Abstract

Peer-to-Peer (P2P) communicating is a networking and distributed communication paradigm which allows symmetric sharing of messages between two entities, ideally without any interception from any third entity. Privacy in peer-to-peer communication is, however, can be compromised via a large number of approaches. It is therefore a need of the hour to provide security against eavesdropping and electronic surveillance while exchanging confidential and/or personal information. SMS or Short Message Service is the most widely used mode of communication for information exchange around the globe. In this paper, an approach to android application is presented which will be helpful for users of android based mobile phones to share textual information via SMS without the fear of it being intercepted by any middle-man. A cryptography technique is implemented which avoids the leakage of clear messages that is
being transferred from one end to the other, by encrypting it using an already exchanged private key, thereby making the middle-man unable to decipher the intercepted information. The private key exchange is done using the Diffie-Hellman key exchange algorithm, and AES-128 is used as the encryption/decryption algorithm. The messages sent and received are stored in a database accessible by the application, for future reference to the messages. The implemented application was successfully tested on Android Virtual Machine as well as on mobile phone running android version 2.3. The message received was a random jumble of characters and the original message was available only through the application.

References

- developer.android.com/guide/basics/what-is-android.html

Index Terms

Computer Science  Security
Keywords
  android  cryptography  mobile communication  security  sms communication