SMSCrypt

.

Objective

The project SMSCrypt is aimed to provide a secure SMS communication system between GSM users (phones).

Introduction

The SMSCrypt system provides a transparent means to transmit messages as done by the standard mobile SMS mechanism. User composes an SMS and sends it as usual, but the outgoing message is encrypted. The receiver is able to view the message like any other SMS. The received encrypted message will be automatically and transparently decrypted before being displayed at the receiving end.

The SMSCrypt focuses on the design and implementation of SMS system to send secure, encrypted SMS messages between willing participants without exchanging encryption keys between the participants during the session.

Description

User starts SMSCrypt application and selects the phone number to send the SMS. If the number is present, the process continues and the user composes the message. After completion, Users clicks on Encrypt button. The application randomly selects a key from the set of key present in mobile for that particular buddy and sends a silent message with the key-id used for encrypting the message. Receiver side application receives the silent message and checks whether the same key-id is present. If the key-id is present and is not in use/expired, receiver side application sends an acknowledgement or else a negative acknowledgement. On receiving acknowledgement, sender application encrypts the SMS with that particular key and changes the state of key to "Expired". Application displays the notification message on successful encryption of message. User sends the message. Receiver receives notification of incoming Encrypted message and clicks OK. SMSCrypt application decrypts message by validating unique key from set of key of sender.

EasyBuy System Overview

Technical Benefits

Convenience

SMSCrypt offers a simple and familiar interface for composing and reading text messages. It functions exactly the same way as the standard SMS operations on mobile handsets.

Security

Two levels of security allow the user to select whether to use dynamically generated keys for general use for each message, or to use one-time use keys from a block of pre-generated keys matched with specific buddies.

Portability

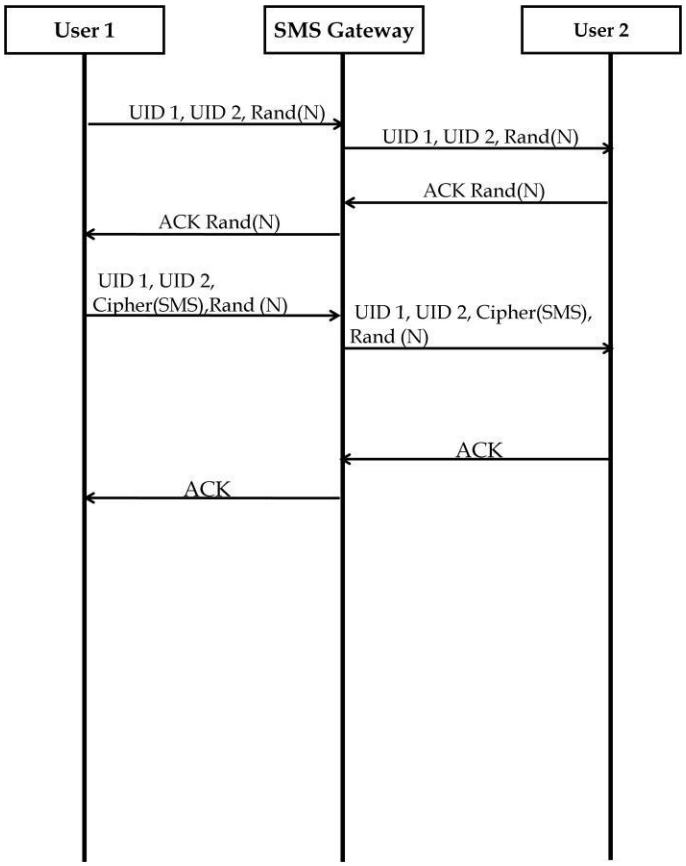
The solution can easily be run on various handsets and back-end servers.

SMSCrypt

Transparency

The solution is operator-agnostic, and thus works transparently between any two handsets regardless of their service providers.

Sequence Diagram



Feature Summary

For Mobile Users

- Mobile application runs on almost all Java-enabled handsets
- Simple registration process enrolls users into the system
- PIN used for both creating and reading encrypted messages
- PIN never stored on the mobile phone
- Single-use keys for each message for higher security
- Choice of high and normal levels of encryption
- Simple option to change PIN through the application UI

Prof. N . BALAKRISHNAN

Supercomputer Education Research Centre
Indian Institute of Science(IISc), Bangalore

E-mail: balki@serc.iisc.ernet.in