Abstract

Lately, there has been an exponential increase in the usage of smartphones. In order to access features and information in Android phones, applications have to explicitly request permissions before they are installed. In all there are 13 permissions, out of which four are reserved for Short Messaging Service. These permissions are required to read, receive, send and write the messages by the application. However there is a possibility of misuse of the permissions by the developers for exploiting and leaking out personal data. While developing a location tracking application, we discovered the possibility for exploiting these permissions. We have tested it on various smartphones. In this paper, we are presenting an idea to avoid leaks in Short Messaging Service by using effective encryption techniques such as AES and Key Distribution Centre in support.

References

Index Terms

Computer Science  Security

Keywords

Aes  Kdc  Location Manager  Sms Manager