A Reliable and Secure One-Time Password Authentication System

A dissertation submitted to the University of Manchester for the degree of Master of Advanced Computer Science

2012

Farhad Ghavam Rankouhi

School of Computer Science

Abstract

Entity authentication is an essential procedure for establishing a secure channel between communication parties. A communication party can be either a user on the client side or a service provider on the server side. Hence, the user is not the only communication party who requires to be authenticated.

In recent years, a variety of authentication methods have been proposed to verify the identity of entities. Among the existing authentication methods, one-time password method provides a high level of security and requires less computation. However, the existing authentication systems based on one-time password have some security flaws which make them vulnerable to various types of attacks such as replay and impersonation attacks. The aim of this project is to provide a cost-effective authentication system based on one-time password method, RSOP.

This project work provides an extensive background research of the existing authentication systems. The strengths and limitations of these systems have been identified and critically analyzed. The analysis has shown that the majority of the practical systems are limited by three primary issues. The first issue is related to the authentication method between users and service provider. At present, most of the systems are using one-way authentication. This makes the system vulnerable to impersonation attacks. Secondly, most of the service providers communicate with the users through unencrypted data. This data can be easily intercepted by masquerade users. Finally, these systems use single-factor authentication method. This makes the system susceptible to man-in-the-middle attacks. The RSOP system, proposed in this research is an efficient solution designed to address these limitations. This exploratory work provides a mutual and multi-factor authentication including static-password, one-time password and Public Key Cryptography.