sCHAT: A SECURE CHAT APPLICATION BASED ON PURE PEER-TO-PEER ARCHITECTURE

MOHAMAD AFENDEE MOHAMED, MOHD NORDIN ABDUL RAHMAN, SYADIAH NOR WAN SHAMSUDDIN

Faculty Of Informatics and Computing,
Universiti Sultan Zainal Abidin (UniSZA), Malaysia.
mafendee@unisza.edu.my

ABSTRACT

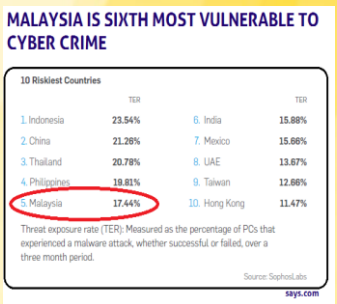
Chat application is increasingly used as an alternative to older communication technologies such as telephony and telegraph. Equipped with advanced features, people can use it for education, business and socialize. Basic requirement for chatting is an ability to exchange text messages, however, recent releases include support for audio and video communications. For some reasons, peer-to-peer now turned out to be a popular architecture and as such, it becomes a choice for developing chat applications such as Skype. Skype however, makes use of centralized server for user registration, login and buddy list. Indeed, this idea could be disastrous in the event of a compromise. In this project, we developed a chat application based on pure peer-to-peer architecture that totally rid of centralized or third party elements. The system security is autonomously managed by the communicating parties. Users have their own database for peer's profiles and they authenticate among each other before exchanging messages. The main contribution of this project is a state-of-the-art chat application having completely been designed with build in security measures. By redesigning the encryption algorithms and protocols and the interface, this concept can be extended for securing communications among government agencies such as the military and police departments.

OBJECTIVES

✓To produce a highly secure chat application for the use of government, commercial and individual entities.

✓To autonomously allow communication parties taking complete control over communication channel and avoid any third party involvement.

✓To embed the latest cryptographic algorithms and protocol to warrant an ultimate security levels.



NOVELTY & INVENTIVENESS

✓A new architecture for 'trust-no-one' chat application.

✓An integration and a migration of existing features from hybrid P2P architecture into this new application.

✓The architecture is adoptable to any application and the engine is configurable for variable security levels.

USEFULNESS & APPLICATION

✓Communication between two or more parties in a covert channel.

✓Idea (architecture, framework, engine) can be extended to any communication applications.

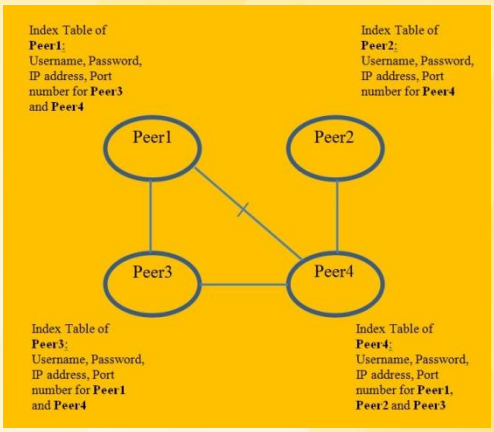
COMMERCIALIZATION POTENTIAL

✓sCHAT targets all sort of entities such as government agencies, commercial institution or even private individual.

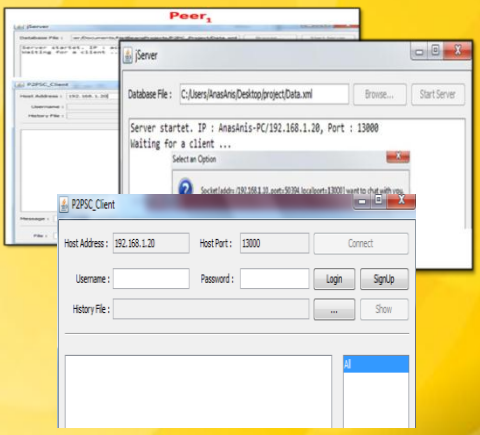
✓Initial plan is to implement a secure channel within UniSZA to serve the need for secure communication among academicians.

✓By leveraging customer expectations with proper security measures, the product can go global.

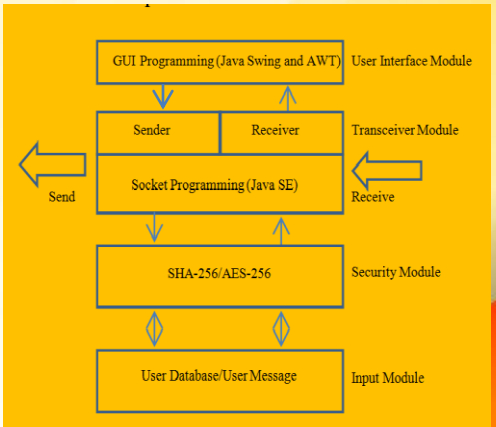
Architecture



Connection Establishment



Framework



Data Transfer