WHY I HACKED TOUCHID
(AND STILL THINK IT'S AWESOME)

Marc Rogers
Lookout
www.lookout.com

Agenda

- Fingerprint Biometrics - How it works & How it doesn't.
- IsTouchIDHackedYet?
- Now what?

FINGERPRINT BIOMETRICS

How Fingerprint Scanners work

Enrollment

1.The subject's finger is scanned.
2.The scanned finger is analyzed and key features are identified and mapped.
3.These features are stores as a template in the systems fingerprint database.

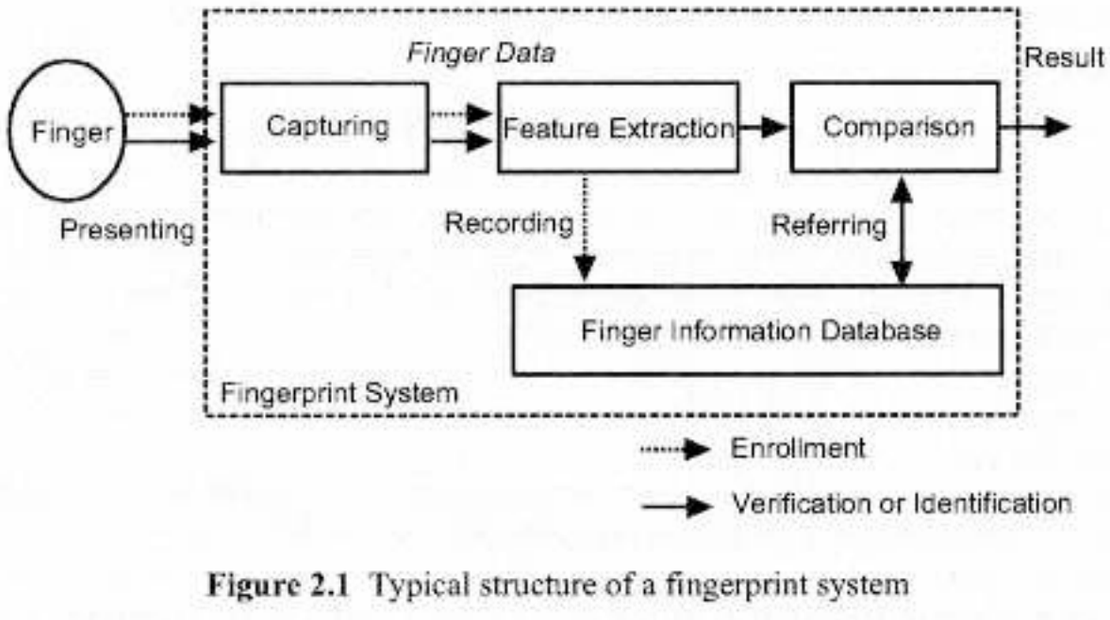
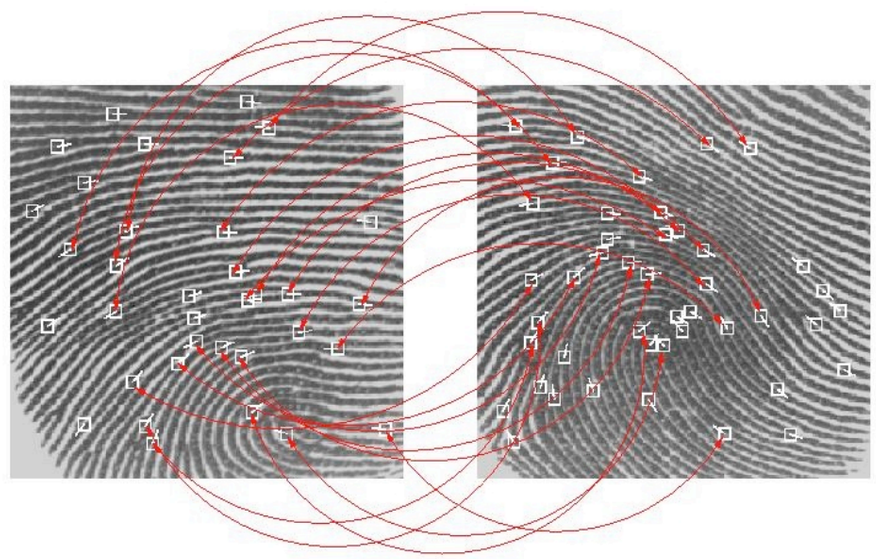


Figure 2.1 Typical structure of a fingerprint system

Source: Courtesy of Identicator Technology

Authentication

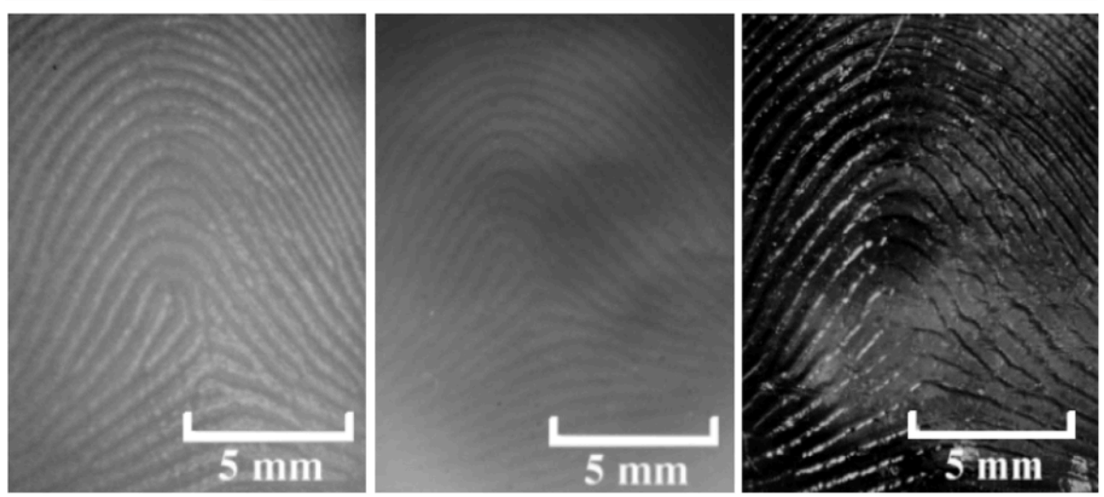
1.The subject's finger is scanned.
2.The scanned finger is analyzed and key features are identified and mapped.
3.These features are compared to the enrolled templates in the fingerprint database.



How Fingerprint Scanners FAIL

- Fingerprint scanners rely on a credential which we leave on everything we touch.
- If you can capture & reproduce the fingerprint detail you can perform replay attacks.
- Yes, gummy bears do work on MANY systems, although pure Gelatin is better.

- Gelatin is a protein made from animal skin so it has properties very similar to human skin.
- So its effectiveness in fingerprint replay attacks is not that surprising.



(a) Live Finger (b) Silicone Finger (c) Gummy Finger

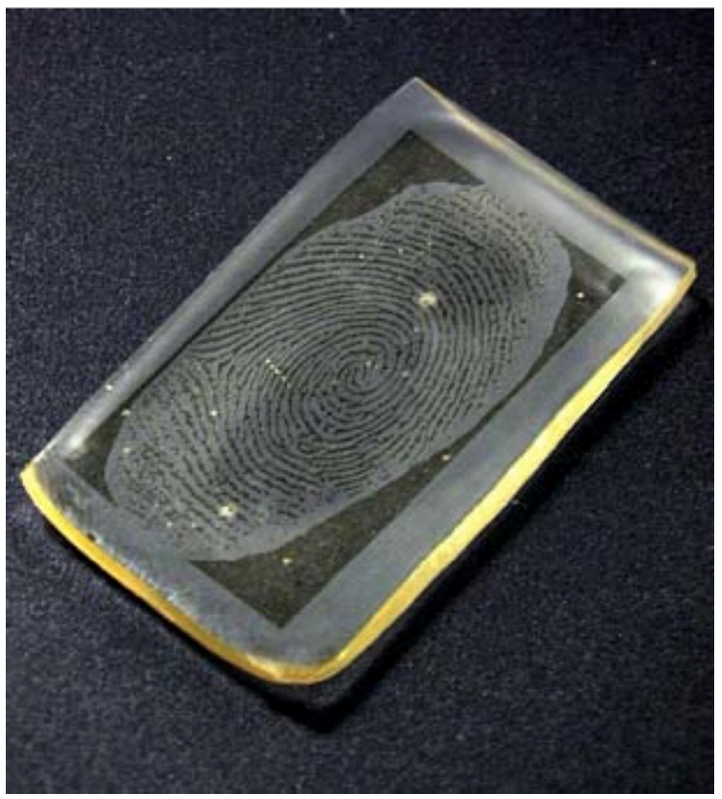
- I have seen systems where just BREATHING on the screen develops the last fingerprint enough for the system to accept it as a valid fingerprint.

Defeating Modern Fingerprint systems

- Matsumoto et al 2002
- CCC et al 2004

- An arms race began between manufacturers and hackers.
- Initially manufacturers just increased the resolution of their scanners enabling them to easily reject smudged copies.
- Today Most decent modern fingerprint scanners also use “LIVENESS” tests to reject “Gummi” fingers or other simulacra.
- Something else was needed.....

- Matsumoto tried a range of different substances and a number of different techniques to create mold from the photograph of a fingerprint.
- A mold created from an etched PCB board produced the best results and Gummi fingers made using these molds defeated fingerprint systems with a success rate of almost 70%
- CCC Found in 2004 that a thin layer of woodglue also defeated many systems with LIVENESS tests.



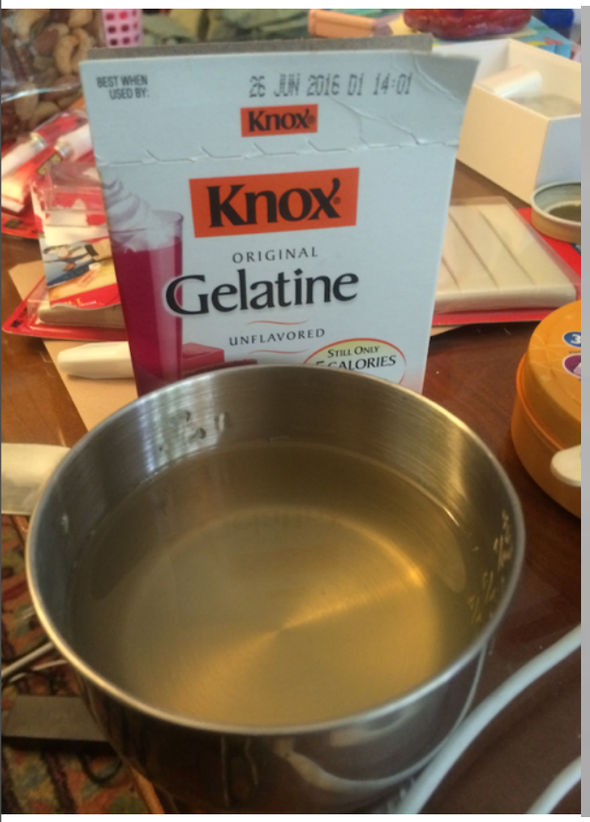
ISTOUCHIDHACKEDYET?

THE “LAB”


COPPER CLAD BOARD
COPPER CLAD BOARD
DANGER
Elmer's School Glue Gel
Elmer's School Glue
Plaster of Paris


ELMER'S
School Glue


brother


BEST WHEN USED BY:
26 JUN 2016 01 14:01
Knox
Knox
ORIGINAL
Gelatine
UNFLAVORED

TOUCHIDISHACKEDNOW

(52 HRS LATER)

BUT, WHAT DOES THIS MEAN?

But, What does this mean?

- Fingerprint security is NOT high security.
  - Fingerprint security IS convenience security.
- Street-thieves will NOT use fingerprint cloning techniques to unlock stolen iPhones.
  - They will just wipe them and sell them.

- Alone, fingerprint security should not be used to protect your banking details, your passport or your stolen top secret documents.
  - A PIN shouldn't be used here either.
  - Stick to cryptography with a recommended algorithm and a strong passphrase.

- Door locks have been defeated with increasing elaborate picking techniques as long as they have been around.... but we still use them.
  - Security DOESNT have to be perfect.
  - It just has to be ENOUGH.

- Today just 50% of people have a pin on their smartphone yet almost 70% of us bank with those same devices.
  - For those people, and anyone wanting simple convenient security, TouchID is AWESOME.

Next Steps?

- Its early days for TouchID and there is plenty of room for improvement.
- Lets stop talking about how broken it is and start talking about how it can be better.

- Here's what I would like:
  1. Multi-factor - I want to use TouchID with pins and even passphrases in situations where addition security is required.
  2. I want a configurable timeout. Right now if your phone hasn't been touched for 48 hrs you have to use a pin before you can use TouchID - I want to choose this value.
  3. I want a configurable failure threshold. - At the moment you get 5 attempts with a fingerprint before it falls back to PIN. I want to chose how many attempts. Like 2.
  4. This one is the big one: I want to chose where and when I am happy to sacrifice security for convenience. For example I want to use a fingerprint to open my photos but a fingerprint AND a PIN to open my banking app.

https://blog.lookout.com/2013/09/23/why-i-hacked-apples-touchid-and-still-think-it-is-awesome/

EVERYTHING GETS PWND

(BUT THATS OKAY)