Polymer fingerprint sensors for biometric system-on-card applications

Ralph W. Bernstein, CEO  IDEX ASA
Outline

1. About IDEX
2. The challenge; Identity fraud a massive problem
3. Biometrics for ID, transactions and access control
4. Biometric system-on-card
5. SmartFinger® Film
6. Summary
Our vision

IDEX shall ensure safe, secure, and simple use of personal ID.
Our business

IDEX develops and delivers world leading swipe fingerprint sensor technology, products and authentication solutions.
About IDEX ASA

- IDEX is headquartered at Fornebu (Oslo), Norway with representative offices in France (Europe) and Philippines (Far East)
- IDEX has recently released the ground-breaking, thin and flexible SmartFinger® Film fingerprint sensor family and embedded authentication solution
- SmartFinger® Film, is a winner of the Sesames Awards For the best IDENTIFICATION / ID CARDS application.
- IDEX is a public company and shares trade at the Oslo Axess list at Oslo Børs (Oslo Stock Exchange)
The challenge

Identity fraud – a massive problem
Chip and PIN is Broken

Steven J. Murdoch, Saar Drimer, Ross Anderson, Mike Bond

University of Cambridge
Computer Laboratory
Cambridge, UK

http://www.cl.cam.ac.uk/users/sjm217,sd410,rja14,mkb23

X. CONCLUSION

We have shown how the PIN verification feature of the EMV protocol is flawed. A lack of authentication on the PIN verification response, coupled with an ambiguity in the encoding of the result of cardholder verification as included in the TVR, allows an attacker with a man-in-the-middle to use a card without the correct PIN. This attack can be used to make fraudulent purchases on a stolen card. We have shown that the live banking network is vulnerable by placing a transaction using the wrong PIN, with every major UK bank and foreign banks too. The records indeed falsely show that the PIN was verified, and the money was actually withdrawn from an account.
GERMAN "SECURE" ID CARDS COMPROMISED ON NATIONAL TV

A German TV program showed hackers from the Chaos Computer Club using off-the-shelf equipment to extract personal information from the government's new "secure" ID card, which stores scans of fingerprints and a six-digit PIN that can be used to sign official documents and declarations.
Identity fraud - a massive problem

- Identity theft is increasing rapidly
- Substantial cost related to fraud:
  - 55 bill. USD in USA
  - 1,2 bill. £ in UK
- Added security is required for ID, transactions and access control.
- **Fingerprint biometrics is an obvious solution.**
Two-Thirds of Consumers Prefer Credit Card Verification by Fingerprint, According to Unisys Poll

- **BLUE BELL, Pa. – October 14, 2010** – A recent online poll by Unisys Corporation (NYSE: UIS) reveals that consumers trust fingerprint biometrics when using a credit card or over photo identification, PIN numbers or handwritten signatures to verify their identities requesting personal information.

- Responding to the question, “Which do you believe is the safest method to prove your credit card is being used by you?” the online poll found that 63 percent preferred fingerprints as the best method for identity verification and authentication.

Biometrics for ID, transactions and access control
Fingerprint authentication

Sensor

Acquire fingerprint data

Requires computing speed and RAM

Reconstruct image

Requires computing power and RAM

Feature extraction

Match against template

Less Resource demanding

YES/NO
Biometric cards; 3 approaches

1. Biometric template-on-card
2. Biometric match-on-card
3. Biometric system-on-card
1. BIOMETRIC TEMPLATE-ON-CARD

1. Fingerprint images or templates stored on card
2. Fingerprint transferred from card to reader
3. Extraction and match on reader

Requires infrastructure of readers for enrollment and verification
2. BIOMETRIC MATCH-ON-CARD

1. Fingerprint templates stored on card
2. Fingerprint transferred from reader to card
3. Feature extraction takes place on reader
4. Matching takes place on card

Requires infrastructure of readers for enrollment and verification
The solution

Biometric system-on-card
Fingerprint ID for the mass-market

Key aspects

1. Security and convenience
   - Multifactor authentication
   - Avoid PIN codes and passwords

2. Privacy
   - Avoid centralized databases of fingerprints
   - Secure storage of personal information

3. Utilize existing infrastructure
   - ATMs and terminals
   - Internet
   - Enterprise systems
   - Access gates
3. BIOMETRIC SYSTEM-ON-CARD

1. Fingerprint template stored on card
2. Enrollment, extraction and match takes place on card
Fingerprint information never leaves the card
Does not require infrastructure for enrollment and verification

3. BIOMETRIC SYSTEM-ON-CARD

1. Fingerprint template stored on card
2. Enrollment, extraction and match takes place on card
Biometric system-on-card

- **All-in-one**: Fingerprint reader incorporated in the card
- Fingerprint information stored on card only
- **On-card** enrollment and verification
- Fingerprint information never leaves the card

Display (visual OTP)

Fingerprint reader
(No biometric data is transmitted from the card)

VALIDcard™
Personal security for every card you own

- **Stand-alone** biometric systems incorporated in the card
- **Independent** of centralized databases and external readers
- Suitable for *mass market* applications
- Ensures safe, secure, and simple use of personal ID in the everyday life
One-time-password (OTP) cards

- Credit & Debit cards
- ATM access
- Online banking
- Secure Network Access
- Secure Online purchases
- Point of sales
- National and governmental ID
Use case examples

**Online Bank Login**

1. User enters username.
2. User generates One-Time Password (OTP) by swiping finger on VALIDcard™.
3. User enters OTP.
4. OTP is authenticated and access is granted.

**ATM Access**

1. User inserts ATM Card.
2. User generates One-Time Password (OTP) by swiping finger on VALIDcard™.
3. User enters OTP into ATM keypad.
4. OTP is authenticated and access is granted.
A variety of applications and markets

- Online bank login
- Online purchases
- Point of sales
- ATM access
- Physical & logical access

- Financial institutions
- Universities
- Health care
- Governmental ID
- Airport security
IDEX SmartFinger® Film

Next generation fingerprint sensor technology
The SmartFinger® Film technology

• IDEX’ next generation fingerprint sensor technology
• Based on state-of-the-art polymer manufacturing and offers small, ultrathin and flexible fingerprint sensors
• Technology and products are covered by approved and filed IDEX patents

• SmartFinger® Film raises card security to the next level by incorporating biometric ID within existing systems.
Presenting the most versatile swipe fingerprint authentication solution

SmartFinger® Film

- *World’s thinnest*, flexible swipe fingerprint sensor
  - Thin (0.35 mm)
  - Flexible
  - Customization of sensor geometry
- *Smallest software footprint* for embedded authentication solutions
SmartFinger® Film - designed for card integration

- Sensing area: 0.05 mm thick
- Electronics: 0.35 mm thick
- Connector
The SmartFinger® sensor family

- Industry's thinnest and most flexible - 0.05 mm thick
- Unsurpassed image quality and biometric performance (false rejection, false acceptance)
- Compliant with ISO Card form factor
- A variety of customizable geometries available
- Alternative I/O connections, ZIF, ACF and BGA
- On-board micro controller capability
SmartFinger® embedded biometric system

- Small software footprint
- Minimal hardware resources required
- On-device enrollment, template storage and verification
- Based on ARM7 and Cortex M3 microcontroller cores
Products

- Biometric system-on-card
- Biometric tokens
- Biometrics USD sticks
- PC peripherals
- Handheld devices and mobile phones
Summary

• ID theft and fraud is an immense problem in the society.
• Biometrics verification is an obvious solution in order to add security and multifactor authentication
• System-on-cards may solve challenges related to introduction of fingerprint ID in mass markets
• IDEX’ groundbreaking SmartFinger® Film fingerprint sensor technology and authentication solution is especially suited for system-on-card applications