Proposal:Secure Chat Messages Via Unstructured Peer-To-Peer Networks

Jan H. Knudsen (20092926) Roland L. Pedersen (20092817)
Kris V. Ebbesen (20094539)

April 7, 2014

1 Use Case

When one wants to talk about democracy, Chinese cartoons, or other sensitive subjects, one might wish to ensure a certain amount of privacy.

Imagine a North Korean human rights activist group wishing to coordinate their efforts in a fight for freedom. Government agencies are monitoring traffic, and might even try to find dissidents based on who they are communicating with. What these freedom fighters need, is a way of communication that is secure not only in terms of content, but disguises sender and receiver as well.

We wish to build a chat client that does just that. No silly signed emails or cleverly disguised letter pigeons, but instead a chat client that works just as easily as a normal IM-client.

2 The How And Why Of P2P

In the proposed project, we wish to use an unstructured P2P network to send messages between computers, in a way that makes it difficult, if not impossible, to determine sender, receiver and content. Unstructured networks have a great deal of usefulness in this, since they require very little routing information, and often ensure that every member of the network receive a message, without them showing any specific interest in its content.

Also, a peer-to-peer chat application does not allow a single server to be controlled and monitored by outside attackers, and with enough traffic, it will be quite difficult to pinpoint any one user as an interesting target.

3 Architecture

We will be using our original network from the P2PN course as the underlying unstructured network, since it already provides us with a suitable structure for

sending and receiving messages between peers, and for balancing the network around stronger peers.

We will be extending it with new methods to forward messages across the network, both by flooding and k-walker, without them being related to searches, and try to implement features from other security-based networks, though we acknowledge that the system itself will be proof-of-concept.

For safe encryption, we will use RSA key pairs. How they are distributed will most likely not be part of the network.

4 Rough Milestones

Week 1-2 Implement simple sending of messages, by flooding, encrypted by RSA.

Week 2-3 Implement acknowledgements, signing of messages.

Week 3-4 Implement delivery by k-walkers

Week 4-6 Try out cover traffic, proof of work, optimized delivery.