Distributed Systems
COMP90015 2016 SM1
Project 2

Project 2

The project involves building on Project 1. If you have not satisfactorily completed Project 1 then you'll need to work with your tutor and lecturer to catch up.

You are required to:

- Implement a security policy and mechanism as discussed next.
- Choose another distributed systems challenge where you believe the existing system can be significantly improved and implement an extension to the existing system that addresses this challenge.

For the security aspect you may make use of certificates, secure sockets, public/private keys and/or shared session keys depending on your approach.

You may need to read through the documentation provided by Oracle or elsewhere to see specific details on the API for working with public/private keys and other cryptographic functions.

Security Policy

Modify your system to implement the following:

- Communication between clients and the server should be secure.
- Communication between servers should be secure.

Working with Cryptographic Functions

DO NOT UNDERESTIMATE THE DIFFICULTIES OF WORKING WITH CRYPTOGRAPHIC FUNCTIONS.

Consider the fundamental operations that you may need to implement:

- secure socket layer
- generating a public/private key
- reading/writing keys from/to a file
- generating a shared key for encryption
- encrypting and decrypting data
- encoding encrypted data for transport

If you intend to use these things, develop and test your own wrapper classes that can do each of these things. Then when they are working, build them into your Chat program.

Backwards compatibility

- Backward's compatibility is a requirement. Your improved system should still work with existing system, however of course connections to exisiting system components will not be secure and may not support improved features.

Technical aspects

- Your programs should start from the command line just as they did in the first project.
- Any additional files that you need, e.g. certificates, should be embedded into the JAR file, rather than being read from the computer's file system.

Report

Your report should detail all aspects of your security implementation. Discuss the technology that you use and explain how it achieves the security objectives of the project. Discuss any limitations or additional benefits that the technology provides.

Provide details of the changes to your existing protocol. Details should be explicit enough such that a third party could implement the features in their own system to be compatible with your own.

You should submit your report plus your modified system; instructions will be given on LMS.

The due date is Friday Week 12, 27th May, 11:59pm.