QUEEN’S UNIVERSITY OF BELFAST COMPUTER SCIENCE

Minute of Project Supervision Meeting

======================================

Student Name: Anurag Rath

Project Module Code: IGR06

Project Supervisor: Indranil Ghosh Ray

Meeting Number: 01

Date of Meeting: 14/10/2022

Progress since in the meeting, and decisions arrived at during meeting:

======================================

In the first meeting we discussed about cryptographic basics like groups and finite fields, Supervisor advised to learn the basics.

Action Points:

==============

Learning Basics.

Getting familiar with concepts.

Date of next meeting: 28/10/2022

====================+

Meeting Number: 02

Date of Meeting: 28/10/2022

Progress since in the meeting, and decisions arrived at during meeting:

======================================

In this meeting cryptographic basics like groups and finite fields discussed in detail after Supervisor advised to learn the basics and introduction to key exchange in terms of mathematical computation. Initial project plan discussed

Action Points:

==============

Getting familiar with concepts taught in the 1st and 2nd orientation.

Date of next meeting: 08/11/2022

====================+

Meeting Number: 03

Date of Meeting: 08/11/2022

Progress since in the meeting, and decisions arrived at during meeting:

======================================

Finished familiarising with basic cryptographic concepts necessary for the project. Key exchange protocol and password authentication key exchange protocol discussed and explained.

Action Points:

==============

Key exchange.

Password.

Attacks.

Mitigation ideas.

Date of next meeting: 09/12/2022

====================+

Meeting Number: 04

Date of Meeting: 09/12/2022

Progress since in the meeting, and decisions arrived at during meeting:

======================================

Complete understanding of key exchange protocol. A code explaining the concepts of key exchange and providing ideas for implementation in java.

Action Points:

==============

Implementation ideas

Strengthening learnt concepts

Practical implementation

Date of next meeting: 04/01/2023

====================+

Meeting Number: 05

Date of Meeting: 04/01/2023

Progress since in the meeting, and decisions arrived at during meeting:

======================================

Updates on the system implementation and discussed solution to problems occurred. filesystem to use for system communication, what security concerns could it entail.

Action Points:

==============

Problem solving

Updated implementation

Multi-threading

Date of next meeting: 11/01/2023

====================+

Meeting Number: 06

Date of Meeting: 11/01/2023

Progress since in the meeting, and decisions arrived at during meeting:

======================================

Interim demo presented. Updated work plan discussed. Updated system demonstrated. Code explained.

Action Points:

==============

New implementations ideas

Updated implementation

Date of next meeting: 21/02/2023

Meeting Number: 07

Date of Meeting: 21/02/2023

Progress since in the meeting, and decisions arrived at during meeting:

======================================

Updates on works on updated system discussed in the interim demo. AES encryption added on file systems. Structure of dissertation and approach discussed.

Action Points:

==============

AES implemented.

Dissertation structure

Date of next meeting: 11/03/2023

Meeting Number: 08

Date of Meeting: 11/03/2023

Progress since in the meeting, and decisions arrived at during meeting:

======================================

first draft of dissertation on basis of the structure discussed and reviewed.

Action Points:

==============

first draft

Dissertation content

Date of next meeting: 04/04/2023

Meeting Number: 09

Date of Meeting: 04/04/2023

Progress since in the meeting, and decisions arrived at during meeting:

======================================

Final draft presented, comments on the final draft and discussed on key points for improvement.

Action Points:

==============

Pointers for improvement

Final draft

Date of next meeting: 10/04/2023

Meeting Number: 10

Date of Meeting: 10/04/2023

Progress since in the meeting, and decisions arrived at during meeting:

======================================

Improvements on basis of the pointers finished and final draft ready for submission.

Action Points:

==============

Pointers for improvement completed.

Final draft

Date of next meeting: n/a

Agreed minute should be initialled by the supervisor.

Supervisor's Initials: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date: \_14/04/2023\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Supervisor's Comments:

=======================