Authentication by Encrypted Negative Password

Abstract

This paper is about securing the passwords and making the system more secured from intruders. Most of the stock management systems uses the method where in the passwords are just encrypted and are not secured properly. This encrypted negative password system uses the technique where in the passwords are first hashed and then converted to and finally encrypted and converted to negative password and stored in the database.However the processor resources and storage resources are becoming more and more abundant, hashed passwords cannot resist precomputation attacks, such as rainbow table attack and lookup table attack. This Encrypted Negative Password system still can resist the precomputation attacks. Thus by securing the pages with negative password system, all these vulnerabilities can be reduced.

**AIM**

The aim of the paper is to enhance password security. There are lots of corresponding ENPs (Encrypted Negative Passwords) for same password, which makes attacks (e.g., lookup table attack and rainbow table attack) infeasible.

**1.2 OBJECTIVE**

1) Even when the database is hacked, the original password cannot be retrieved.

2) The data will be processed with many algorithms which make it hard to hack.

3) The original password is converted into a negative password by performing hashing, permutation,

and encryption.

4) The encrypted value is stored in the database.

5) There will be different encrypted negative passwords for same plain password.

**1.3 PROJECT DESCRIPTION**

The aim of the project is to enhance password security. When carrying an online

guessing attack, there is a limit to the number of login attempts. However, passwords can be

leaked from weak systems. Some old systems are more vulnerable due to their lack of

maintenance. The passwords are often reused, adversaries may log into high security

systems through cracked passwords from low security systems. There are lots of

corresponding ENPs for a given plain password, which makes attacks (e.g., lookup table

attack and rainbow table attack) infeasible. The complexity analyses of algorithm and

comparisons show that the ENP could resist lookup table attack and provide stronger

password protection under dictionary attack. It is mentioning that the ENP does not

introduce extra elements (e.g. salt). Most importantly, the ENP is the first password

protection scheme that combines the cryptographic hash function, the negative password and

the symmetric-key algorithm without the need of any for additional information except the

plain password.

**1.4 PROJECT PLAN**

Project plan is a part of project management which relates to the use of schedules

such as Gantt Charts to plan and subsequently report progress within the project

environment. It is a discipline for stating how to complete a project within a certain frame

usually with defined stages and with resources. Initially, the project scope is defined andUser Authentication Using Encrypted Negative Password

3

Master of Computer Application

CUCEK

the methods for completing the project are determined. The duration for various tasks

necessary to complete are listed and grouped in to a work break down structure.

**Gantt chart**

The Gantt chart is an excellent tool for quickly assessing the status of a project. It is

a project control technique that can be used for several purposes. It is used for tracking and

reporting progress, as well as for graphically displaying a schedule. Gantt chart is used to

report progress they represent in easily understood picture & project status.

It includes

• Scheduling

• Budgeting

• Resource planning

This allows us to see at a glance:

•

What the various activities are.

•

When each activity begins and ends.

•

How long each activity is scheduled to last.

•

Where activities overlap with other activities, and by how much.

•

The start and end date of the whole project