Abstract

The techniques such as secured socket layer (SSL) with client-side certificates are well known in the security research community, most commercial web sites rely on a relatively weak form of password authentication, the browser simply sends a user's plaintext password to a remote web server, often using SSL. Even when used over an encrypted connection, this form of password authentication is vulnerable to attack. In common password attacks, hackers exploit the fact that web users often use the same password at many different sites. This allows hackers to break into a low security site that simply stores username/passwords in the clear and use the retrieved passwords at a high security site. While password authentication could be abandoned in favor of hardware tokens or client certificates, both options are difficult to adopt because of the cost and inconvenience of hardware tokens and the overhead of managing client certificates.

Recently, some collisions have been exposed for a variety of cryptographic hash functions including some of the most widely used today. Many other hash functions using similar constructions can however still be considered secure. Nevertheless, this has drawn attention on the need for new hash function designs. This work developed an improved secure hash function, whose security is directly related to the syndrome decoding problem from the theory of error-correcting codes. The proposal design and develop a user interface, and implementation of a browser extension, password hash, that strengthens web password authentication. Providing customized passwords, can reduce the threat of password attacks with no server changes and little or no change to the user experience. The proposed techniques are designed to transparently provide novice users with the benefits of password practices that are otherwise
only feasible for security experts. Experimentation are done with Internet Explorer and Firefox implementations and report the result of initial user.

Reference


Index Terms

Computer Science Security

Key words

Password Authentication Hash Functions

Message Digest

Secure Socket Layer

Random Password Generator
Pseudo Random Function