©2010 International Journal of Computer Applications (0975 - 8887)
Volume 1 – No. 19

Provable Secured Hash Password Authentication

T.S.Thangavel
AP / Dept. of MCA
K.S.Rangasamy College of Technology
Tiruchengode, Tamil Nadu

A. Krishnan
Dean
K.S.Rangasamy College of Technology
Tiruchengode, Tamil Nadu

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 Fire fox implementations and report the result of initial user.

The hash is implemented using a Pseudo Random Function keyed by the password. Since the hash output is tailored to meet server password requirements, the resulting hashed password is handled normally at the server with no server modifications are required. This technique deters password phishing since the password received at a phishing site is not useful at any other domain. The cryptographic hash makes it difficult to compute hash(pwd,dom2) from hash(pwd,dom1) for any domain dom2 distinct from dom1. For the same reason, passwords gathered by breaking into a low security site are not useful at any other site. The hash attack is always exponential in terms of the length of the hash value. We also study the work-factor of this attack, along with other attacks from coding theory, for non asymptotic range, i.e. for practical values. Accordingly, we propose a few sets of parameters giving a good security and either a faster hashing or a shorter description for the function.