Project Proposal

**WhisPeerer – a WebRTC messaging application**

05/01/2016

Dominic Rathbone

Student number: 12843140

CI360 – Mobile Application Development

School of Computing, Engineering and Mathematics

# Summary

My android application will allow two users to message as well as voice and video chat directly with each other without the need for an intermediary server. To do so, my application will use WebRTC, a new technology aimed to provide peer-to-peer connectivity to the web. By avoiding the need for an intermediary server, it provides a service with greater anonymity and security which a lot of people find important in an age where online privacy has become such a concern.

# Rationale

On a shallow level, my android application aims to provide a free service to users who want to to message as well as video and audio chat with each other over Wi-Fi.

However, it is also being created to provide a method of communication and data exchange that avoids the inherent data privacy and security issues associated with client-server architectures due to the trust being placed on the providers running these applications and services to securely store your data. These problems are growing larger in the domain of mobile applications as many deploy a server based infrastructure to take the stress of data processing away from client devices and this is shown by the current OWASP (Open Web Application Security Project) top 10 mobile security concerns with the first on list is “Weak server side controls” [1].

These issues have become more apparent in the mainstream media in recent years with consumer's application data not only being susceptible to these illegal and unethical attacks [2] but also becoming susceptible to legal, intentional access with bills such as the “Investigatory Powers Bill” being drafted by the UK government which aims to force mobile and internet service providers to be able to decrypt user's data on request [3].

In this case, my application also serves users who are becoming more aware of these issues and want to avoid the possibility of third parties inappropriately using the data being stored on their servers.

# Application

At the moment, the largest messaging platforms such as WhatsApp and Facebook Messenger both provide mobile applications for their services. From a normal user's perspective, it is hard to criticise these two applications as they have a great user interface and range of functionality, this being shown by their user bases of 900 million [4] and 700 million [5] respectively. However, they are liable to criticism from a technical perspective.

Although WhatsApp has implemented VoIP functionality through a library called PJSIP, it is not as advanced as WebRTC in terms of protocolling and technologies used [6]. On top of this, the majority of it's functionality is based on a client-server architecture which, again, is vulnerable to the issues previously described with WhatsApp even being a target of a proposed ban by the government for their use of strong data encryption protocols [7].

In contrast to this, Facebook Messenger has implemented WebRTC for it's mobile video and voice calling early on in 2015. Although this is a good example of how WebRTC can be applied, Facebook Messenger has a security flaw in it's implementation in that it uses SDES (Session Description Protocol Security Descriptions) encryption instead of DTLS (Datagram Transport Layer Security) which is the standard encryption scheme for WebRTC. The problem with this is “the encryption keys are sent via the signaling servers and can be used to retroactively decrypt traffic.”[8]. This would mean that for example, this service would be liable to access by the government in the case that the “Investigatory Powers Bill” is passed even though it is using technology which should avoid this.

One application that provides an alternative to these applications is Sicher which aims to provide a free instant messaging service that is encrypted end-to-end. From their FAQ, it states it uses “point-to-point encryption, based on asymmetric cryptography. It means that only the recipient who owns the private key can decrypt the message. RSA cryptosystem is used with 2048 bit keys. Additionally all data exchange between mobile apps and Sicher servers is protected using SSL.”[9] to achieve this. Although, it does exchange this encrypted data through a server, it attempts to reduce the risk of this by immediately deleting this data off their servers as soon as the recipient receives it [10]. However, the level of encryption that it bases it's product on could suffer if the “Investigatory Powers Bill” was passed and they were forced to downgrade. Another criticism of mine is that the user interface is relatively immature and it has only been designed for use with a mobile phone as opposed to larger devices such as tablets.

A criticism of all of these applications is that they lack transparency in terms of their source code due to the fact that they are proprietary. By using an application that is open source, the level of transparency almost guarantees that there is very little room for inappropriate usage of the data that goes through it e.g. for marketing. One messaging application like this is ChatSecure. An application that aims to provides symmetric OTR (off the record) encryption, which is a method of encryption specific to real time messaging, this works by using a new key for each and every message sent by an application.

My application would provide an alternative to traditional instant messaging applications such as these by completely basing it around the WebRTC (Web Real Time Communication) native API for Android. This API allows the an instance of the application to form a peer to peer connection with another instance to directly exchange data over. From the user's perspective, this connection gives them the ability to stream data such as text, video and audio to and from one another. By using this alternative architecture, it avoids the data passing through a third party server and avoids the security and privacy issues associated with third party client-server applications mentioned previously.

# Scenario of use

A use case for my application would be someone (referred to as user A) who wants to communicate with their friend (referred to as user B) privately. They would open up the application and enter a temporary name to identify themselves by. From the application, they would then share this name with user B by email (amongst the various other forms of sharing my application would implement e.g. text, Facebook). After user B receives this email, user B would go to the application, click “join chat” and enter user A's name, sending a chat offer to User A. This would trigger a notification on user A's application with their offer, once user A has accepted the offer, they enter a new chat room and either of them could either trigger a video/voice chat or just send plain text messages to each other. After they are done and the users would disconnect from the room and it would be disposed.

# Technical overview

The basis of the application will be LibJingle, a C++ library that implements the W3C WebRTC API definition that can be compiled for use with Android, for this application, a precompiled version will be used. In order for a connection to be formed between two applications, it uses an architecture called JSEP (JavaScript Session Establishment Protocol). However, in our case with the LibJingle library, the browser would be replaced by our Android client.

As you can see in the diagram, the applications needs a method of signalling to establish a session, normally a server but this is purposefully left up to the developer in order to allow them to to fit WebRTC into their current architecture. In our case, the method of signalling will be via a Node.js server. This signalling server is used to exchange client meta data in order to establish the session and will not touch any of the data sent via the peer-to-peer connection. To do this, this server needs to use a communications protocol that can send data bi-directionally such as WebSockets. To implement WebSockets, the Socket.io library for Node.js will be used.

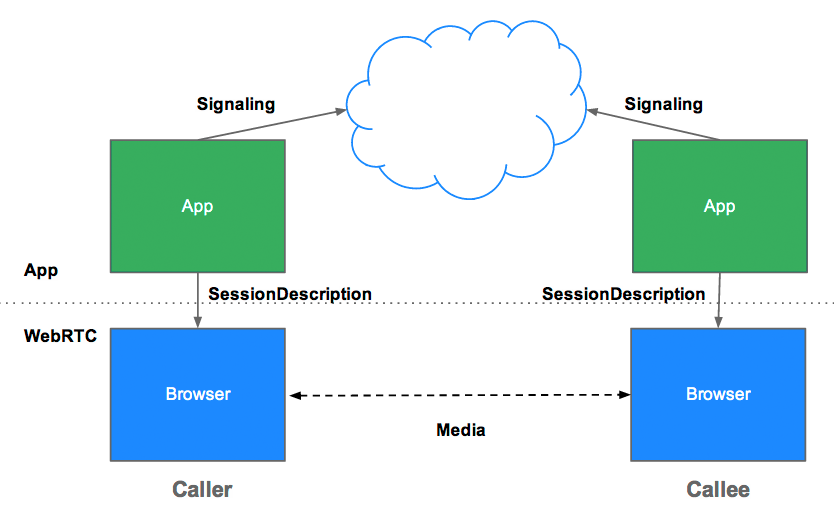
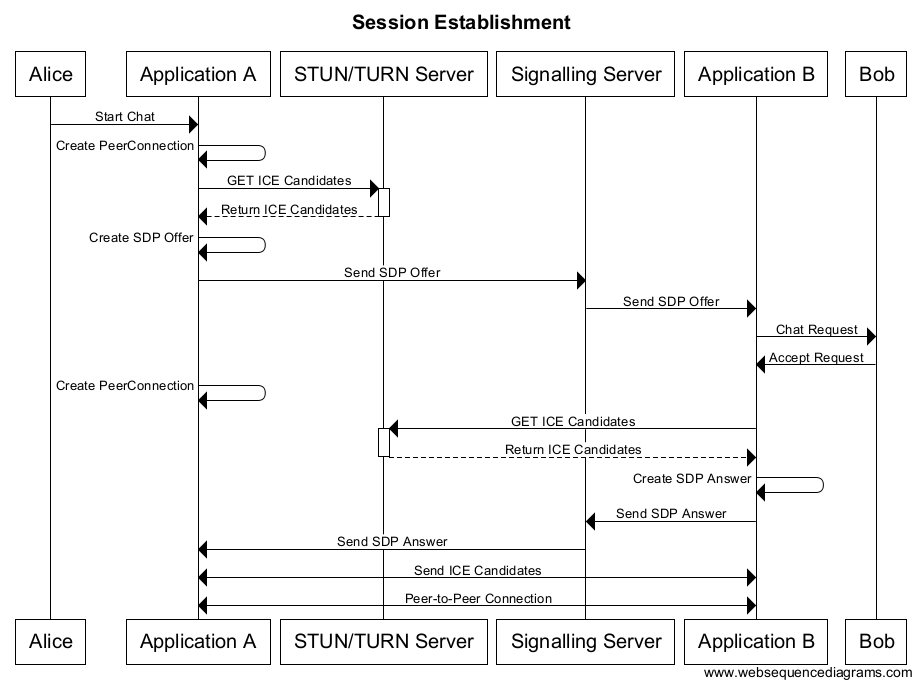


Figure 1: Justin Uberti. (2011). Javascript Session Establishment Protocol (JSEP).Available: https://lists.w3.org/Archives/Public/public-webrtc/2012Jan/att-0002/JavascriptSessionEstablishmentProtocol.pdf. Last accessed 09/01/2016.

To model the body of the messages exchanged during session establishment, SDP (Session Description Protocol) is used. The flow of session establishment is as follows:

Before everything, a PeerConnectionFactory object is instantiated, this will represent the connection between the two applications and from it, streams can be added, offers and answers can be created and various other things can be achieved. The offer and the answer contain meta data such as the media streams that have been added to it, a list of media constraints that describe what they have allowed access to (e.g. video & audio sources) as well as a list of ICE Candidates that have been retrieved before the offer was sent. ICE (Interactive Connectivity Establishment) candidates are a list of IP addresses and ports that the offer is potentially being sent from, once these have been exchanged, the application will attempt to form a connection with each of these until it finds one that works. This is a technique that allows the application to avoid issues caused by network address translation. It gets these candidates by hitting an external server (STUN or TURN) that returns the client's external IP back to themselves. As this process is asynchronous, the applications can send new ICE candidates to each other after the offer or answer has been sent, in the case the callback was not triggered before they were sent. For our application, we will use Google's public STUN server to retrieve potential candidates as it is free and reliable.

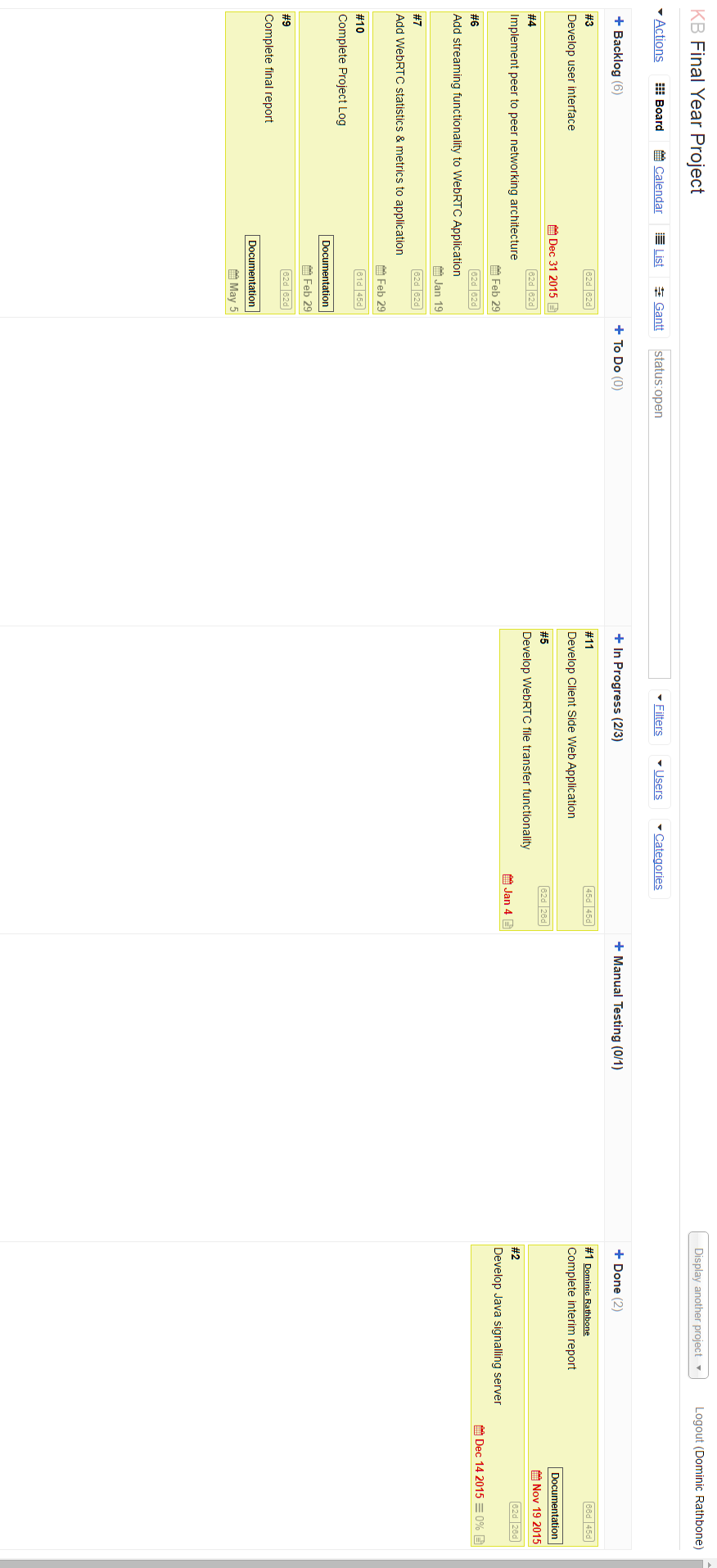
To get video streams from the camera, the API has a class called “VideoCapturerAndroid” that acts as a wrapper for the camera functionality on your phone, allowing the application to retrieve the camera input as a stream that can be added to the PeerConnectionFactory object. To do this, once a VideoCapturerAndroid object has been instantiated, you can instantiate a VideoSource or AudioSource object with the capturer as a parameter and then create a MediaStream object. To this MediaStream, the VideoSource and AudioSource can then be added. The source and stream objects are all created using PeerConnectionFactory methods. To output this video, the API again provides a class to do so called “VideoRendererGui” that uses OpenGL to render the stream to a view.

# Technical challenges

The main technical challenge will be getting to grips with the WebRTC Native API for Android as it is a change from how I have worked with it before as a JavaScript API where it seems to be a lot more mature as a technology. Another problem I've found is sending data over WebRTC that isn't in the form of a stream is normally handled by the DataChannel API. However, I am struggling to find any documentation on this and it might not have been implemented yet, in this case I will have a challenge finding a solution for plain text messaging between two peers. On top of this, I am not familiar with OpenGL or video rendering techniques so handling this in conjunction with remote streaming might be complicated.

# Work plan

To develop the project, I will use a methodology called Kanban. This focuses on using a task board to complete work iteratively. This work is tasked up before the project starts and belongs to a queue until it is pulled into the work flow, at this point it goes through an iteration of development, testing and stakeholder approval. This approach avoids the pitfalls of sequential approaches such as waterfall as each iteration through the work flow is relatively small and it is easy to reiterate through a step if it fails at some point whereas in waterfall, each step in the work flow takes months to complete and would cause a major delay if the work didn't meet stakeholder approval. It also avoids overloading developers with too much work as it uses a WIP (work-in-progress) limit, indicating how many tasks they should have in the workflow at one time meaning the work will be to a higher quality. The kanban board is a big part of this process as it allows all the stakeholders of the team to visualise where the project is at in it's timeline, for my board I will use “Kanboard”, a free and open source web application that I have hosted on an Amazon Web Services server instance. I have been using this approach with this board in particular for my Final Year Project and it has been working very well.



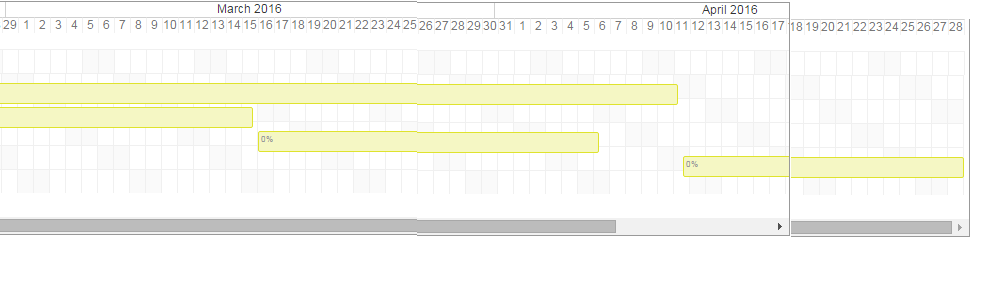
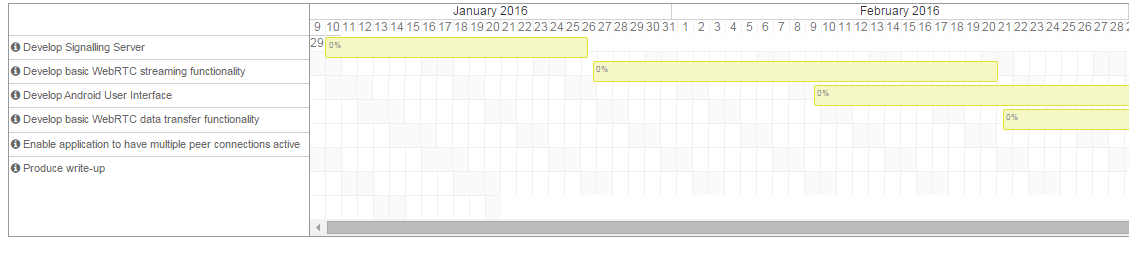
For my development workflow, I will use a test-driven development methodology for the application logic in order to produce code that I know will work. This methodology focuses on writing unit tests first and writing the code to make the tests pass in order to produce clean code that will work. This can be represented by a traffic light system:

Once code has gone through this development process , it then goes to a manual testing phase in which I will test it from a user's perspective in order to make sure the flow throughout the application works and actually makes sense.

My application will be split up into several tasks but overall, there will be 4 deliverables, three end products and one intermediate. The first will be the Node.Js signalling server as it needs to be completed to allow my application to form a connection between two applications. The intermediate product will be the bare bones application with working WebRTC streaming functionality, with this eventually becoming the second end product at which point it will have a fully developed user interface. The last product will be the write-up of my project, detailing how the project went.

# Project Estimation

As an initial estimate for my project, I have produced a gantt chart:



(Please, note: if the images are too small, there is a gantt chart within the zip file, along with larger version of all the images in this document).

# Ethical considerations

Discuss any ethical considerations related to the project or the application you develop. With respect to the application, think about privacy, data protection, health and safety or any moral implications. With respect to the development project, think about the involvement of users in your requirements analysis and testing. (max. 200 words)

# Resources

List the resources you need to carry out the project, including access to specific hardware (e.g. smartphone), software (e.g. development environment), data sets, online services, organisations, people, etc. (up to 200 words).

# UI design draft



# 

# References

[1] OWASP. (2014). *OWASP Mobile Security Project - Top Ten Mobile Risks.*Available: https://www.owasp.org/index.php/Mobile\_Top\_10\_2014-M1. Last accessed 06/01/2016.

[2] William Enck, Damien Octeau, Patrick McDaniel, and Swarat Chaudhuri. (N/A). *A Study of Android Application Security.* Available: http://www.cs.rice.edu/~sc40/pubs/enck-sec11.pdf. Last accessed 06/01/2016.

[3] Home Office. (2015). *Draft Investigatory Powers Bill.* Available: https://www.gov.uk/government/publications/draft-investigatory-powers-bill. Last accessed 06/01/2016.

[4] Leo Sun. (2015). *Facebook Inc.'s WhatsApp Hits 900 Million Users: What Now?.*Available: http://www.fool.com/investing/general/2015/09/11/facebook-incs-whatsapp-hits-900-million-users-what.aspx. Last accessed 06/01/2016.

[5] Alexei Oreskovic. (2015). *Facebook Messenger added 100 million users in the last three months.* Available: http://uk.businessinsider.com/facebook-messenger-has-700-million-users-2015-6?r=US&IR=T. Last accessed 06/01/2016.

[6] Philipp Hancke. (2015). *What’s up with WhatsApp and WebRTC?.* Available: https://webrtchacks.com/whats-up-with-whatsapp-and-webrtc/. Last accessed 06/01/2016.

[7] Rory Cellan-Jones. (2015). *Does the government really want to ban WhatsApp, iMessage and Skype?.* Available: http://www.bbc.co.uk/news/technology-33737813. Last accessed 06/01/2016.

[8] Philipp Hancke. (2015). *MESSENGER EXPOSED: Investigative Report.* Available: https://cdn.andyet.com/webrtc-reports/messenger-report.pdf. Last accessed 06/01/2016.

[9] N/A. (N/A). *Sicher FAQ.* Available: http://www.shape.ag/en/faq/sections/sicher.php#why-is-sicher-secure. Last accessed 06/01/2016.

[10] N/A. (N/A). *Sicher Privacy Policy.* Available: http://www.shape.ag/en/privacy/sicher/. Last accessed 06/01/2016.