RESEARCH ARTICLE OPEN ACCESS

Android Based Total Security for System Authentication

Mithil Vasani*, Bhavesh Pandya**, Charmi Chaniyara***
*(Information Technology, Mumbai University, Sfit)
** (Assistant Profsor in Sfit Mumbai, Mumbai University)
*** (Assistant Profsor, Mumbai University)

ABSTRACT
In this Paper [5], A highly severe menace to any computing device is the impersonation of an authenticate user. The most frequent computer authentication scheme is to use alphanumerical usernames and passwords. But the textual passwords are prone to dictionary attacks, eves dropping, shoulder surfing and social engineering. As such, graphical passwords have been introduced as an alternative to the traditional authentication process. Though the graphical password schemes provide a way of making more user friendly passwords, while increasing the level of security, they are vulnerable to shoulder surfing. To address this problem, text can be used in combination with the colors and images to generate the session passwords, thereby making a stronger authentication means. In general, session passwords are those that can be used only once and for every new session, a new password is engendered.
This paper [7] describes a method of implementing two factor authentication using mobile phones. The proposed method guarantees that authenticating to services, such as online banking or ATM machines, is done in a very secure manner. The proposed system involves using a mobile phone as a software token for One Time Password generation. The generated One Time Password is valid for only a short user defined period of time and is generated by factors that are unique to both, the user and the mobile device itself. Additionally, an SMS-based mechanism is implemented as both a backup mechanism for retrieving the password and as a possible mean of synchronization. The proposed method has been implemented and tested. Initial results show the success of the proposed method.
Keywords **–** Authentication, Security, Mobile, Access control, Least expensive

I. INTRODUCTION

Log-in applications till date requires user to enter the username and password in textual format. We have seen so many cases where the textual passwords are easily cracked and intruder breaks into the system's vital information section. As a result, private data becomes accessible and modification of these data causes great harm and financial losses to businesses.

Authentication scheme of our application provides one additional level of protection in the form of comparing two types of passwords (textual as well as mobile number). This provides enhanced security to a machine and makes it difficult for the attacker to gain access to system's resources.

1.1 Description of the Project

The usage of passwords for authentication is no longer sufficient and stronger authentication schemes are necessary. Strong authentication solutions require often two identification factors i.e. in addition to the first factor "something you know" represented by passwords, it is introduced a second factor "something you have" materialized by a security token.

We can use our mobile message as a password to the application. For lot of security reasons one generally requires a very secure password, and a mobile message is a unique one. Here we connect our mobile phone to a computer where the application is running.

The application may be of different types, only we are providing a very secure login to that application. The number which we have already predefined as a mobile password can act as password. Message from another mobile does not allow authorized user to login.

1.2 Motivation

In the war of functionality versus security, the former wins more often. Security has always been viewed upon as an overhead or afterthought by software developers. Nevertheless, there is a growing awareness in developer community regarding security due to several attacks that have surfaced off late.

Our motivation for developing this API is to eliminate the need for application developers to know the intricate details of security implementation of multi-factor authentication (MFA) and rather focus on the core functionality of the application. Our design is somewhat analogous to Java Authentication and Authorization Services (JAAS) which provides API for performing common authentication and authorization tasks. Our scope is limited to web-

applications that are built atop Java Enterprise Edition (JEE) technology. We have incorporated Spring MVC to make our API modular and easily configurable. With our API, the developers can add MFA to their existing web-applications just by making some configuration changes. This approach not just increases the productivity of a developer but also reduces the chances of security misconfiguration that renders web-applications vulnerable to attacks.

1.3 Problem Formulation and Methodology used

In today's world, most serious threat is the theft of identity which causes grave damages both for the victim and also his entourage such as employee, banks, hobby clubs, etc. The protection of digital identities is getting more and more crucial. The usage of passwords for authentication is no longer sufficient and stronger authentication schemes are necessary.

Strong authentication solutions require often two identification factors i.e., in addition to the first factor "something you know" represented by passwords it is introduced a second factor "something you have" materialized by a security token.

The introduction of the additional device could be costly for the service providers in terms of deployment and administration at the same time as it could be inconvenient for mobile users.

Furthermore, there is very little re-use or sharing such that the same security token can be used for several systems. To remedy the situation, there are proposed several authentication solutions that avoid introducing extra device by re-using existing devices, namely the mobile phone.

It is not specified which authentication level can be considered as strong but level 3 with multi-factor authentication is definitely considered a strong authentication. It is also clear that strong authentication does not have to be multi-factor.

1.4 Relevance of the project

- Least expensive authentication method to use.
- Enhance the image of the organization by securing user credentials more effectively.
- Users don't need to remember complex passwords.
- Can be used for login and transaction authentication.

1.5 Objectives

We have improved the security for Authentication by introducing a third level of security i.e. SMS (Short Messaging Service).

- Tying a system identity to an individual user by the use of a credential
- Providing reasonable authentication controls as per the application's risk.
- Denying access to attackers who use various methods to attack the authentication system

II. Literature Review

[1]Digital identity is the key representation of user and getting most crucial subject for information security. The password based authentication is weak solution and no longer adequate. User select static password which is easy to guess and remember, relevant information or common for all authentication process. This simplicity makes weak authentication scheme; as so far, static passwords are known as easiest target for attackers.

[1]Further, Security Token based runtime interaction could extend the strength of authentication control. Security tokens can be used for strong authentication but inconvenient for user and costly for the service providers.

[1]To avoid the user inconvenient and extra cost mobile phone is an emerging alternative. These papers comprise the study of various digital identification schemes and give motivation to integrate mobile token.

[1]In order to establish standard for mobile token, work starts with the review of current schemes and explores the security architecture for strong authentication with mobile token. Password algorithm is derived to generate dynamic password for token authentication.

[1]Thereafter explore various authentication mechanisms to implement mobile token on different prospective. At the end, it describes the various test cases and evolutionary result of various attacks on suggested schemes

.

2.1 Authentication Using Mobile Phone as a Security Token

[4]The protection of digital identities is getting more and more crucial. The usage of passwords for authentication is no longer sufficient and stronger authentication schemes are necessary. Strong authentication solutions using two identification factors require often an additional device, which could be inconvenient for the user and costly for the service providers.

[4]To avoid the usage of additional device, the mobile phone is adopted as security token. This paper provides a study of the various ways the mobile phone can be used as an authentication token towards service providers on the Internet. It starts with discussing the need for a strong authentication scheme, and the motivation for using the mobile phone to improve on several aspects of the current authentication processes. Thereafter, the general architecture for authentication with mobile phones is presented.

Several different authentication solutions using the mobile phone as authentication token are then

described, where the solutions vary in complexity, strength and user-friendliness. The paper ends with an evaluation of the different solutions, and a discussion of the most probable attacks. A classification of the solutions is also provided, according to defined criteria.

III. System Study and Analysis

3.1 Proposed and Existing System/Concept

The Existing system allows user to enter only textual passwords which can be easily cracked into using various methods (very common of them being brute force attack).

The Proposed System will allow a particular user to be authenticated only when a message from a predefined number is obtained. User won't be authenticated if message from some other number is provided.

PC will scan this text box for the entry of predefined mobile number. Compare the password with password in database. If it matches user is authenticated else not authenticated

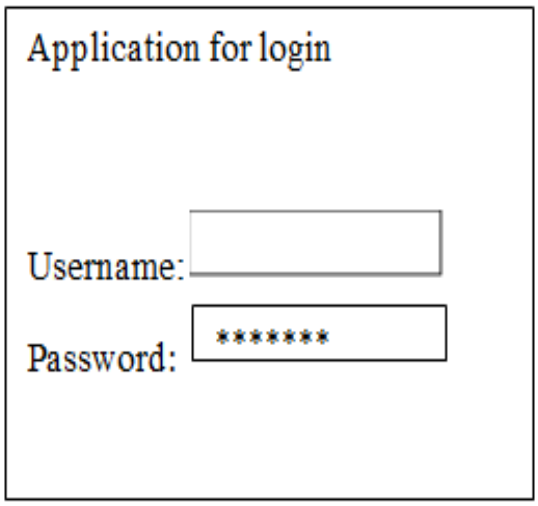

Figure 1: Login GUI

3.1 Flow Chart:-

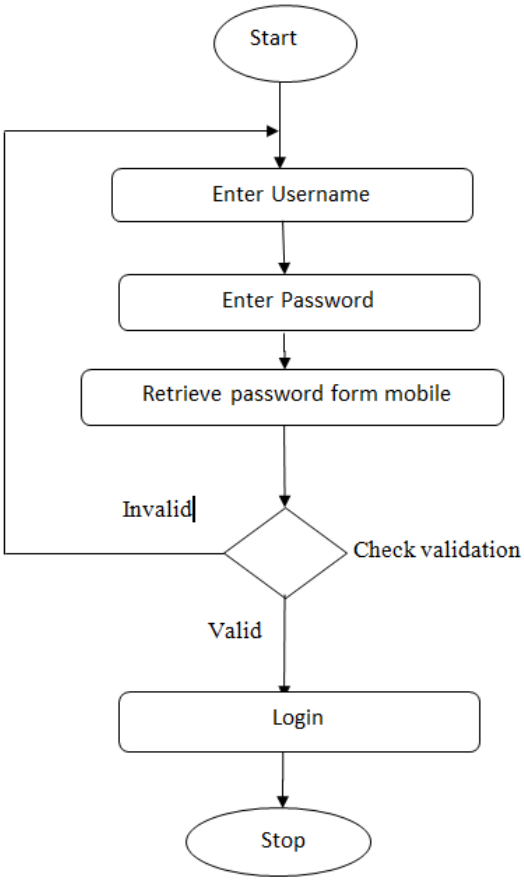

Figure 2 Flow chart of the system

3.3 Architectural Design

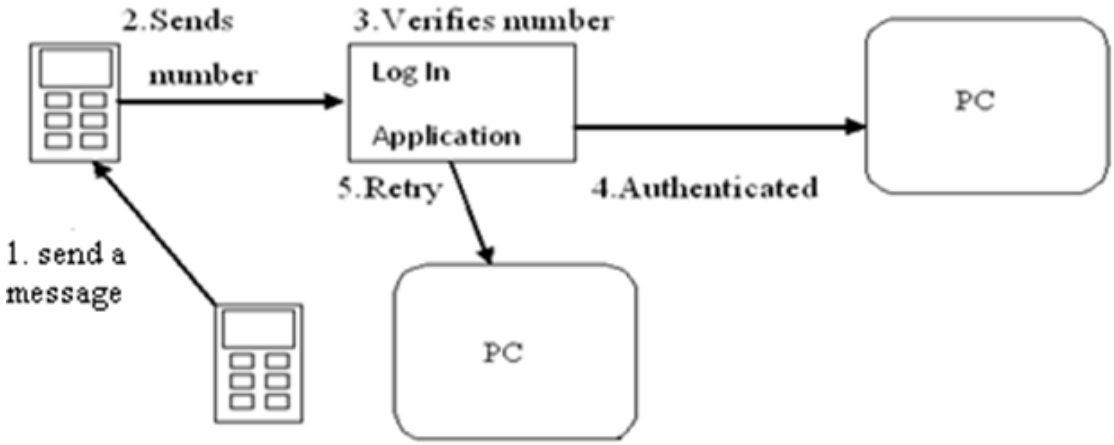

Figure 3: Architectural design of system

3.4 Requirement Analysis

- Economic Feasibility The expenditure for this project is limited to the cost of the hardware. The software's to be used for development of the project are freely available.
- Operational Feasibility Combination of the linear sequential method approach plus the incremental model has been employed during the development of the project. The linear sequential model approach was being employed during the analysis and the design phase.

3.5 Scope of the Project

- To ensure that user data is not abused, all requests for access must be approved by the account holder.
- Access control has two components, authentication and authorization. *Authentication* ensures that a valid user is logged-in, based on an ID and password provided by the user. Strong authentication is described as:

IV. Result and Discussion

The four modules namely:

- Admin
- Client
- Database
- TCP/IP

Have been successfully tested and are working smoothly. All forms were connected and tested successfully. The MySQL database was connected to Netbeans successfully. Data has been transmitted and received at the destination with the help of TCP/IP protocol

.

V. Testing

White Box Testing**:**

Module wise white box testing involves as below:

5.1 Admin Module:

5.1.1 Admin should be able to view all Projects.

5.1.2 Admin should be able to add and edit Project.

5.1.3 Admin should be able to link Project to TCP/IP.

5.2 TCP/IP: It will allow and establish the connection between mobile devices.

5.3 Database: It will store the parameters such as username, password, confirm password and the phone number of the admin

5.4 Client: Client will ask for permission from the admin to gain access of the system.

Both testing i.e. manual and automated is implemented:

1. Manual: This testing is implemented to have proper and thorough check of the system functionality while system is being created because until and unless entire system is ready automated testing will not be a good idea.
2. Automated Testing: This testing is implemented to check for the error while there is deployment done further so that the tester work is easily completed as it just requires running a testing script.

Automated testing is implemented using Selenium.

VI. Conclusion

Authentication is critical for security of computer systems. Without the knowledge of the identity of a principal requesting an operation, it is difficult to decide whether the operation should be allowed. Traditional authentication methods are not suitable for use in computer networks where attacker monitor network traffic to intercept passwords. The use of strong authentication method that do not disclose password is imperative. This authentication system is well suited for authentication of user in such environments.

Access control is concerned with limiting the activity of legitimate users. Access control assumes that the authentication of the user has been successfully verified prior to enforcement of access control via a reference monitor as correctly establishing the identity of the user is the responsibility of the authentication service.

VII. Appendix

- APCS: Automated Project Cost System
- Centralized: The process of coagulating decision making system
- Hierarchical: Arranging objects in a tree structure form
- UI: User Interface
- SQL: Structured Query Language
- HQL: Hibernate query language
- MVC: Model view controller architecture
- LOB: Line of Business
- WBS: Work Breakdown structure
- PM: Project manager

VIII. Glossary

Activity - Any work performed on a project which uses resources (people, materials or facilities) has an associated cost and duration and results in one or more products .Usually specified in a Work Breakdown Structure (WBS).

Budget – the amount of money allocated to the project.

Client – the people who benefit most from project success .Also known as the customer.

Constraints – restrictions to project duration, budget and resources.

Estimate - the prediction of measurable input or output, for example the cost or the duration of the project.

Gantt Chart – a visual representation of the project schedule, in the form of a bar chart.
Phase – the set of activities leading up to project milestones. These are usually represented on the Work Breakdown Structure (WBS).
Project Management-The process of managing (planning, running, monitoring and controlling) a project.
Project Manager – the person responsible and ultimately accountable for a project's performance.
Schedule – timeline identifying start/end dates for all project activities.
Work Breakdown Structure (WBS) - a hierarchical breakdown of the project activities.

References

[1] -Parekh Tanvi SIMS, Indore tanvi.parekh@sims-indore.com
[2] Gawshinde Sonal SSSIST, Indore sonal209@yahoo.co.in
[3] Sharma Mayank Kumar IET-DAVV, Indore leomayank @yahoo.com
[4] -IEEE paper by-Do van Thanh – Telenor & NTNU, Norway , Ivar Jorstad – Ubisafe, NorwayIEEE 978-1-4244-5113-5/09
[5] S.Balaji, Lakshmi.A, V.Revanth, M.Saragini, V.Venkateswara Reddy.
[6] Professor T.Venkat Narayana Rao, Vedavathi K
[7] Wassim El-Hajj College of Information technology UAE University welhajj@uaeu.ac.ae