BEST: International Journal of Management, Information Technology and Engineering (BEST: IJMITE)
ISSN 2348-0513
Vol. 2, Issue 3, Mar 2014, 73-76

SECURITY USING FOUR FACTOR PASSWORD AUTHENTICATION

DEVIDAS LOLGE, YOGESH DAKE, ANAND MOKASHI & SUNIL PATIL

Department of Computer Science, The Pune University, Pune, Maharashtra, India

ABSTRACT

The project entitled as "Security Using Four Factor Password Authentication". In the scheme the remote user does not need to use smart cards. The scheme is easy to implement. However, this authentication scheme is vulnerable to impersonation attacks and middle man attacks.

An attacker could impersonate legitimate users to login and access the remote server. The scheme suffers from replay attacks and impersonation attacks. Lamport proposed a password authentication scheme to provide authentication between the users and the remote server. Since then, many password-based remote user authentication schemes have been proposed.

In a smartcard based password authentication scheme, the smart card takes the password and Finger print from the users as input, computes the login message and sends the login message to the server. The server checks the validity of the user's login message. In the mutual authentication situation, not only the server can verify the user but also a user can verify the server.

KEYWORDS: Android, Location, Social Networks, REST Api

INTRODUCTION

Typically to gain access to a system that provide what we call a factor of authentication. Authentication tools provide the ability to determine the identity of a party to an interaction and to ensure that a message came from who it claims to have come from. Authentication is seldom used in isolation. Authentication is used as the basis for authorization (determining whether a privilege will be granted to a particular user or process), privacy (keeping information from becoming known to non-participants), and non-repudiation (not being able to deny having done something that was authorized to be done based on the authentication).

An increasing number of internet-based end-customer applications require four factor authentications. Text message based one-time code distribution (as second factor) is rapidly becoming the most popular choice when strong authentication is needed, for example in e-banking. With multi-factor authentication, each token available for authenticating the user falls into one of the following three categories:

- Something the user knows (e.g. a password)
- Something the user has (e.g. hardware token)
- Something the user is (e.g. a fingerprint)

OBJECTIVES OF THE STUDY

To secure bank transactions and various systems using four different factors as follows:

- User ID.

- TXT Password.
- Fingerprint Authentication
- OTP (One Time Password).

SYSTEM ARCHITECTURE

Similar to other application the main functionality of this application is to provide a better security to the bank transactions and the systems. And the whole architecture is divided into modules as described below:

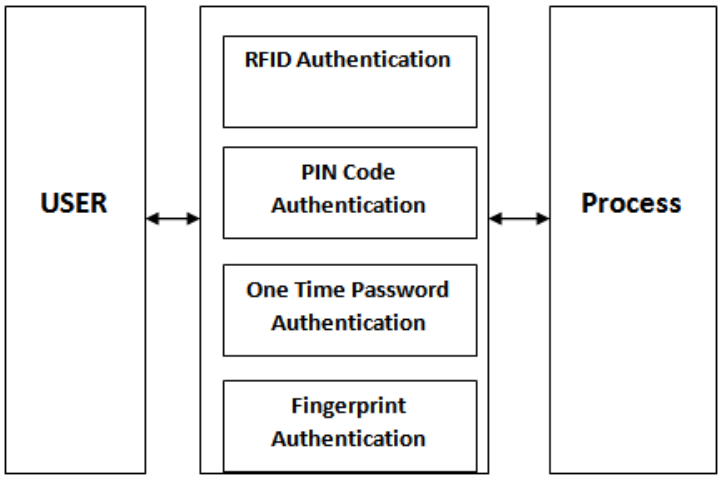

Figure 1

MODULES DESCRIPTIONS

User Interaction

- Users must have access to a computer and a method of payment. In our system, the user interactions are login, registration and communication. User details are handled in backend common database.

PIN Code Authentication

- In computer security, a login or logon is the process by which individual access to a computer system is controlled by identifying and authenticating the user referring to credentials presented by the user.
- A user can log in to a system to obtain access and can then log out or log off when the access is no longer needed. To log out is to close off one's access to a computer system after having previously logged in.

RFID Authentication

- Radio frequency identification (RFID) is a generic term that is used to describe a system that transmits the identity (in the form of a unique serial number) of an object or person wirelessly, using radio waves. It's grouped under the broad category of automatic identification technologies.

One Time Password

- The main security for our system is one time password. This password provides by service provider to customer. It’s only valid in five minutes only.

Fingerprint Authentication

- Fingerprint identification or hand print identification, is the process of comparing two instances of friction ridge skin impressions, from human fingers or toes, or even the palm of the hand or sole of the foot, to determine whether these impressions could have come from the same individual. The flexibility of friction ridge skin means that no two finger or palm prints are ever exactly alike in every detail; even two impressions recorded immediately after each other from the same hand may be slightly different. Fingerprint identification, also referred to as individualization, involves an expert, or an expert computer system operating under threshold scoring rules, determining whether two friction ridge impressions are likely to have originated from the same finger or palm.

Application Maintenance

- Final module of our project as application maintenance. That is, to maintain our application with more and more security. Such as PIN code evaluation, RFID, OPASS and Fingerprint verification.

CONCLUSIONS

The role of this system is to provide more security to the bank transactions and other important systems this can be done using four different modules.

By these users can securely make their transactions successful or can access important systems.

ACKNOWLEDGEMENTS

We would like to express our gratitude towards Prof.H.A.Hingoliwala whose support and consideration has been an invaluable asset during the course of this project.

First and foremost, we would like to thank our guide Prof.M.D.Ingle for providing us with their invaluable guidance throughout the course of this project. It would have been an almost impossible task to complete this project without his support, motivation, valuable suggestions and criticism.

We convey our gratitude to our respected Head of Department, Prof .S. Shinde for his motivation, guidance, and criticism and also for providing various facilities, which helped us greatly in the course of this project.

And, last but not the least we would like to thank Principal M.D.Jadhav and all the teaching, non-teaching staff of Computer Department and also our friends for directly or indirectly helping us for the project completion and all the resources provided.

REFERENCES

1. Simon Robinson, Christian Nagel, Karli Watson, “PROFESSIONAL C#”, Wiley Dreamtech India Pvt ltd., third edition.
2. Andy Harris, “MICROSOFT C# PROGRAMMING”, Prentice hall of India Pvt ltd.,
3. Roger S.Pressman, **“**SOFTWARE ENGINEERING**”**, TataMcGraw Hill Publications, fifth edition.
4. Elias M.Award’s, “SYSTEM ANALYSIS AND DESIGN**”,** Galgotia Publications Private Limited Companies, 1997 Edition.
5. Herbert Schildt, “THE COMPLETE REFERNCE C# 2.0”, TataMcGraw Hill Publications, second edition.

6. V.K.Jain, **"**THE COMPLETE GUIDE TO C# PROGRAMMING**",** Dreamtech press.

7. E.Balagurusamy, "PROGRAMMING IN C#", TataMcGraw Hill Publications.

8. Gregory S.Macbeth, "C# PROGRAMMERS HANDBOOK", Shroff publishers & distributors Pvt ltd.