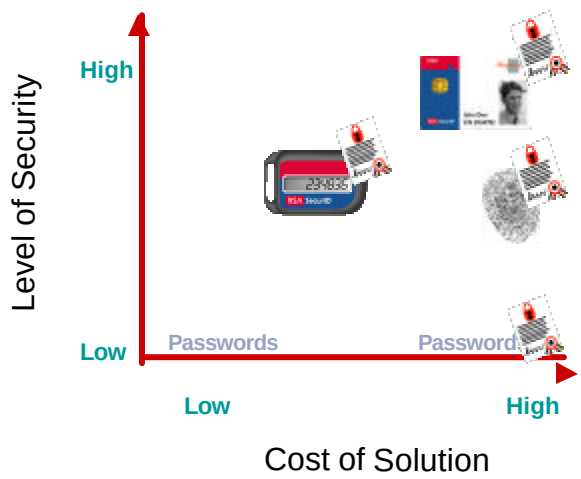
Biometrics: Back to Security Basics

Chris Mills
Product Manager
Strong Authentication
RSA Security
Feb. 2002

RSA SECURITY™

Comparing Authentication Solutions



RSA SECURITY™

Biometric Drivers & Inhibitors

Key Drivers

- Growing demand
  - Government
  - Wall Street
- Convenience
  - Replace passwords
  - Difficult to forget it
- Protect PKI credentials
  - Keys, applications
- "Bond" factor

Key Inhibitors

- Privacy
- Security
- Usability
  - FAR, FRR, FTA
- Infrastructure
  - Readers still too expensive
- Interoperability

RSA SECURITY

Security VS Convenience

- RSA's Position
  - Biometrics is a strategic priority for RSA
  - RSA's customers expect strong security
- Security Prerequisites to Enterprise Adoption
  - Coverage
  - Agent side spoofing
  - Server side spoofing
  - Cross System Replay
  - Social issues
  - Identity Theft and Revocation

RSA SECURITY

An Important Note

- **Biometrics no more secure than PINs!**
  - Static values
  - False acceptance rates imply, e.g., 1/100,000 security (I.e., perhaps 17 bits)
- **Thus, it is at present unwise to protect cryptographic systems with biometrics alone**

RSA SECURITY

Client VS Server-side Matching

- **Client side Match**
  - Fine for, e.g., locking desktop with screen saver
  - Not secure for remote authentication... client can be made to lie!
- **Server Side Match**
  - Yet another server...
  - Risk of theft *en bloc* from server
  - Matching is CPU-intensive
- **All sensors should be cryptographically-enabled**
  - Accept *only* samples from legitimate sensors

RSA SECURITY

On-device matching

- **Pros:**
  - Full privacy and integrity
  - With smartcard, biometric unlocks card, thus no need for modification of client or server software
- **Cons:**
  - Users must always have their smart cards – convenience and portability lost
  - At present, "true" on-device match units are expensive (> $200)
  - Many "on-card" matching systems process data on PC, reducing security

RSA SECURITY

The Key Issue with Biometrics

- **The biggest problem with biometrics**
  - If someone steals a token, IT issues a replacement
  - If someone gets your private key, you can revoke the matching certificate and make that key useless
    - A new certificate is created with the new public key
- **What do you do when someone steals your template or spoofs your biometric?**
  - The concept of a revocable credential does not exist in single-factor biometric solutions

RSA SECURITY

Good Uses of Biometrics

- In some cases, FAR, FRR and FTE are worth the tradeoff
  - For example, in hospitals
  - Or on a Wall Street trading floor
- In these situations, biometrics are typically being used in one of two ways:
  - Biometric+PIN for 2 factor authentication
  - Biometric as a replacement for a PIN

RSA SECURITY

Better Uses of Biometrics

- An excellent use of biometrics: integration of biometrics with smart cards
  - Use the biometric to unlock another authentication credential like a private key
- Benefit: template stored in a tamper resistant container
  - Like a private key, the biometric template file should not be readable
  - The private key and the matching digital certificate become the primary authentication method
- Result: revocable credentials, with good convenience

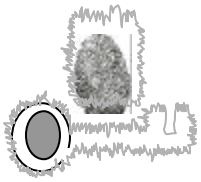
RSA SECURITY

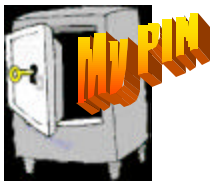
“Fuzzy Vault”: A New Architecture

RSA LABORATORIES

Basic idea in pictures

[my PIN]

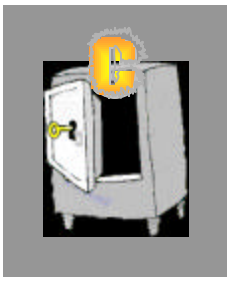




RSA SECURITY

What do we get?

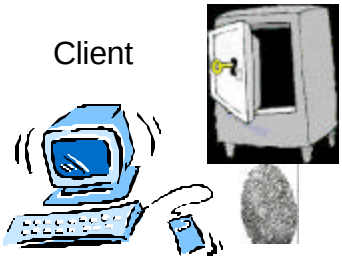
Fingerprint (and features) *not* stored in clear



RSA SECURITY

Fuzzy vault

Vault can be unlocked and stored on client or in public directory



RSA SECURITY

Fuzzy vault

- No need for biometric server
- No need for smart card
  - Fuzzy vault can be placed on card for added flexibility, though
- Simplified, more flexible architecture
- No need for cryptography on reader: readers at half the cost!

RSA SECURITY

Fuzzy vault

- RSA Laboratories patent pending
  - filed 27 November 2000
- Promises to transform architecture for biometrics

RSA SECURITY

Comparison at a Glance

Match type	Security	Ease of Engineering	Cost effectiveness	Note
On-device				**Loss of portability**
Server-side (crypto reader)				**Doesn't yet exist**
Server-side (reader w/o crypto)				**Current standard**
Client-side				**Secure for local locking**
Fuzzy vault				**Doesn't yet exist**

RSA SECURITY

RSA SECURITY

The Most Trusted Name in e-Security

WWW.RSASECURITY.COM