THREE LEVEL PASSWORD AUTHENTICATION

Prof. Mrs.S.N.Shitole
Dept Of Computer Eng.
MIT Polytechnic, Pune Kothrud.

Anushka Dhanve
Diploma in Computer Engineering,
MIT Polytechnic, Pune Kothrud

Aachal Khadke
Diploma in Computer Engineering
MIT Polytechnic, Pune Kothrud

Ashwini Bansode
Diploma in Computer Engineering,
MIT Polytechnic, Pune Kothrud

Abstract:— The project is an authentication system that validates user for accessing the system only when they have input correct password. The project involves three levels of user authentication. There are varieties of password systems available, many of which have failed due to bot attacks while few have sustained it but to a limit. In short, almost all the passwords available today can be broken to a limit. Hence this project is aimed to achieve the highest security in authenticating users. It contains three logins having three different kinds of password system. The password difficulty increases with each level. Users have to input correct password for successful login. Users would be given privilege to set passwords according to their wish. The project comprises of text password i.e. passphrase, image based password and graphical password for the three levels respectively. This way there would be negligible chances of bot or anyone to crack passwords even if they have cracked the first level or second level, it would be impossible to crack the third one. Hence while creating the technology the emphasis was put on the use of innovative and untraditional methods. Many users find the most widespread text-based password systems unfriendly, so in the case of three level passwords we tried creating a simple user interface and providing users with the best possible comfort in solving password.

Keywords: Dynamic Password, One factor authentication, Database, One Time Password

I. INTRODUCTION

Security is that the degree of protection to safeguard a nation, union of states, persons or person against danger, damage, loss, and crime. Security as a kind of protection is structures and processes that give or improve security as a condition. The Institute for Security and Open Methodologies (ISECOM) within the OSSTMM three defines security as a kind of protection wherever a separation is formed between the assets and also the threat. Security as a national condition was outlined during a global organisation study (1986) in order to that countries will develop
and progress safely. Security has got to be compared
to connected concepts: safety, continuity, responsibility. The key distinction between security and re-
ponsibility is that security should take under con-
sideration the actions of individuals making an at-
tempt to cause destruction. The project is an authen-
tication system that validates user for accessing the
system only when they have input correct password.
The project involves three levels of user authentica-
tion.

II. LITERATURE SURVEY

In a research product, tolling practice and technolo-
gies are presented. likely development and enhance-
ment are reviewed, along with potential to other in-
telligent transportation system.

1. IEEE Xplore, Three Level Password Authenti-
cation System. This paper suggest the use of both hardware token (smart-card) and the soft-
ware token (HOTP which is system generated).
These two tokens are used as separate levels of
authentication to ensure the security to user pro-
file.

2. Implementation of Security System Using 3-
Level Authentication This paper is a unique and
an esoteric study of using pattern as password
and implementation of an extremely secured sys-
tem, employing 3 levels of security-(Text Pass-
word, Pattern-Lock, and One-Time automated
generated password).

3. IEEE Xplore, 4, April 2014, 3-Level Password
Authentication System. They proposed a multi-
factor authentication scheme that combines the
benefits of the existing authentication schemes
and thereby, overcomes the pitfalls of the cur-
rently used authentication schemes.

III. SYSTEM ARCHITECTURE

Generally, authentication methods are classified into
three categories (Manjunath et. al., 2013)(Suo et. al.,
2005).

1. Text based authentication
2. Graphical based authentication
3. Image based authentication

1. Text based authentication
A password is a secret word or phrase that gives us-
ers access to computer resources such as programs,
files, messages, printers, internet, etc (Akinwale and
Ibharalu, 2009). Passwords are more than just a key.
They ensure our privacy, keeping our sensitive in-
formation secure. There are mainly two types of
password (Himika et. al., 2012):

1. Static password
2. Dynamic

Static password is the traditional password which is
usually changed only when it is necessary: it is
changed when the user has to reset the password,
i.e., either the user has forgotten the password or the
password has expired. While dynamic password,
also known as One Time Password (OTP), is a pass-
word which changes every time the user logs in. An
OTP is a set of characters that can act as a form
identity for one time only. Once the password is used, it
is no longer used for any further authentication.
Moreover, the first level employs the static password
due to the complexity of the One Time Password
(OTP).
2. Graphical password

- In this we have to set an code such as a color code e.g. color is red green blue so the colour code will be red-green-red-blue-green.

- If the user forgets the password then he/she can click on forgot password and he/she can re-set new password.

3. Image-Based Password

- In this level user need to upload an image and then the image will be cut into parts then while logging the user need to set the image according previous image.

- If the user forgets the image he/she can upload it by clicking on forgot button.
IV. PROPOSED METHODOLOGY

In the registration phase in Fig1.1, the user should provide user’s details along with his/her user name and user conventional textual password which is as strong as much and difficult to guess. This will protect the system from Tempest attack, Brute-force attack at client side. User have to register with his/her mobile number along with one security question for validation phase of authentication and forget password recovery purpose simultaneously. Above all, user has to select position of pattern according to his/her choice it’s nothing but pattern-lock for that individual user, one advantage that selecting pattern is user can provide any kind of pattern he wanted while registration. Security at text-based level has been imposed by using Text based password (with special characters), which is a usual and now an anachronistic approach. At pattern-lock level the security has been imposed using patterns, where the user will be asked to select an patterns as difficulty level which is unique one for each and every individual user. After preceding above two levels in registration system will generate random-code which is used to provide one-time password authentication level that is next and uppermost third level of authentication. This generated random code is valid for that particular registration phase only. After the successful registration only all the related data about user for authorised/legal use of system (or) application will stored in database. In the authentication phase in Fig1.2, the user should provide user name along with it’s registered text-base password for textual password authentication which is level1, after preceding level1 user will ask for entering pattern in pattern-lock at level2, this pattern should match to the pattern in pattern-lock which is unique one and different for each and every user and has selected by user at the time of registration. At this stage pattern should be same as that of registered pattern in pattern-lock for individual user. If it’s fails to match simply that user is unauthorised user to access that particular system (or) application. After preceding above two levels, random-code which has generated by system, will send to registered user’s mobile number (or) for application flexibility purpose it can be send to user’s entered mobile number at level3, it’s a six digit code, and advantage of this code is that it’s valid for current login session only. If any one of above 3 levels of security get mismatched (or) compromised user will not authenticate to system (or) application simply that would be restricted user. This unique and user-friendly 3-Level Security System is involving three levels of security. Where the preceding level must be passed in order to proceed to next level. · Security at level1 has been imposed by using Text based password (with special characters), which is a usual and now an anachronistic approach. · At level2 the security has been imposed using Pattern-Lock authentication where the user will be asked to select pattern levels. For each and every user will have different levels with unique pattern-lock, from where the user has to select any kind of pattern he want. · After the successful clearance of the above two levels, the Level3 Security System will then generate a one-time numeric password that would be valid just for that registration (or) login session only.

V. FUTURE SCOPE

In future we are planning of making this system more accurate.also we will be implementing the facility of authentication more secure.

VI. CONCLUSION

The conclusion came out is that to implement modern system of password authentication. We will design the system with high security. Then levels in the
system for authentication will be tough to crack. We use one time password authentication process in one of the level.

VII. REFERENCES