Ayu Tiwari
MW200505

A Multifactor Security Protocol for Wireless payment- Secure Web Authentication using Mobile Devices

Abstract

The Cell phones have revolutionized the way we live. Cellular phones and PDA's have largely grown in popularity and as a result users have started online banking, purchasing of internet-based products and other online services. Previous web access authentication systems have used either the Internet or the wireless Mobile channel independently to authenticate the identity of remote user.

Accessing today's web-based services always requires a username and password to authenticate the user identity. This is a significant vulnerability since the password can be hacked by the man in the middle attack and later used for making illegal access to the user's account.

Our goal is to create an authentication system that is both secure and highly usable based on multifactor authentication approach. It uses a novel approach to create an authentication system based on TICs (Transaction Identification code) and SMS (Short Message Service) to enforce an extra security level with the traditional Login/password system.

We have also used an encryption/decryption technique which is based on symmetric key and an iterated block cipher concept. This concept has been used to keep TICs as secret code on cell phones/PDAs and is also used to initiate secure web transaction using cell phones/PDAs. Finally we extend the system for two way authentication which authenticates both parties (user and e- service provider).

A detailed threat analysis demonstrates that the proposed system is secure against various types of internet attacks like phishing, man-in-the-middle, viruses etc.