A DECENTRALISED PUBLIC KEY INFRASTRUCTURE AND MESSAGING SYSTEM.

HENRY MORTIMER

1 AIMS AND OBJECTIVES

1.1 Aims

To learn more about networking, more specifically peer to peer networks and improve my knowledge of public key cryptography, key exchange and key signing protocols. Use this knwoledge to produce a better way to distribute public keys.

1.2 Objectives

1. Review information on peer to peer protocols such as "chord" and current strategies for exchanging and signing public keys
2. Build a peer to peer network.
   a) It must allow peers to quickly discover each other.
   b) It must allow peers to exchange messages.
3. Implement a key signing and exchange system based on the GPG web of trust.
   a) It must facilitate peers signing keys for other peers.
   b) It must allow peers to lookup keys using some identifier (e.g email).
   c) Peers should be able to make some effort to mark key as invlaid.
4. Create a simple messaging system that uses the network to encrypt and sign messages.
   a) Should work seamlessly i.e messages are automatically encyrpted, sign decrypted etc without interaction from the user.
5. Evaluate the network based on properties such as speed of key lookup and authenticity of results.

2 DELIVERABLES

1. A protocol specification for the key exchange and signing system

2. A simple messaging system or plugin for an existing message system that implements the protocol as a proof of concept
3. A report detailing testing of the system and reviewing the results and performance of the system.

3 WORK PLAN

- Project start to end October (4 weeks). Research peer to peer networks and public key infrastructure. Produce a list of resources for reference during the next stages.
- Mid-October to mid-November (4 weeks). Refine your requirements and start the initial iteration(s).
- November (16 weeks) to mid February. Work through Iterations.
    1. Produce initial simple peer to peer system prototype to test setting up connections between various vertual machines.(1 week)
    2. Implement peer to peer protocol in full.(5 weeks)
    3. Integrate key insertion and lookup methods into protocol.(4 weeks)
    4. Implement messaging application or plugin.(4 weeks)
    5. Test and review functionality and performance of the protocol and application.(2 weeks)
- Mid-February to end of March (6 weeks). Work on Final Report