# Liveness Detection

## Biometrics 2006
## London, Sept 18

**Jean-François Mainguet**
**Biometrics Chief Scientist**

*Everywhere You Are®*

*www.atmel.com*

# Agenda

- Problem description
- Electronic & Aliveness Security
- Other ways to secure a system
- Copying biometric traits
- What is life? How to detect liveliness?
- Some liveness detection systems

FingerChip®

# The Problem

- New security feature => new workarounds
- Biometrics => *fake/cut fingers* problem
- Most biometric systems cannot detect liveliness.
- Even a perfect system, won't stop bad guys from trying to cut a finger or remove an eyeball.

FingerChip®

# "I agree to the transaction"

- Proving that you are living is not enough.
- What is desired is to prove that:
  - I'm a living person not under threat, and I agree to make such and such action
- This is impossible: you can't read a person's mind.
- Once again, 100% security does not exist.

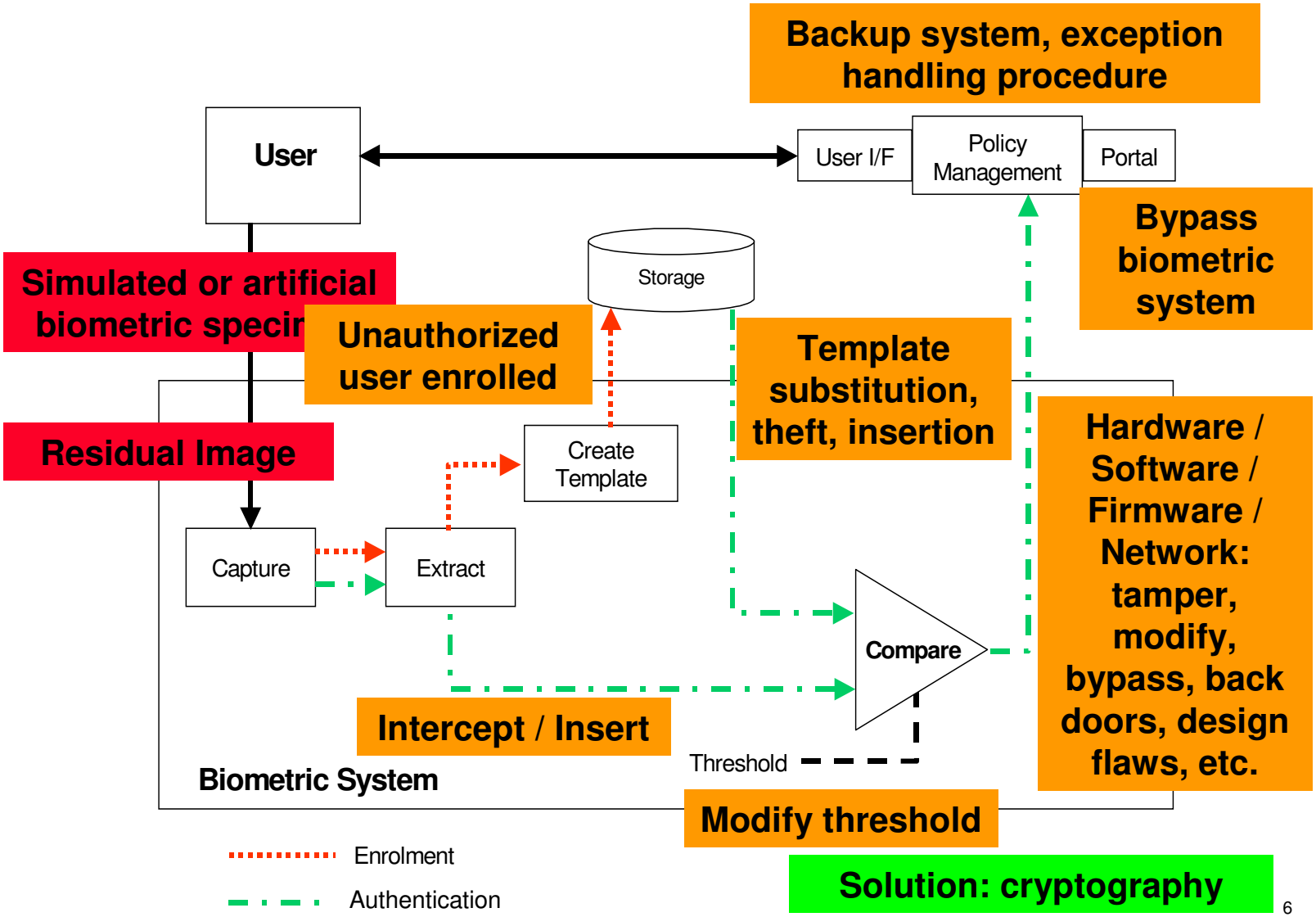
FingerChip®

# Electronic & Aliveness Security

- Security of an (electronic) biometric system may be divided into two main areas:
  - Electronic security
    - Is it an authorized biometric system at the other end of the wires?
  - "Living" security
    - Is this finger alive, fake or dead?

FingerChip®

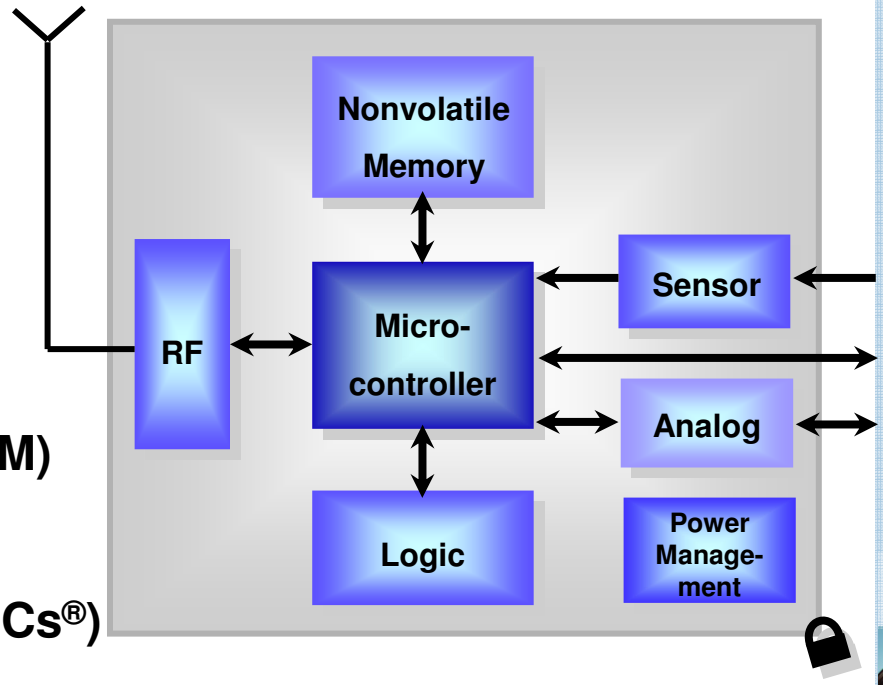
# Biometric System Security




# Atmel Secure Solutions

## Atmel is a market leader in Secure Solutions:

- Secure Microcontrollers
  - AVR® and ARM®
  - Smart Card IC Readers
- Transaction Processing ICs
- Trusted Platform Module (TPM)
- Secure RF
- RF Identification Devices (IDICs®)
- CryptoMemory®
- Biometrics
  - FingerChip®




*Atmel secure products are qualified to some of the highest security standards in the industry*

FingerChip®

# Security breaches

- Weakest point is always attacked
- Enrollment / storage
  - Enrollment is mandatory.
  - Someone (a trusted person?) will make the link between the real person and the recorded biometric trait.
    - Fingerprint enrollment by mail, using ink and paper is NOT a secure way
  - What if the recorded fingerprint (on a smart card for instance) is later corrupted?

# Security breaches

- Attended / unattended system?
  - Attended:
    - Aliveness detection is likely not useful.
    - Do you better trust a person or a machine?
    - You can show your finger to say:
      “This is a true finger, not a fake!”
  - Unattended:
    - Aliveness detection is desirable.

# Increasing security

- Aliveness detection is not the only way to increase security:
  - You may require three fingerprints: it is more difficult to get three fake fingers than one
  - Layered biometrics: using face AND fingerprint AND iris
  - Add a token: a phone, a smart card
  - Share a secret: a specific finger may be used as a silent alarm
  - Add a password (something you know)

FingerChip®

# Compromised biometric traits

- Common belief: If your fingerprint (face, iris…) has been copied once and used to spoof a system, then you cannot reuse it.

  It is *compromised*.

- Solutions:
  - Aliveness detection
  - Encryption: Cypher / sign the recorded biometric trait, so you can revoke this record.
    - If someone steals your credit card with your fingerprint inside, then it is possible to reject this card; the fake is of no use with this card.
  - Distortion: This is a kind of encryption at biometric trait level. A random distortion is applied, and this is the shared secret that can be revoked. [Ratha]

FingerChip®

# Aliveness detection levels

- **Aliveness: hard to detect**
  - **What is a dead finger?**
    **A surgeon is able to mend a cut finger (if kept in ice)!**
  - **Whole hands have already be transplanted from a deceased donor: also the fingerprints!**

- **Definition of levels:**
  - **Zero effort: a latent print left on the sensor**
  - **Fake/copies:**
    - **Fingerprint image**
    - **Fake made of gelatin, latex…**
    - **Thin layer of material glued to a real finger**
  - **Original finger:**
    - **Cut out**
    - **Belonging to a dead person**

# Key on the lock: sweep is better

- It is possible to reactivate the latent print left on the sensor (the lock!).
- Sweep technique avoids this.

Reactivating latent prints: cooling device with cold water, breath. Zero effort.

# Copying biometric traits

- Biometric information is often public.
  - Think about face recognition!
  - You cannot rely on the biometric data secrecy!
- Donor cooperation helps but is not mandatory.
  - DNA: just pick up organic residues
  - Face: a simple photo
  - Iris: a good high resolution photo
  - Fingerprint: latent prints
  - Voice: a recorder
  - Hand: a mold
  - Vein: no visible trace
- Having the original sensor device helps.
  - You get a genuine electronic copy!
  - And so, you can create a fake to spoof this sensor…

FingerChip®

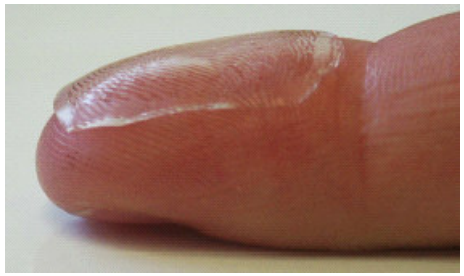
# Copying biometric traits

- How difficult is it to make a fake finger?
  - With cooperation
    - Making a mold is quite easy, and you can find information over the Internet.
    - Most articles dealing with this suppose cooperation.
  - From a latent print
    - Having the right latent print is not so obvious. (It is difficult to know which finger it is!)
    - Identifying the latent print is very often difficult, even for a forensic professional.
    - From a good picture, making a mold is not too hard; like a rubber stamp or a printed board.
- We consider that making a latex copy is difficult, but far from being impossible.

FingerChip®

# Dead/Cut Finger

- **Even with a fake finger detector, making the difference between a live and a dead finger will be difficult.**
  - What is the difference between a dead and live finger? Pretty small… remember that a surgeon can mend a cut finger, and so it is still "living" for a few hours.
  - Blood pulse is likely to be a good criteria, but quite a large population shows the Raynaud's phenomenon (blood circulation almost stopped, and fingers are becoming cold).



- **A thin, transparent layer of latex over a real finger will be extremely hard to detect.**
- **It is possible to grow skin cells (to replace severely burned skin): what about creating a "live" fingerprint...**
- **What if someone "scalps" the fingerprint skin?**

FingerChip®

# Life criteria

- What is life? How detecting life?
- Passive: use some specific physiological data
  - Example of the fingerprint
- Active: response to a stimulus
  - Voluntary or involuntary

FingerChip®

# Physiological data about fingers

- Cells, a bone, and a nail make a structure of about 1 to 10cm3. Note that there is no muscle (and so electrical activity is coming from other areas).
- Arterial blood brings all chemicals, oxygen and heat. Return to the body in veins.
- Skin is composed of three layers:
  - Stratum corneum made of dead cells, more or less hydrated, 100µm thick, very variable electrical conductivity
  - Blood-free epidermis, 0.05 to 1mm thick made of proteins, lipids, melanin-forming cells
  - Dermis: dense connective tissues, capillaries arranged in vertical loops.
- Arteriovenous anastomoses, innervated by nerve fibers regulate the blood flow of a factor of 30 in response to heat.
- Temperature range: 10°C to 40°C, not regulated.
- Skin emits some specific molecules (odor).
- Skin presents some plasticity.

FingerChip®

# Physiological data about fingers

- Remark: The external layer of the skin is made of dead cells, which is not a favorable configuration for aliveness detection!
- Any aliveness detection reader should read one or several data related to the previous list!

FingerChip®

# Bodily Response to a Stimulus (Challenge-Response)

- **Involuntary** (reflexive) challenge-response:
  **A stimulus induces an automatic physiological change or reaction within the user.**
  - the response of muscles to electrical stimulation (electromyography EMG)
  - the response of the pupil to varying light levels
  - the dynamic change in the color of skin when pressure is applied
  - the rapid movement of a hand when shocked
  - the reflex of a knee when struck

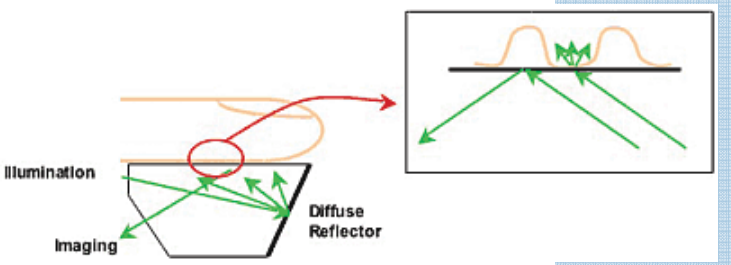
- **Voluntary** (behavioral) challenge-response:
  **User provides a logical response to a prompt generated by the system. Tactile (thermal, electrical, poke) stimulation involves feeling something and saying or doing something in response.**
  - Touch Button A if the platen is hot or touch Button B if the platen is cold.
  - Remove the feature from the platen when you feel an electrical impulse.
  - Enter the number of pokes felt by the finger.
  - Visual stimulation involves seeing something and saying or doing something in response.
  - Auditory stimulation involves hearing something and saying or doing something in response.

  - the closest to your brain, so to your **identity**!

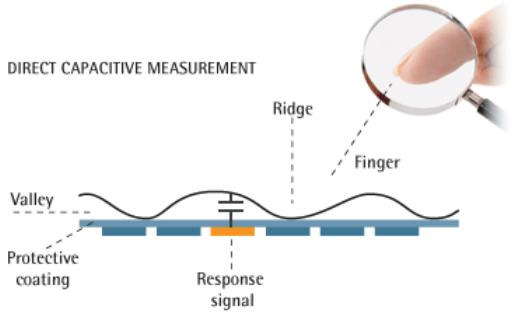
FingerChip®

# Fingerprint sensors

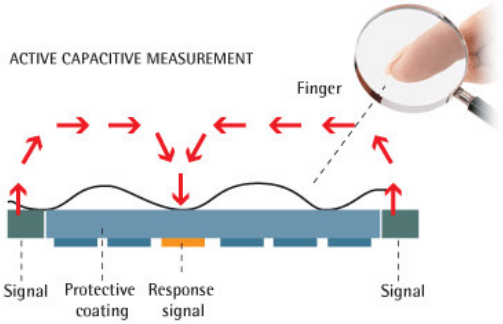
- **Optical sensors**
  - Very sensitive to the hydration level of the skin =>gummy fingers
  - No direct aliveness content in basic sensor




- **Capacitance sensors**
  - Distance between the skin and the pixel is measured thanks to a capacitive effect = sensitive to hydration.
  - No aliveness content in the capacitance data

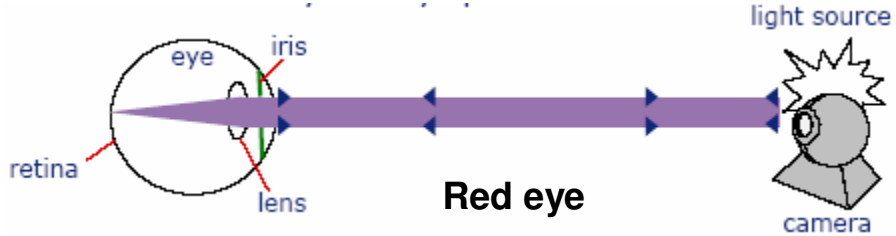



- **RF & electro-optical sensors**
  - use skin conductivity = sensitive to hydration
  - To spoof these sensors, a conductive fake is required
    - In that sense, this can be announced as a anti-spoof feature (latex does not work).




FingerChip®

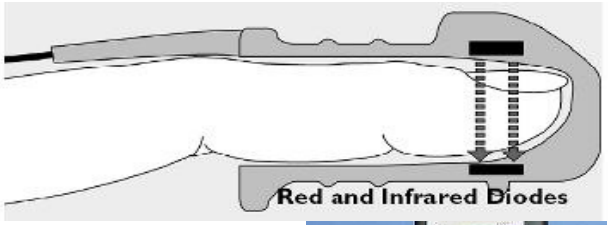
# Some liveness detection systems




Red eye

Skin distorsion (Maltoni)

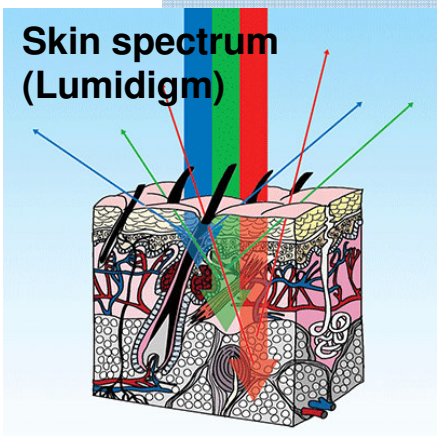
Skin impedance (Guardware)



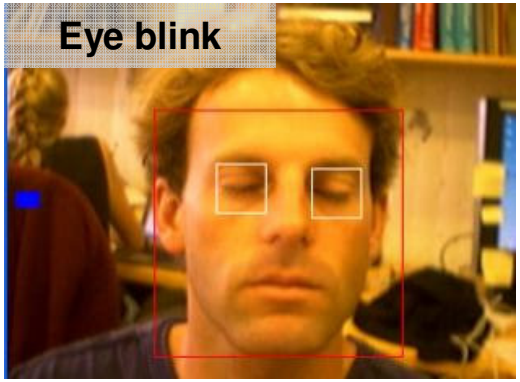

Pulse oxymetry associated with an optical fingerprint sensor

pupillary light reflex / hippus

Skin spectrum (Lumidigm)



Eye blink



Perspiration (Schuckers)

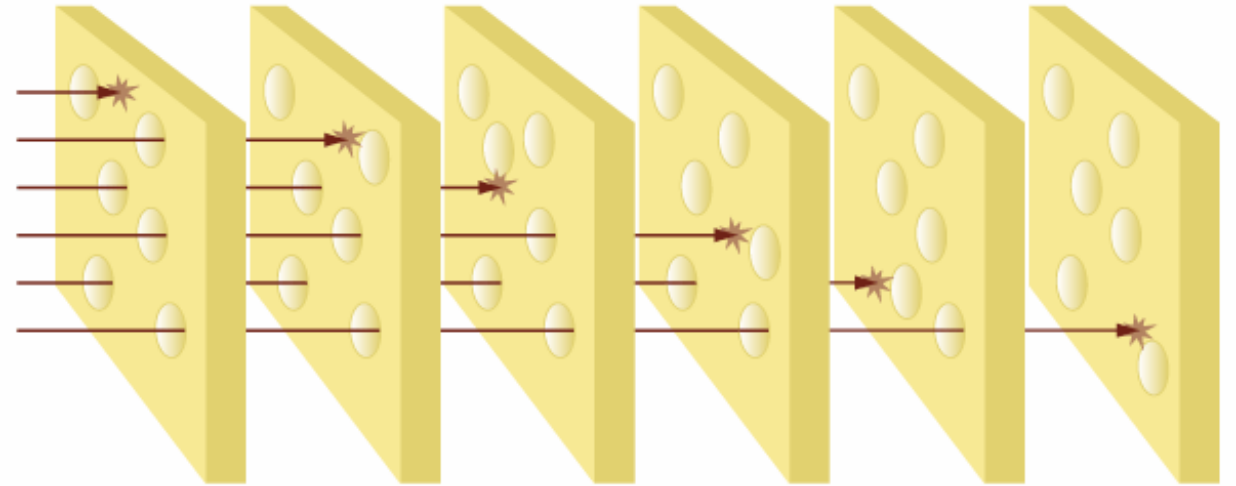
# Faking the counter measures

- Remember that any measurement can be faked:
  - Electrical method can be faked by the appropriate voltage applied on the sensing area (or even a simple connection to real skin while a fake is applied).
  - Optical methods can be faked by the appropriate plastic with the correct absorption characteristics.
  - An optical sensor is made of photodiodes: it is always possible to send the appropriate light, synchronized with the light sent by the system.
  - Cardiac pulse can be faked with the appropriate pump and pipes.

FingerChip®

# Conclusion

- 100% secure is a myth.
- But — several different sensors reading different information at the same time will be very hard to deceive.
  - The “Swiss cheese” model: Each slice is not 100%; some holes exist. More slices will stop most of threats.
  - But at the cost of each slice!



# Open-Source References

- Six biometric devices point their finger at security
  - Network computing – Jun 1998 / Fingerprint
- Biometric security
  - PC magazine – Feb 1999 / Fingerprint / face / voice
- Fingerprint recognition–don't get your fingers burned
  - Van der Putte, Keuning, Jan 2000
- Impact of artificial "gummy" fingers
  - Matsumoto, Jan 2002
- Biometric access devices & programs put to the test
  - c't magazine, may 2002 / Fingerprint / face / iris
- Thesis: Liveness Detection in Fingerprint Recognition Systems
  - Marie Sandström, Linkoping 2004, Sweden

FingerChip®