.	5 business days
Email: Unit Coordinator (electrical)	Discussion about lack of supervisor communication (minimum 2 incidents of no response within 5 business days)	5 business days
Email / call client	If communications to supervisor is disrupted used to discuss communication issues.	5 business days

References

2021 Apple Inc. (2021, 4 11). *Deployment Reference for iPhone and iPad*. Retrieved from Lost Mode, remote wipe and remote lock: https://support.apple.com/en-gb/guide/deployment-reference-ios/apd713df1b14/web

2021 Oracle. (2021, 4 20). *Java Platform, Standard Edition Security Developer's Guide*. Retrieved from Documentation: https://docs.oracle.com/javase/9/security/java-security-overview1.htm#JSSEC-GUID-2EF0B3B8-9F3A-41CF-A7DA-63DB52180084

A. A. Hasib and A. A. M. M. Haque. (2008). A Comparative Study of the Performance and Security Issues of AES and RSA Cryptography,. *008 Third International Conference on Convergence and Hybrid Information Technology* (pp. pp. 505-510). Busan, Korea (South): IEEE. doi:doi: 10.1109/ICCIT.2008.179.

Australian Signals Directorate. (2021, March). Australian Government Information Security Manual . Canberra, ACT, Australia .

Baihaqi, O. C. (2017). Implementation of RSA 2048-bit and AES 128-bit for Secure e-learning web-based application. *2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA)* (pp. pp. 1-5). Lombok, Indonesia: IEEE. doi:doi: 10.1109/TSSA.2017.8272903.

Commonwealth of Australia . (2018, April 2018). *ASDEFCON Technical Data and Intellectual Property.* Canberra: Capability Acquisition and Sustainment Group.

Commonwealth of Australia . (2019). *CASG Handbook (E&T) 12-2-003 V1.1.* Canberra : Capability Acquisition and Sustainment Group.

Commonwealth of Australia. (2021, 4 11). *Australian Intelligence Corps*. Retrieved from Army: https://www.army.gov.au/our-people/organisation-structure/army-corps/australian-intelligence-corps

Commonwealth of Australia. (2021, 4 21). *Privacy Act 1988.* Retrieved from Federal Register of Legislation: https://www.legislation.gov.au/Details/C2021C00139

Priyadarshini Patil, P. N. (2015). A Comprehensive Evaluation of Cryptographic Algorithms: DES,. *International Conference on Information Security & Privacy (ICISP2015). 78*, pp. 617 – 624. Nagpur, INDIA: Procedia Computer Science. doi:https://doi.org/10.1016/j.procs.2016.02.108.

Queensland University of Technology. (2021, 4 24). *C/5.3 Academic integrity*. Retrieved from Manual of Policies and Procedures: https://www.mopp.qut.edu.au/C/C_05_03.jsp

R. V. Mankar, S. I. (2013). C Implementation of SHA-256 Algorithm. *International Journal of Emerging Technology and Advanced Engineering*, pp. 167-170. Retrieved from https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.413.7088&rep=rep1&type=pdf

Wardhani, M. A. (2016). Implementation of RSA 2048-bit and AES 256-bit with digital signature for secure electronic health record application. *2016 International Seminar on Intelligent Technology and Its Applications (ISITIA),* (pp. pp. 387-392). Lombok, Indonesia, : IEEE. doi:doi: 10.1109/ISITIA.2016.7828691.

Z. Al-Odat, A. A. (2019). Randomness Analyses of the Secure Hash Algorithms, SHA-1, SHA-2 and Modified SHA. *2019 International Conference on Frontiers of Information Technology (FIT)* (pp. pp. 316-3165). Islamabad, Pakistan: IEEE. doi:doi: 10.1109/FIT47737.2019.00066.

Appendix 1 – Project Gantt Chart

Refer to excel file for easier read.