A Password Extension for Improved Human Factors

Sig Porter

June 9, 1981

Abstract

In the composition of high security passwords one must compromise between maximizing the keyspace (or number of possible keys) and minimizing the probability that the password owner will have such difficulty remembering his password that he will write it down. My solution is to have a fairly large keyspace (64 bits) and a very long "pass-phrase" (up to 80 characters). The phrase is hashed into the key, which is then stored in encrypted form. The hashing necessarily includes one-way encryption. Since the phrase is long, one would expect a large keyspace for the actual phrase as well as for the hashed phrase. Since the phrase is meaningful to the owner it should be easier to remember. Since it is user generated, there is one fewer compromise path. The only problem is to insure that the users will not choose an obvious phrase.

One way to hash the pass-phrase is to encrypt it using DES block-chaining and a standard key. The last block of the encrypted chain is the hashed result. This procedure insures that every bit of the hashed result is a function of every bit of the phrase; also, assuming the presence of DES hardware, it is very efficient.

In order to protect the user (in a timely way) from password theft by simulation of the log-in system, the system should reply (to correct password entry) with a recognition phrase known only to the user (and the system). This recognition phrase can be stored in encrypted form, using the (hashed) password as the key.