Password cracking

[5]Passwords are a system designed to provide authentication.Storing user names and corresponding passwords in clear text is an unacceptable solution. Attempting to hide passwords stored as clear text (such as putting the password file deep in a convoluted directory hierarchy) would amount to “Security Through Obscurity” which would also be unacceptable.

Storing the hashed or encrypted values for passwords is certainly much more secure than storing their plain text in a password file.

The password file for Windows, known as the Security Accounts Manager (SAM) file, is located in C:\windows\system32\config\sam. An entry in the SAM file contains seven colon deliminated fields.Windows SAM file is not readable once the operating system has booted. Alternatively,

people have installed secondary operating systems to read the SAM file from there.

Storing the hashed or encrypted values for passwords is certainly much more secure than storing their plain text in a password file, but there is a common additional measure of security that can be implemented.This tactic involves adding additional randomness to passwords and is known as a password or cryptographic salt. When a password is created, the system will add some sort of randomness to the password. This randomness (or salt) should be different every time a password is made. Because of this, the exact same password will be stored as a different hash on different machines or different accounts on the same machine.

[10]A common threat Web developers face is a password-guessing attack known as a **brute-force attack**. A brute-force attack is an attempt to discover a password by systematically trying every possible combination of letters, numbers, and symbols until you discover the one correct combination that works.To block brute force attacks, different methods used are Locking of Accounts, Time bound login, Query-based Authentication, One time password authentication, using captcha and unique IP address login.

Depending on the password's length and complexity, there could be trillions of possible combinations. To speed things up a bit, a brute-force attack could start with dictionary words or slightly modified dictionary words because most people will use those rather than a completely random password. These attacks are called **dictionary attacks or hybrid brute-force attacks**. Brute-force attacks put user accounts at risk and flood your site with unnecessary traffic.

Solutions:

1. Hashed passwords
2. Salting password
3. Honeyword generation method[9]