Something You Are: Biometric: Disadvantages

- Key disadvantages to these biometric authentication techniques are
  - the number of false positives,
  - number of false negatives generated,
  - their varying social acceptance, and
  - key management issues.

Something You Are: Biometric: Disadvantages

- A *false negative* occurs when a user is indeed an authentic user of the system, but the biometric authentication device rejects the user.
- A *false positive* occurs when an impersonator successfully impersonates a user.
- Tradeoff needed for both (Tutorial)
- Social acceptance is another issue to take into account when considering biometric authentication techniques.
- All the biometric authentication techniques discussed here are less socially accepted than entering a password.

Something You Are: Biometric: Disadvantages

- The final disadvantage for biometric authentication techniques is the key management issue.
- In each of these biometric authentication techniques, measurements of the user's biology are used to construct a key, a supposedly unique sequence of zeros and ones that corresponds only to a particular user.
- If an attacker is able to obtain a user's biological measurements, however, the attacker will be able to impersonate the user.
- For example, a criminal may able to "copy" a user's fingerprint by re-creating it with a wax imprint that the criminal puts on top of his finger.

Something You Are: Biometric: Disadvantages

- If you think of the user's fingerprint as a "key," then the key management issue in this case is that we cannot revoke the user's key because the user cannot get a new fingerprint—even though her original fingerprint has been stolen.
- By contrast, the keys in password systems are generated from passwords, and users can easily have their passwords changed if they are ever stolen or compromised.
- Biometric authentication becomes ineffective once attackers are able to impersonate biometric measurements.

Gummy and Conductive Silicone Rubber Fingers

— Importance of Vulnerability Analysis —

Tsutomu Matsumoto

Yokohama National University
Graduate School of Environment and Information Sciences
79-7 Tokiwadai, Hodogaya, Yokohama 240-8501, Japan
tsutomu@mlab.jks.ynu.ac.jp

Matsumoto Fingerprint Paper-Asiacrypt2002

- Biometrics are utilized in individual authentication techniques which identify individuals by checking physiological or behavioral characteristics, such as fingerprints, faces, voice, iris patterns, signatures, etc.
- Biometric systems are said to be convenient because they need neither something to memorize such as passwords nor something to carry about such as ID tokens.
- In spite of that, a user of biometric systems would get into a dangerous situation when her/his biometric data are abused.
- For example, you cannot change your fingerprints while you can change your passwords or ID tokens when they are compromised.

*SECURITY ASSESSMENT OF BIOMETRIC user identification systems should be conducted not only for accuracy of authentication, but also for **security against fraud!***

-Matsumoto

Matsumoto Fingerprint Paper

- Therefore, biometric systems must protect the information for biometrics against abuse, and they must also prevent fake biometrics.