**PASSWORD HASHING**

**ABSTRACT**

**The Common Password Problem.** Users tend to use a single password at many different web sites. By now there are several reported cases where attackers breaks into a low security site to retrieve thousands of username/password pairs and directly try them one by one at a high security e-commerce site such as eBay. As expected, this attack is remarkably effective.

**A Simple Solution.** PwdHash is an browser extension that transparently converts a user's password into a domain-specific password. The user can activate this hashing by choosing passwords that start with a special prefix (@@) or by pressing a special password key (F2). PwdHash automatically replaces the contents of these password fields with a one-way hash of the pair (password, domain-name). As a result, the site only sees a domain-specific hash of the password, as opposed to the password itself. A break-in at a low security site exposes password hashes rather than an actual password. We emphasize that the hash function we use is public and can be computed on any machine which enables users to login to their web accounts from any machine in the world. Hashing is done using a Pseudo Random Function (PRF).

**Phishing protection.** A major benefit of PwdHash is that it provides a defense against password phishing scams. In a phishing scam, users are directed to a spoof web site where they are asked to enter their username and password. SpoofGuard is a browser extension that alerts the user when a phishing page is encountered. PwdHash complements SpoofGuard in defending users from phishng scams: using PwdHash the phisher only sees a hash of the password specific to the domain hosting the spoof page. This hash is useless at the site that the phisher intended to spoof.

Submitted by

Asif Hameed

Aswin Kumar

S7R

MACE Kothamangalam

Mail id :asifhameedn@gmail.com,aswin\_prasannan@yahoo.co.in