

## Science News

### BioVault Locks Up Biometrics

*ScienceDaily* (Aug. 4, 2009) — A system that allows biometric data to be used to create a secret key for data encryption has been developed by researchers in South Africa. They describe details of the new technology in the *International Journal of Electronic Security and Digital Forensics* this month.

---

If a user, a web customer say, wishes to send a message or other data to another user, an online shop, over an unsecured network, the message must be encrypted to avoid interception of sensitive information such as passwords and credit card information.

Encryption relies on authentication being symmetric to work. In other words, the user's password or PIN must match the password or PIN stored by the online shop to lock and unlock the data. This is because encryption systems use the password or PIN to produce, or seed, a random number that is used as the cipher for encrypting the data. If the passwords do not match exactly then the seed will be incorrect, the random number different and the decryption will fail.

One way to avoid users having to remember endless, complicated passwords is to use biometrics, including fingerprints, iris pattern, face recognition. However, biometrics is not a symmetric process. The initial recording of biometric data samples only a limited amount of the information, the pigment pattern in one's iris, for instance. The unlocking process then compares the iris pattern, or other biometric "token", being presented for access with the sample stored in the database. If the match is close enough, the user can gain entry.

The reason for this asymmetry is that any biometric system takes only a digital sample of data from the fingerprint or iris, for instance. Moreover, even the legitimate user will not be able to present exactly the same biometric data repeatedly. The close enough aspect of biometrics does not make biometrics insecure, provided that the closeness is very precise, but it does mean that biometric tokens cannot be used to create a secret key for an encryption algorithm.

Bobby Tait and Basie von Solms of the University of Johannesburg, Gauteng, South Africa, explain how biometrics can nevertheless be used to make a consistent secret key for encryption.

In conventional encryption, if Alice wishes to send a secret message to Bill, then she must encrypt the message, whether it is an email or credit card details transmitted from her computer to the online shop. In order for the encryption algorithm to provide cipher text that is random, a secret key must be provided. Alice and Bill must share exact copies of their secret key for this to work.

Aside from the asymmetry in biometrics, this approach will not work because Alice and Bill cannot provide the same biometric token to encrypt and decrypt the message. Now, Tait and von Solms have used the so-called BioVault infrastructure to provide a safe and secure way for Alice and Bill to share biometric tokens and so use their fingerprints, iris pattern, or other biometric to encrypt and decrypt their data without their biometrics being intercepted.

The BioVault encryption system works as follows:

In phase 1, Alice identifies herself to the authentication server, and indicates that she wants to send an encrypted message to Bill and requests Bill's biometric key from the server.

In phase 2, the server retrieves a random biometric key from Bill's stored biometric keys.

In phase 3, Alice uses the biometric key to encrypt her message and sends it to Bill.

In phase 4, Bill receives the message sent by Alice, and decrypts the message by testing the biometric keys in his database against the received cipher text.

The fact that each biometric key (data) is unique means that the BioVault system can irrevocably identify and authenticate users through their biometric keys (data) and detect fraudulent use of biometric keys.

Tait adds that the same approach could also be used to digitally sign electronic documents, files, or software executables using biometrics. He will be presenting the team's results on this aspect of their work in the UK at the beginning of September. "If passwords or tokens are used for authentication, only the password or token is proven as authentic - not the user that supplied the token or password," he explains, "Biometrics authenticates the user directly - this was one of the drivers behind the BioVault development."

---

**Journal reference:**

1. . **BioVault: biometrically based encryption.** *Int. J. Electronic Security and Digital Forensics*, 2009, 2, 269-279

*Adapted from materials provided by [Inderscience Publishers](#), via [EurekAlert!](#), a service of AAAS.*