

mnemonic systems are not designed to facilitate user memorization of random sequences, and may not even enforce a minimum sequence length in user password entry. A mnemonic system may also be cumbersome in terms of the user interaction involved in entering a password, in some cases demanding an involved sequence of non-uniform mouse movements to enter the password into a computer system.

[0010] Implementations of authentication systems typically use cryptographic protocols that are conventionally predicated on exact knowledge. An authentication system using RSA signatures, for example, derives its security largely from the presumption that a legitimate user with public key (N, e) possesses a corresponding secret key of the uniquely specifiable form (N, d) . There are situations, however, in which human and other factors undermine the possibility of exactness in a security system. For example, in biometric systems in which users identify themselves by means of fingerprint features, variability in user interaction is such that a finger is rarely read exactly the same way twice. Moreover, there are situations in which although the original information in a system is exact, its transmission may only be approximate. For example, users typically make typing errors when entering passwords on keyboards. Similarly, data transmission channels are often subject to random noise.

[0011] An element of some cryptographic protocols is referred to as a bit commitment scheme. In a conventional bit commitment scheme, one player, whom we denote the sender, aims to conceal a bit b . The sender produces an encryption of b , denoted by y , and sends y to a second player, known as the receiver. Generally, a bit commitment scheme is such that it is infeasible for the second player to learn the bit b . Additionally, the sender later "opens" the commitment y , that is, proves to the receiver that y indeed represents an encryption of b . It is generally only feasible, however, for the sender to "open" y in one way, that is, to decrypt a unique value of b . We may view this, intuitively, as a process whereby the sender places the bit b in a safe and gives the safe to the receiver. Only the sender can open the safe, since she alone knows the combination. Moreover, she cannot change the value contained in the safe while it is in the keeping of the receiver.

[0012] An example of a bit commitment scheme is the storage of the hash of user's password in a UNIX file accessible only to the UNIX system administrator. Since the system administrator only has access to the hash of the password, the system administrator does not know what the user's plaintext password is. Nonetheless, when the user provides a password for authentication, the system administrator can compare the hash of the provided password to the stored hash and, if the hashes match, confirm that the user has provided the proper password. Bit commitment may alternatively be done, for example, using a symmetric encryption algorithm, an asymmetric encryption algorithm, a pseudo-random sequence generator, or any other one-way function.

[0013] Formally, a bit commitment scheme consists of a function $F: \{0, 1\} \times X \rightarrow Y$. To commit a bit b , the sender chooses a witness $x \in X$, generally uniformly at random. The sender then computes $y = F(b, x)$. This value y is known as a blob. It represents the bit b sealed in a "safe". To "open" or decommit the blob y , the sender produces the bit b and the

witness x . The blob is successfully opened if the receiver has been convinced that y indeed represents an encryption of b . A bit commitment scheme is said to be concealing if it is infeasible for the receiver to guess b with probability significantly greater than $1/2$. It is said to be binding if it is infeasible for the sender to decommit the blob y with the incorrect bit, that is, with $(1-b)$. It is possible to deploy a bit commitment scheme as a commitment scheme on an arbitrarily long string of bits by committing each bit independently. The term commitment scheme shall refer to a scheme that involves commitment of a bit string c (or other potentially non-binary value) in a single blob, and for which it is possible to extract c efficiently given a witness for the blob. Thus we assume $F: C \times X \rightarrow Y$, where C is some potentially non-binary space.

[0014] Vendors of biometric authentication systems have for some time recognized the importance of achieving a practical system that stores biometric information in a non-explicit, protected form and that also can tolerate some corruption in subsequent biometric readings. To this end, the Mytec Technologies Inc. has developed an encryption process in which biometric information serves as an unlocking key. Sold under the brand name Bioscrypt¹⁹⁸, Mytec Technologies's process overcomes the problem of corruption in biometric readings by means of Fourier transforms. While fairly efficient, however, the BioscryptTM process carries no rigorous security guarantees.

[0015] Davida, Frankel, and Matt have proposed a system in which a biometric template is stored in non-explicit, protected form. The Davida et al. system, described in "On Enabling Secure Applications Through Off-Line Biometric Identification," *IEEE Symposium on Privacy and Security* (May 5, 1998), requires multiple biometric readings from which the check bits may be derived. A hash of the Davida et al. template which includes the check bits is then stored. The multiple biometric readings required by the Davida et al. system may be too time-consuming to be practical or attractive for many real-world applications. Further, the Davida system does not have the necessary error tolerance to work in many real-world applications.

SUMMARY OF THE INVENTION

[0016] Like biometric systems, authentication systems that make use of visual information to authenticate users also can require storage of information in a non-explicit, protected form that can tolerate some corruption in subsequent readings. For example, in an authentication system in which a user selects an area or object on a graphical display, it may be difficult for a user that is not dexterously gifted to consistently specify a small particular area or object on a graphical display. Yet, it can be useful to allow this sort of data entry as a "visual password." Benefits of such a "visual password" are derived from the fact that it may be easier for an individual user to remember such a password, particularly if the user has other alphanumeric passwords to remember, and the fact that there presently is no obvious dictionary attack for such a password.

[0017] In co-pending U.S. patent application Ser. No. 09/544,809, visual authentication data entry systems and methods are described. In International Patent Application Ser. No. PCT/US00/03522, a "fuzzy" commitment scheme is described that can store information in a non-explicit,