**Project Proposal for Computer and Network Security**

**A Secure Image Repository**

March 6, 2017

Team Members: Riccardo Gulia, Terry Griffin, SrividyaKuppa VenkataNaga, Bharadwaj Nallavelli, Bill Stronge

Our proposal is to create a client/server application that provides a secure image repository. This application allows authorized users to securely upload and download images to/from the repository. The uploaded images are signed so that they are associated with the person who uploaded them. The signing can help resolve copy right issues, both in helping to identify who owns an image and to identify anyone who tries to take credit for someone else’s images. In addition to uploading, authorized users may download images. The downloaded images are accompanied by an authentication which can be used to verify the image and identify the person who uploaded it. Each upload and download is tracked in a transaction log with the name of the image and the user who uploaded or downloaded it. This transaction log can be used for purposes like billing.

An example of someone who might use such an application is TMZ. They could authorize their Paparazzi photographers to upload their images of Angelina Jolie and Brad Pitt to the secure image repository. The Paparazzi would know that each image they uploaded would be owned by them and they could get an accounting of who downloaded each of their images.

This proposal satisfies the networking requirement because it is a client/server application. The security requirements are satisfied by:

1. User authentication at the server using Public Key Certificates
2. The use of public key/private keys to agree on a session key for the image uploads and downloads
3. Encrypting/Decrypting the image uploads and downloads
4. Using HMAC to sign the image downloads so that the downloader can know who is the image owner.