Jean-François MAINGUET
Atmel-Grenoble, Avenue de Rochepleine, BP 123, 38521 Saint-Egrève, France
Biometric consortium conference 2003
Agenda

- Introduction
- Requirements
- Biometrics selection
- Fingerprint
  - Hardware selection
  - Software implementation
- Convenience & Security
  - Security related parameters
  - Legal aspect
- Conclusion: more security, more applications
Introduction

Are you using the password application on your PDA? Why?

- Hassle to remember a password
- a 4-PIN number seems a poor protection
- People are looking at you when you are typing your PIN/password
- Even enabled, generally activated only after hours without use
Introduction (2)

- **Biometrics can help!**
  - No password, people may look at you
  - Ease of use: each time you start your PDA, you can check
  - More secure for your private data!

- **How adding biometric features in a PDA?**
  - What biometrics? At what cost?
Requirements

If you are a PDA maker, what requirements will you ask for?

- Built-in technology
  - users does not want to hassle with additional hardware
  - more secure

- 1. Low cost
- 2. Small form factor
- 3. Easy to use, fast
- 4. Reliable
- 5. Industrial device / mature technology
- 6. Acceptance (by users)


**Biometrics selection (1)**

- **Signature recognition**
  - already available, but only as third-party soft.
  - Reliability / acceptance by users / not high-tech?

- **Voice recognition**
  - microphone already built-in, software available
  - poor reliability / “talking to your PDA” effect

- **Hand geometry, vein recognition**
  - too large sensor

- **Iris/retina recognition**
  - autofocus camera
    - too large
    - too expensive
  - reliable
Biometrics selection (2)

- **Face recognition**
  - low cost if camera already built-in
  - recognition rate not very accurate, but enough for a low security application
  - acceptance by users / passive recognition

- **Fingerprint**
  - very similar to typing a password (finger use)
  - accuracy is well-known (police)
  - "ease of use" most difficult point as most people are not used to fingerprinting.
## Fingerprint sensors
- flat device required
- classical optical system too large
- silicon sensors
  - physical effect: capacitive, thermal...
  - static: square sensor
  - sweep: smaller form factor and less expensive
    similar to credit card swipe
- mature / industrial technology required
Fingerprint swipe sensor
Costs reduction

- Silicon price directly linked to silicon area

Wafer cost is the same whatever the chip area

Ratio for chip area 4 / 1
Ratio for candidates 4.5 / 1
Software implementation

- **Driver**
  - must help the user to easily acquire a fingerprint
  - very high priority, or the user may be “locked out”

- **Authentication software (bioengine)**
  - enrollment -> signature/template storage
  - authentication

- **Applications**
  - password application
    - adjust parameters -> ease of use = only few parameters
    - enroll
  - logon
  - training
Applications

Select mode

Training

Password

Password OR fingerprint
No password
Simple 4 digit PIN
Strong alphanumeric password
PIN OR fingerprint
PIN AND fingerprint
Password OR fingerprint
Password AND fingerprint
Fingerprint-only

Training -- Learn by Example

Please follow the demonstration to swipe a finger.

GOAL: 6 out of 8 successful swipes

Restart
Applications (2)

Enroll

- Settings
- Fingerprint
- Good. Please continue!
- Progress %
- Discard
- Training
- Go Back

Logon

- Password
- Enter your PIN or swipe one of the enrolled fingers.
- PIN
- Fingerprint
- About
Convenience & Security

What security?
- Absolute security does not exist
- Protect the internal data / not the device!
- External memory card not protected (software to add)
- Compared to password: increased security, convenient

Parameters
- Simple security levels: do not hassle the user with complicated parameters!
  - Levels: regular / high / very high
  - Number of authorized trials before clearing the memory
- Password still necessary for remote access
  (IR, Wi-Fi, Bluetooth, USB)

Legal
- no database / no name
HP iPAQ h5450 / h5550
First PDA with built-in biometrics
- Release at Comdex, Nov 2002
- FingerChip sensor from Atmel
- Cogent authentication software
More? / Conclusion

More security
- Use fingerprint AND password
- Multi-biometrics: unlikely for PDA
- Use a smart card for “match on card” and portability (your “identity is inside the smart card”)

More applications
- Encryption of data using fingerprint as a key
- Electronic signature
- Electronic commerce
- Personal access control device: the "door" asks
  - your (wireless) device, properly registered (what you have)
  - sweep your finger (what you are)
  - ask your password (what you know)
- ...

!!
More?
!!