

MULTIFACTOR AUTHENTICATION & SECURITY

ABSTRACT

As computing becomes pervasive, people increasingly rely on public computers to do business over the Internet. Now the Internet has become the preferred environment for a multitude of e-services: e-commerce, e-banking, e-voting, e-government, etc. Financial institutions offering Internet-based products and services to their customers should use effective methods to authenticate the identity of customers using those products and services.

Accessing today's web-based services invariably requires typing a username and password to authenticate. This is a significant vulnerability since the password can be captured by the public computer and later reused by a hostile party. The current online payment systems do not provide adequate authentication of users. As a result it is always possible for an unscrupulous user to enter credit card number or account details stolen from valid users. The Financial Agencies consider single-factor authentication to be inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties using web browsers or cell phones/PDAs. So we need Multifactor Authentication techniques to secure our web transactions and to increase faith of users on mobile financial transactions. In this paper we propose an authentication system that is both secure and highly usable, based on multifactor authentication approach. It uses a novel approach to create authentication system based on Transaction Identification code (TICs) and SMS to enforce extra security level with traditional Login/password system.

TICs are user specific unique transaction identification codes which can be issued by banks or financial institutions to the user. This code is similar to One Time Password (OTP) and one code is used only once. This talk also suggests an encryption/decryption technique that would be used to keep TICs as secret code on cell phones/PDAs. The user can easily pick up a TIC (from the stored list of TICs) to initiate secure web transaction using cell phones/PDAs, instead of typing complicated TIC code in each transaction. We also describe a system for two way authentication which authenticates both parties. This would authenticate the company or service provider to the user along with the authentication of user to the financial institution.

About Professor Sanyal:

Prof. Sugata Sanyal is in the faculty of the Tata Institute of Fundamental Research, India, from 1973. He received his Ph D degree from TIFR under Mumbai University, M Tech from IIT, Kharagpur and B E from Jadavpur University, India. His current research interest includes security in wireless and mobile ad hoc networks, distributed processing and scheduling techniques. He has published numerous papers in National and International journals and attended many conferences. He is in the editorial board of

three international journals. He is co-recipient of VASVIK award for Electrical & Electronics Science and Technologies for the year 1985. He was a visiting professor in the Department of Electrical and Computer Engineering and Computer Science in the University of Cincinnati, USA, in 2003. He delivered a series of lectures and also interacted with the Research Scholars and faculties in University of Cincinnati, University of Iowa, Iowa State University and Oklahoma State University. He has been an Honorary Member of Technical Board in UTI, SIDBI, CMPFO and MSEB. He has also acted as a consultant to a number of leading industrial houses in India. More information about his activities is available at <http://www.tifr.res.in/~sanyal>