Progress Report

Progress update

build process/testing and Socket connections.

The Project consist of two applications being the user app and server. The user app was created to be a downloadable application for mobile phone and the server was created as a command line program for a desktop (however will run on any windows device). To create a socket connection, it was decided that these programs would communicate over the internet using TCP/IP (transmission control protocol/internet protocol). TCP was chosen due to it being a standardised protocol that governs communications among computers on the internet that is used on every device connected to the internet. Note that port 12345 was selected to be used for the sever, this port was selected as it is used for nothing that a dedicated sever would use. An unused port was selected to prevent other programs from congesting the sever program.

Once a simple program that could both send and receive messages was created a method to compile the written program was needed. The open-source software Gradle was selected to compile code for both server and user apps. Gradle was chosen due to it being the compiler recommended by android and because it is available on nearly all ide's (integrated developer environment).

After a rudimentary server and mobile app could be compiled several mobile phone emulators with different sized screens were downloaded from android to use for testing the mobile app (used to check if GUI would work on all sized screens) during this time a physical phone was also sourced to use for testing. Also, during this time debugging tools where explored.

Encryption and key exchange

Army and defence have high encryption standards and it was decided that a security level of top secret would be aim for. For general encryption AES-256 would be used however due to AES being a symmetrical encryption algorithm meaning the same secret key is used to encrypt and decrypt messages. A method of exchanging keys was needed which was an asymmetrical encryption algorithm meaning the keys are different for encryption and decryption. RSA with a key size of 3072 bit was selected. Note that RSA was not used for general message encryption due to its high encryption and decryption times and RSA is also easier to crack the longer the message. AES does not share these disadvantages. At this point both programs where able to exchange keys and communicate fully encrypted however do note that message encryption is not user authentication. Encryption prevents the ability to listen or intercept messages between 2 parties.

Multi-threaded server

At this point the server could only handle one user at a time, to allow multiple users the sever was redesigned to create a new tread per connection to it (allow programs to execute code in parallel). This also had the benefit of creating a unique encryption key per user app connections.

Login functionality

The first thing after the programs were communicating fully encrypted was the ability to authenticate what the sever was communicating with, which was done in the form of a login page. To do this a rudimentary database was created to store username and passwords and sever connection to said database was tested as well as the ability to query the database (how to get and change information on the database from the sever program). A login page for the user app was also

created to allow users to send inputted information over to the sever then check it against the record in its database and send a response back to the user app. After this login functionality was implemented. A visual of the login page can be seen in figure 1 below.

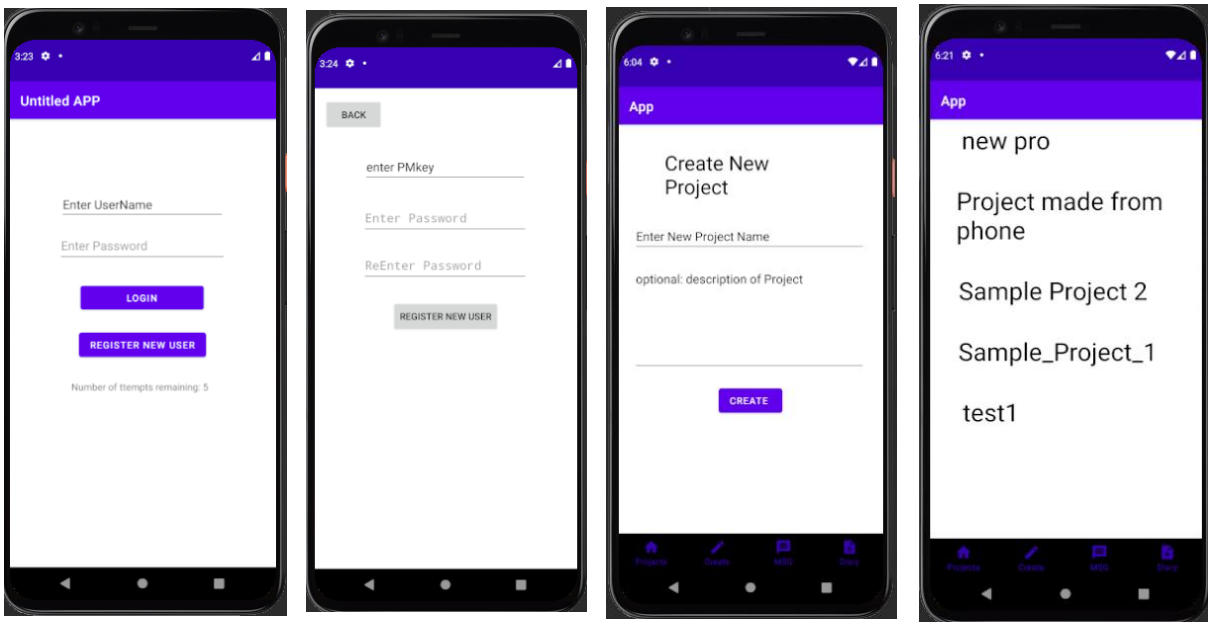

Figure 1: From left to right - Login Page Figure, Registration Page, Create New Project Page, Projects Page

User registration

A page to register new users to the database was created, this worked the same way as the login page except it will add information to the database instead of authenticating a user. If/when this app is implemented the server should probability have some way of authenticating new users such as checking pmkeys or needing a defence email to add a new user to simply prevent non-defence personnel from even accessing the network. Currently program just excepts all new entries if username is not already in database. A visual of the registration page can be seen in figure 2 below.

SHA encryption

Storing passwords and other identifying information in plain text on severs would allow anyone with database access to looked at user's information, to prevent this a one-way encryption is used on this sort of information. The encryption algorithm of SHA with 384-bit output with salting (a key is used during encryption) was used as recommended by defence for information up to top secret.

Home UI skeleton

Once a user has been authenticated by the sever the user app will enter its main navigation area. It was decided to use a bottom navigation bar with four possible displays being a projects page, create project page, messages, and diary tabs to navigate to the future planed feature of the app. At this point each of the displays where empty/had placeholding images.

Database design

The database in its current form would not be capable of storing the necessary information needed to represent a user's work-project. At this point creating some functionality to end users was being

planned out and the database needed to go through a redesign to represent the information needed for a user's work project.

Create project page.

Once the database was redesigned a way to allow users to store information was needed. Under the create new project tab from the bottom navigation option a create new projects page was created seen in figure 3. This page functioned like the registration page as it would send information to the sever to be stored.

Project Selection page.

The project selection page is the tab of the bottom navigation options that a user will be sent to after login. This page displays each project the user is connected to (as indicated by the server) and can be scrolled through. The plan is to make each of these projects a button which will send the user to a projects individual information page however this is not yet implemented.

Provide Update of achievements using Milestones.

Project progress can be seen in the table below.

The first milestone that was completed was the Client to Server Database encrypted communication, these entailed the ability for the client and server to communicate over the internet using AES-256 encryption algorithm and to exchange the AES secret keys securely using RSA key exchange algorithm this will allow the two programs to communicate securely.

The second milestone that was complete was the user authentication / login. This included creating a database for the sever and the ability to interact with it and a login page for the client app. This milestone would allow a user to authenticate themselves from the user app. This milestone showed the ability to read information from the database from client apps.

The next completed milestone was user registration this would allow user to create an identity for themselves when interacting with the server. This showed the ability to upload information to the server.

The milestone Home ui design / app navigation design is complete this milestone creates the sections in the user app that act as placeholders for future works or the planned features in its current state basic app navigation is achieved with placeholders for future features.

Milestone Feature 1 – team organiser has just been started and is 10% complete. Currently database has been updated to allow work project information to be stored and user apps are able to create new projects and upload them to the server/database.

Milestones / deliverables	**Progress**
Development Milestones	
Client to Server Database encrypted communication	100% completed

User authentication / login	100% completed
User registration	100% completed
Home ui design / app navigation design	100% completed
Feature 1 – team organiser	10% completed
Feature 2 – group and individual messaging	0% completed
Feature 3 – personalised check list	0% completed
Feature 4 – team message board	0% completed

Identify any changes to Milestones.

No changes to milestones

Risk identification and assessment

As this project will be a software driven project there will be no physical risks to associated with this project.

The client or risks to army associated with this project will include the overall quality of work and time constraints put on the project. As the client will be giving projects to students it is likely that their ability due to inexperience or lack of knowledge may result in producing a lower work/project quality.

As students will likely have other study to complete and a year to complete their projects it is likely that project taken by student will take far longer duration to complete due to other study commitments and for longer projects assigning new student to continue ongoing projects that last more than a year will also increase duration of projects. The client could also have a cost risk however this project will not require funding to complete.

The risks to QUT associated with this project include QUT's reputations and its relationship with the client. As QUT is the organisation that provides students to work on projects their behaviour will impact QUT's reputation and image. Negative behaviour from student could impact relations with army and this could impact acquiring new clients or put in to question existing client relations. The risks to students associated with this project will include their own reputation with a potential employer. If students create a negative relationship with the client this reputation will likely extend pass the project.

The risks to the project supervisor associated with this project will include their reputation toward both the client and QUT this is because as project supervisor student conduct and performance is their responsibility.

Sustainability statement

For the goal of not exceeding the limits of regeneration the project will only require energy and hardware such as phones and computers to remain operational. The hardware devices can be recycled and rebuilt indefinitely.

The energy required to maintain these programs will be dependent on public power sources which may not be renewable however the power to run the devices required is small and similar hardware have been used for similar purposes showing this is an acceptable price to pay for enduring asset value.

The goal of considering longevity, component re-use, repair, and recyclability the software for this project has been developed using an agile approach meaning it is written in a way to allow continuous improvement and may be repurposed/improved when and if ever required from clients, this should also increase the longevity of the project.

The goal of having proactive and integrated solutions can not be achieve in all cases for this project however some reactive solutions cannot be achieved as the project is vulnerable to sever issues as client app are dependent on the sever running to remain operational. If the server is down for maintenance or is forced offline from natural events such as fires or earthquakes the client apps will not work which may impede user work projects if users are not notified of the issue. To limit the damage these events may cause sever data will need to be backed up regularly and stored offsite. With this data a new sever could quickly be restabilised and client app could be given the new IP address in the form of an update.

Being a majority software driven project there is no waste and will not release of any substances into the environment associated with this project. Note that power supply may release substances into the environment.

Where scientific information is inconclusive, or incomplete, the precautionary principle and risk management practices should be applied to ensure irreversible negative consequences are avoided cannot always be achieved as it is unlikely however possible that 1 of if not all the encryption algorithms used to secure communication and encrypt information could be broken in the future. This would be a major issue with irreversible consequences including loss of user information and work project information. If it is known that an encryption algorithm has been broken, then a different unbroken algorithm can be used to replace the previously used one. If it is unknown, then there is no way of even knowing messages between the user apps and server are at risk and the project is vulnerable to both man in the middle and observation from attackers. This is an issue that cannot be prepared for however do note that the encryption algorithms used have not been broken for decades.

Ethics Statement

Engineers Australia Code of ethics has four principles or values that engineer much adhere to while practicing engineering these being to demonstrate integrity, practice competently, exercise leadership and to Promote sustainability.

The project has been able to demonstrate integrity by following the guidelines set by engineers Australia. The project has been able to achieve the goal of acting on a well-informed conscience as the project will be mostly implemented by programming a skill that is closely tied to majoring in computer and software systems where all people assigned to this project are majoring in. For the goal of being honest and trustworthy is being address as where idea or processes are being replicated to achieve objectives within the project, the project proposal was used to detail and explain design decisions and reasoning and cite/reference works where this information was being taken from. To further ensure honesty the online resource of GitHub is being used to keep track of individual developer contribution to the project to ensure contributions are being recorded. Regarding fraudulent, corrupt, or criminal conduct as a QUT student the student code of conduct will apply and act a source of consequence for misconduct.

The project has been able to practise competently by following the guidelines set by engineers Australia. As previously stated, the project will be mostly implemented by programming a skill that is closely tied to majoring in computer and software systems where all people assigned to this project are majoring in allowing developers to stay in their area of expertise. This will achieve the goal that members will represent areas of competence objectively. For the goal of maintaining and developing knowledge and skills and to ensure that the project will act based on adequate knowledge is being address as the design decision made are following current trends and practices are found by conducting a literature review during the project proposal to explore and determine if new skills or knowledge where required to complete this project.

The project has been able to exercise leadership by following the guidelines set by engineers Australia. The goal of making a reasonable effort to communicate honestly and effectively to all stakeholders is addressed by creating and adhering to a communication plan which demonstrates a reasonable attempt to communicate honestly and effectively to the project supervisor. Attempts to keep army informed on project progress has been done in the form of emails.

The project has been able to promote sustainability by following the guidelines set by engineers Australia. For the goal of engage responsibly with the community and other stakeholders will be addressed by addressing both user and client concerns have been taken into consideration for this project the main example of responsiveness of the application with security (will usually make an app less responsive). For the goal of practising engineering to foster the health, safety and wellbeing of the community and the environment, the project has taken into consideration the safety and wellbeing of user by ensuring that the project will take appropriate action to protect and handle user data. To balance the needs of the present with the needs of the future the encryption and key exchange algorithms used have a long history of effectiveness as well as user data is only taken when needed.

Adherence to communication plan

In my communication plan I planned to attend open offices hours that my supervisor had set up weekly to discuss issues and give updates on the progress of the project and I have been able to attend a meeting each week. No issues have arisen which would require me to enact any higher levels of communication as indicated by the communication matrix in the project proposal.