All Things Security

Bypass Touch ID

With a Forged Fingerprint

9am - noon

J. Ivy Thomas
keybase.io/ivydigitalstorm

All Things Security

Agenda

9 am - 10:15	Bypass TouchID with a Forged Fingerprint Lecture & Demo
10:15 - 10:45	Break
10:45 - 12 pm	Bypass TouchID with a Forged Fingerprint Lab Exercises
12 - 1:30	Lunch
1:30 - 2:45	Locking down Mac OS. Lecture
2:45 - 3:15	Break
3:15 - 4:30	Physical Security & The Art of Lockpocking Lecture & Lab Exercise
5 pm	Dinner Evening Activities

Security Team

Pam Lefkowitz

@alwaysdns

Jennifer Unger

@quovadimus82

J. Ivy Thomas

@ivydigitalstorm

Shannon Barragan

@shan2104

All Things Security

Conduct and Safety

- ★ Activities covered in today's workshop are for academic purposes only and are not for use outside of the classroom
- ★ Lab methods include heating processes and use of chemicals
- ★ Laws regarding lock picks may vary per state http://toool.us/laws.html
- ★ Please maintain caution and awareness when participating in lab activities

All Things Security

Security. Right at your fingertip.

Touch ID

All Things Security

Bypass Touch ID

With a Forged Fingerprint

9am - noon

Ivy Thomas
@ivydigital

Your fingerprint is the perfect password.

You can always have it with you.

And no one can ever guess what it is.

Security. Right at your fingertip.

Touch ID

Touch ID Hacked in under 48 hours!

Defeating Apple's Touch ID: It's easier than you may think ...
arstechnica.com/.../defeating-apples-touch-id-its-easier-than... ▾ Ars Technica ▾
Sep 23, 2013 - Hacker Starbug overcame the purported ability of Touch ID to read prints at a .... The thief only has 48 hours to fool the sensor and then only the ...

Touch ID hack verified as legit - CNET
www.cnet.com/news/touch-id-hack-verified-as-legit/ ▾ CNET ▾
Sep 23, 2013 - Barely 48 hours after the iPhone 5S hit the streets, its Touch ID fingerprint sensor has been fooled by a Germany-based group called the Chaos ...

iPhone 5S Touch ID: Hacked by 'Star Bug' - ABC News
abcnews.go.com › Technology ▾
Sep 23, 2013 - A hacking group in Germany is claiming to have fooled the iPhone 5S fingerprint sensor and software, known as Touch ID, less than 48 hours ...

Touch ID fooled - not hacked - by a lifted fingerprint | iMore
www.imore.com/touch-id-fooled-not-hacked-lifted-fingerprint ▾
Sep 22, 2013 - To its credit, Chaos Computer Club isn't calling the spoof a hack, but that isn't stopping it from being widely misreported, thanks in part to the ... Getting the most of Mac IDUnlock your Mac with Touch ID ..... I gave it 48 hours. :-).

Touch ID Hacked Only 48 Hours After Release
www.itbusinessedge.com/.../touch-id-hacked-only-48-hours-after-release... ▾
Sep 23, 2013 - The much-heralded Touch ID on the new iPhone 5S has allegedly been hacked by a group of German hackers. It took all of 48 hours after the ...

ars technica

MAIN MENU ▾ MY STORIES: 25 ▾ FORUMS SUBSCRIBE JOBS ARS CONS

RISK ASSESSMENT / SECURITY & HACKTIVIS

Defeating Apple's Touch ID: It's easier than you may think

→ Touch ID Hacked Only 48 Hours After Release

Touch ID Hacked Only 48 Hours After Release

If you have finger-smudged glass, a laser printer, and latex milk, you can beat it too.

EDITION: US ▾

ZDNet SEARCH | STORAGE INNOVATION MOBILITY MORE ▾ NEWSLETTERS ALL WRITERS

MUST READ READING BETWEEN THE LINES OF NADELLA'S STATE OF THE UNION MISSIVE

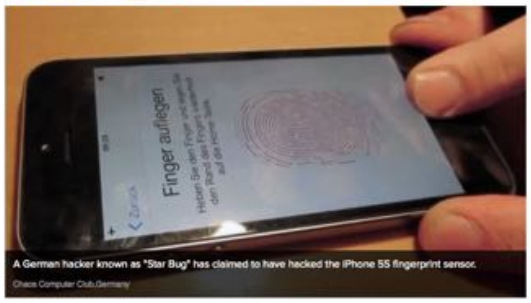
Apple's advanced fingerprint technology is hacked; should you worry?

Less than 48 hours after the iPhone 5s went on sale, a group of German hackers claimed to have lifted a fingerprint and created a fake finger that could spoof Apple's "advanced" biometric technology. But anyone who's been paying attention to biometrics wasn't surprised.

iPhone 5S Fingerprint Sensor Fooled by German Hacker Group

Sept. 23, 2013
By JON M. CHANG

Like 264 share 36 Tweet 86 +1 32 14 Comments



A German hacker known as "Star Bug" has claimed to have hacked the iPhone 5S fingerprint sensor.
Chaos Computer Club,Germany

All Things Security

istouchidhackedyet.com

No!

...but the following have offered a reward to the first person who can reliably and repeatedly break into an iPhone 5s by lifting prints (like from a beer mug):

Maybe!

The Chaos Computer Club in Germany may have done it! Awaiting video showing them lifting a print (like from a beer mug) and using it to unlock the phone. If so, they'll win...

Scope

Illicitly access stored Personal Identity Information (Pii)

Steal Touch ID Secure Enclave cryptographic key (UID)

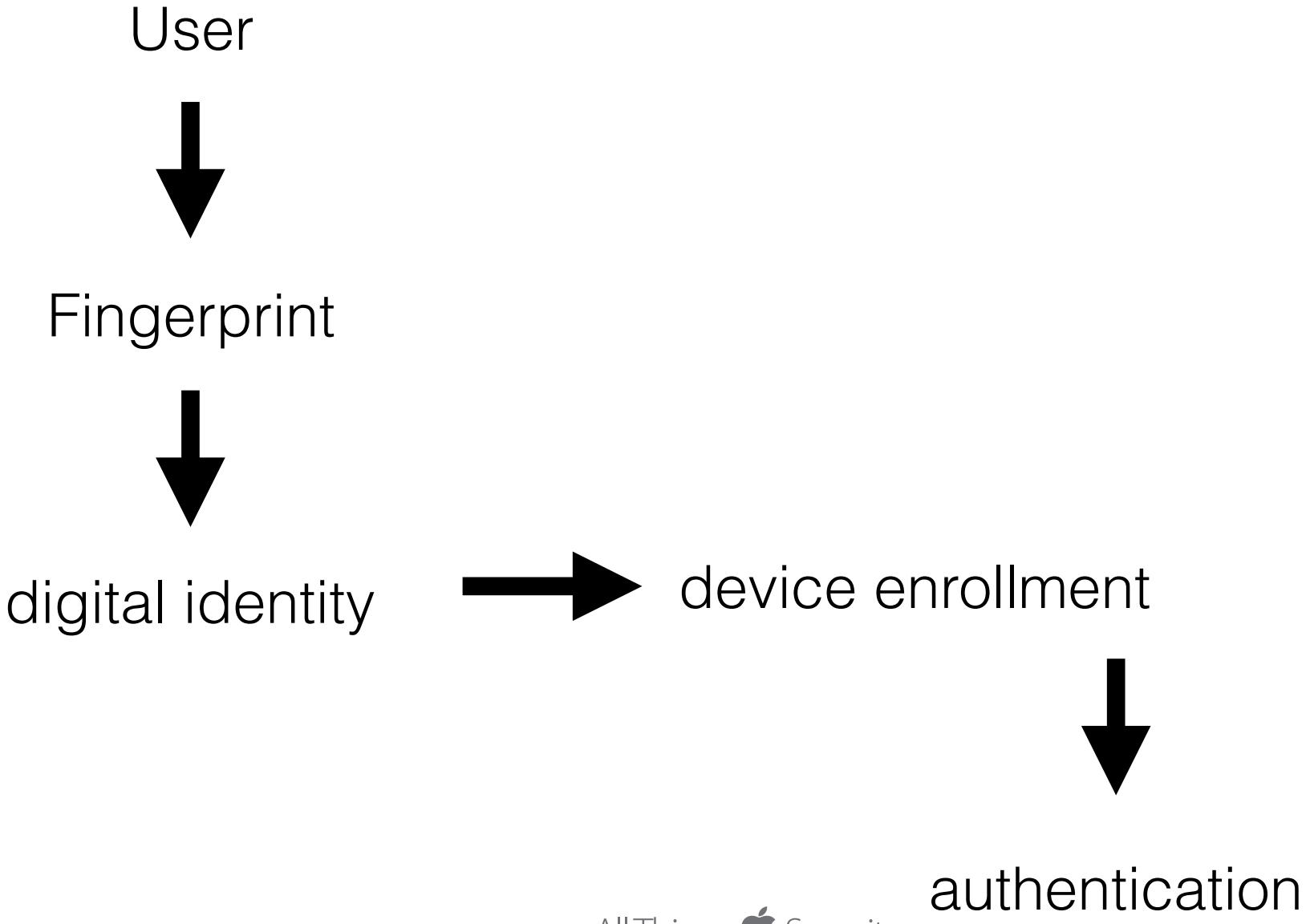
Unlock the iPhone using a forged fingerprint

All things Security

The Touch ID System

How does Apple do biometric authentication?

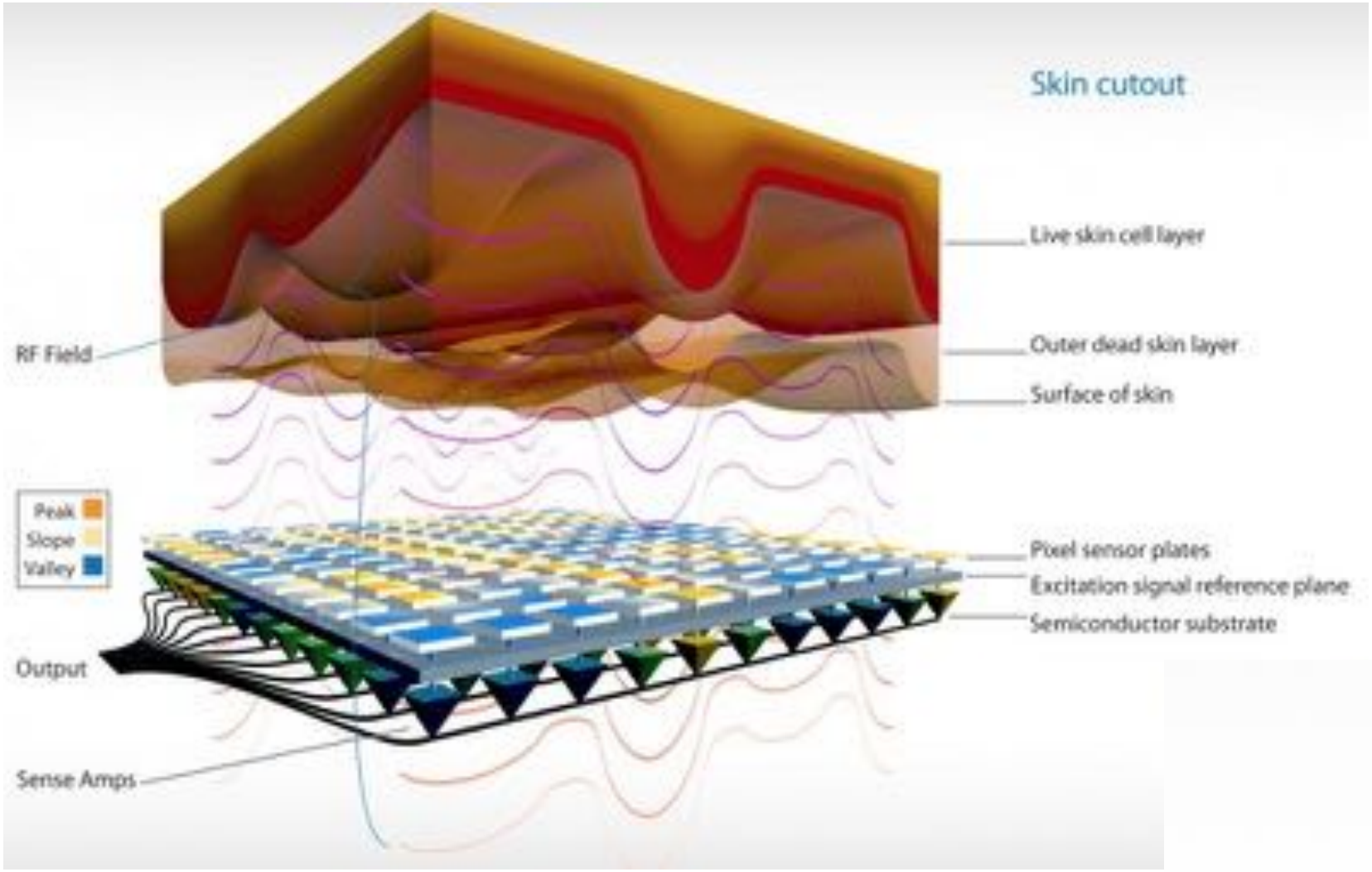
Enrollment - Logical



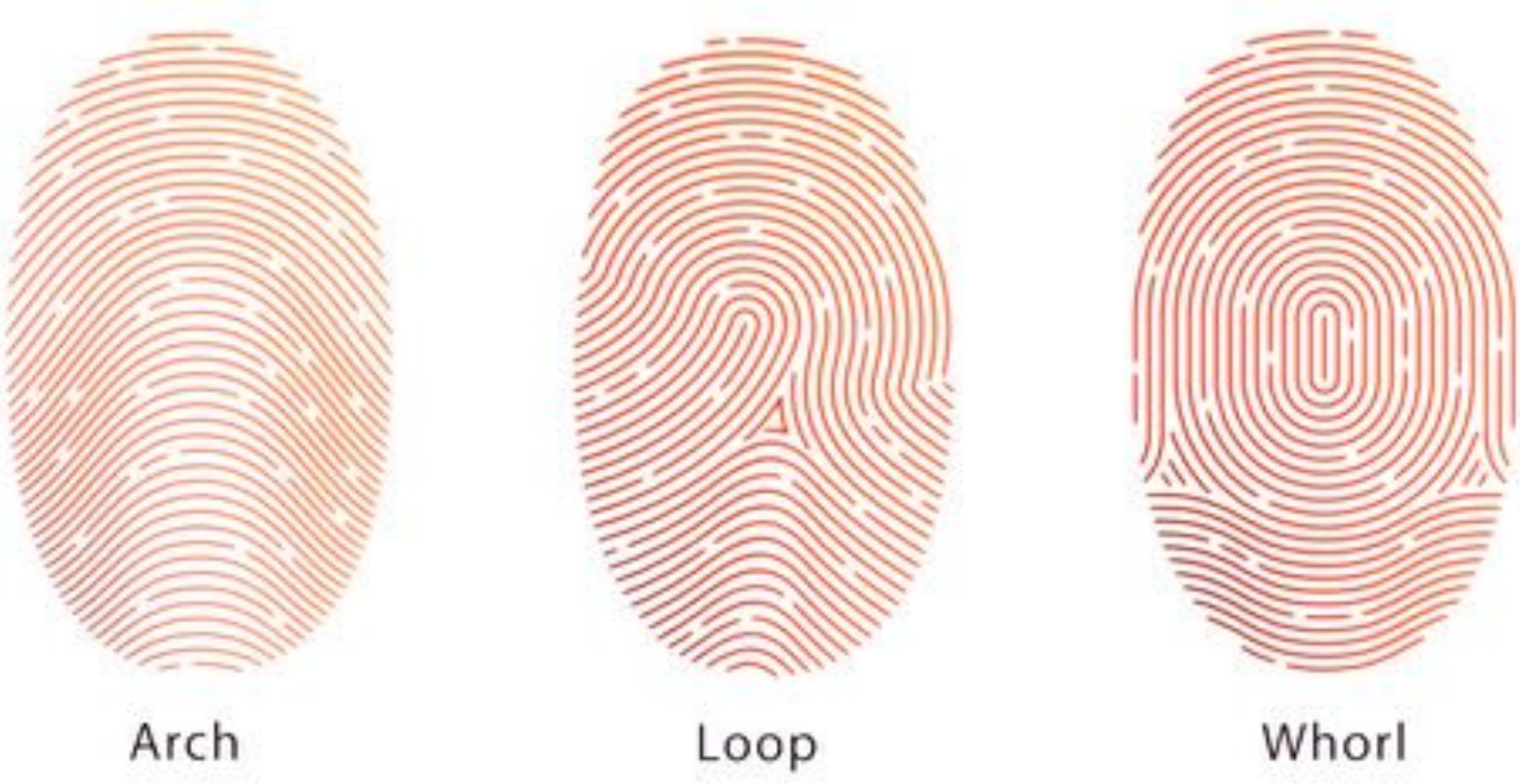
Touch ID - Systematic

The technology behind Touch ID.

Touch ID - Systematic



Touch ID - Systematic



Touch ID - Systematic

All Things Security

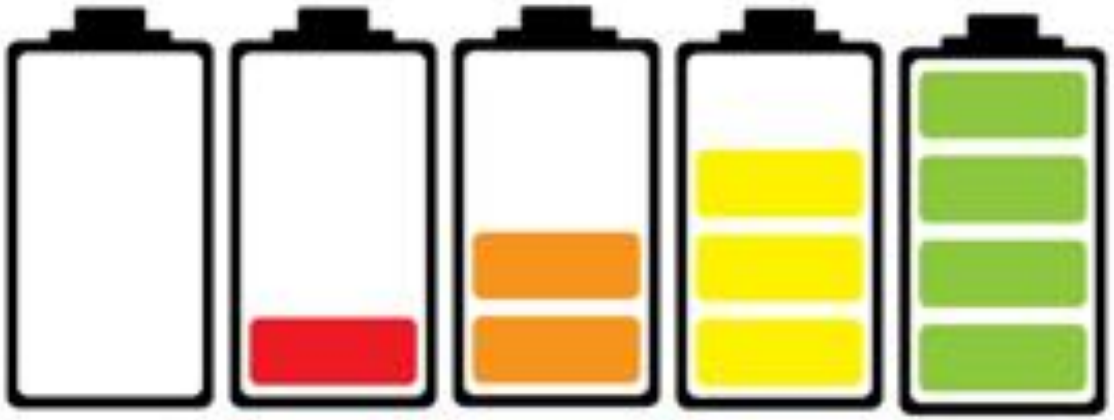
Touch ID - Systematic

Touch ID - Authentication

The technology behind Touch ID.

There's a lot of technology at work belov
Home button. Touch it and the surround
ring detects your finger and wakes the c
sensor. The laser-cut sapphire crystal sur
then directs the image of your finger to
reads beneath the outer layers of your sk
fingerprint. Software then reads the ridg
fingerprint and finds the match to unloc

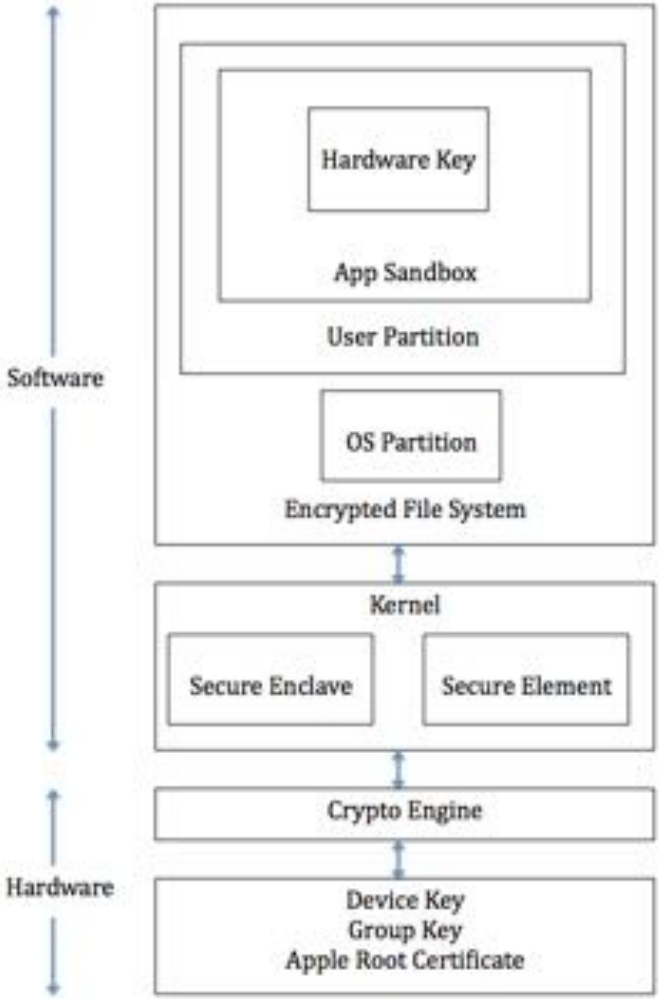
Built for Mobility

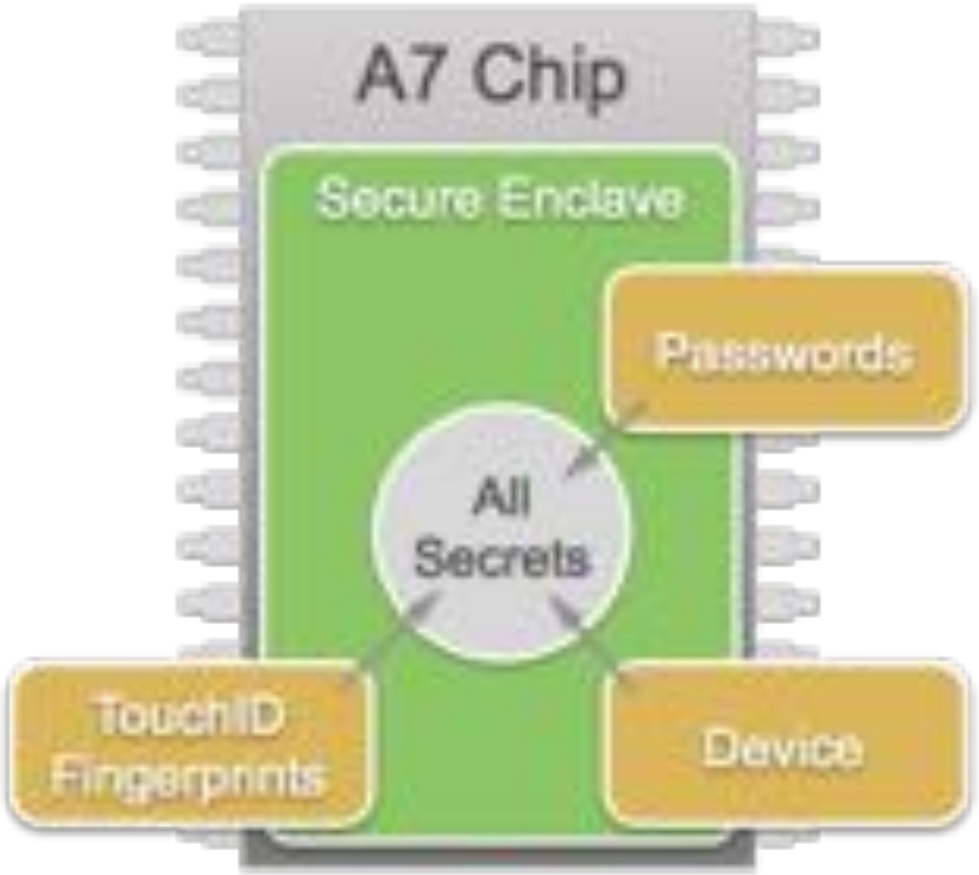


Touch ID Security Architecture

- ★ SEP
- ★ Secure Boot Chain
- ★ A7

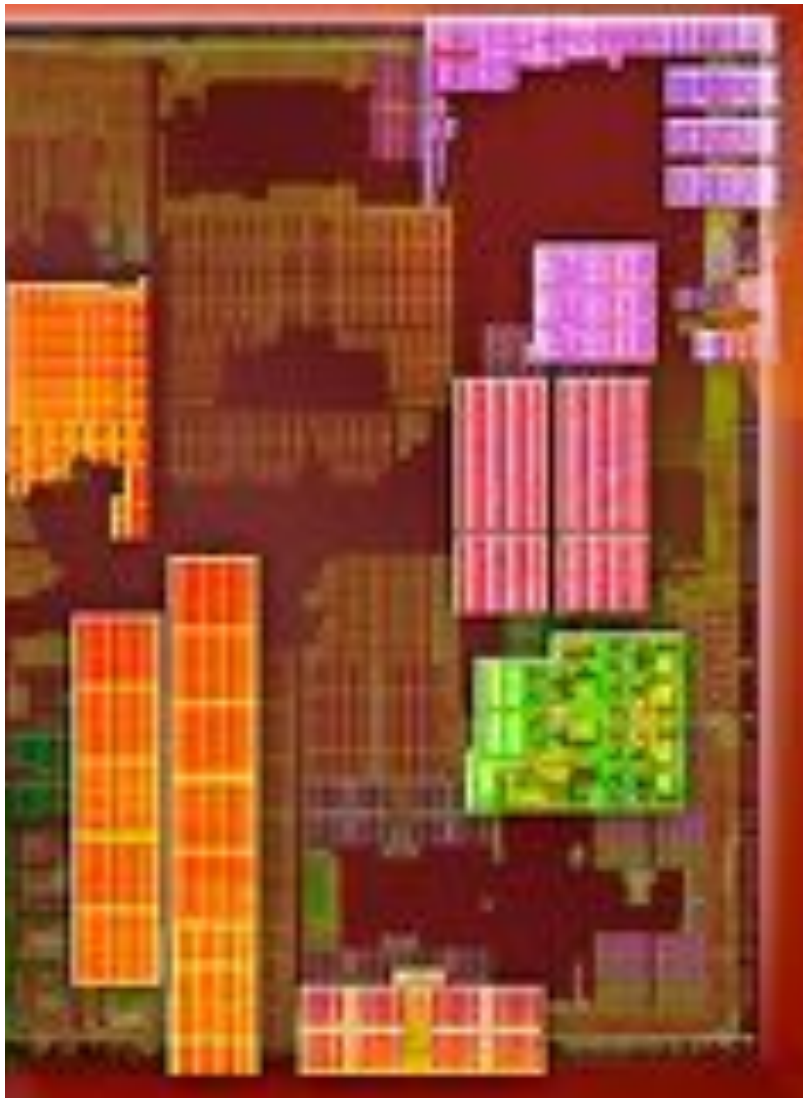
A7 Secure Enclave Processor & FIPS POST



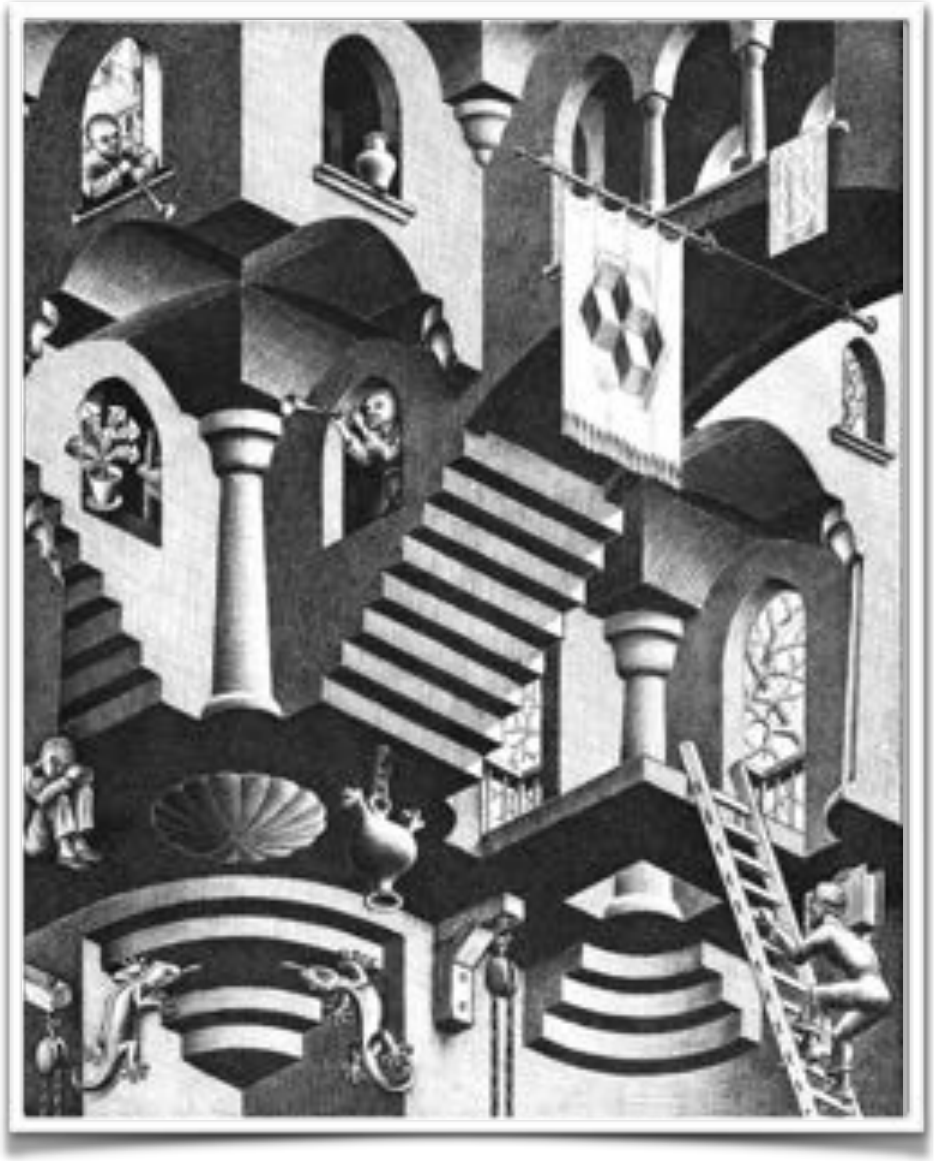


Secure Boot Chain & Power-On-Self-Test

Intel Pentium



 A7



Touch ID Security Architecture

All Things Security

All things Security

The Forged Fingerprint

Methodology

@ivydigital

The Goals of the Forgery

★ Collect the fingerprint enrolled to Touch ID

★ Make a high accuracy 3D forgery of the fingerprint

★ Fool Touch ID into interpreting a live finger

The Tradecraft of Forgery

- ★ Forensics "Crime Scene Investigation" methodologies
- ★ Scanning and Digitizing
- ★ Photo retouching
- ★ DIY Printed Circuit Board (PCB) Etching
- ★ Materials analysis, conductivity assessment
- ★ Moulding skin-like material

Wild Fingerprints

Latent Fingerprint

- composed of trace deposits of fat and sweat
- is not visible to the naked eye

Patent Fingerprint

- is visible to the eye
- marked by a substance on the fingers

If I can get the fingerprint, then I can bypass Touch ID

All Things Security

Fingerprinting Methods

The "10-print"

- old ink and card methodology
- civilian, juvenile, and criminal fingerprints

LiveScan Fingerprint

- An ink-less, electronic means of processing fingerprints
- high resolution scans

If I can get the fingerprint, then I can bypass Touch ID

Let's get some prints.

Find a Latent Print…

- On the glassware
- On iPhone Home Button

Fingerprint Repositories

- Civilian 10-print
- Criminal 10-print
- Child Identification

Digital Photography Archives (Facebook, Websites, etc)

- Public speakers who gesture
- Surveillance tapes

If I can get the fingerprint, then I can bypass Touch ID

All Things Security

Integrated Automated Fingerprint Identification System (AFIS)

- 76 million criminal subjects
- 34 million civilian 10-prints
- e-exchange to +18,000 entities internationally
- 24 / 7 / 365 access
- no apparent retention policy

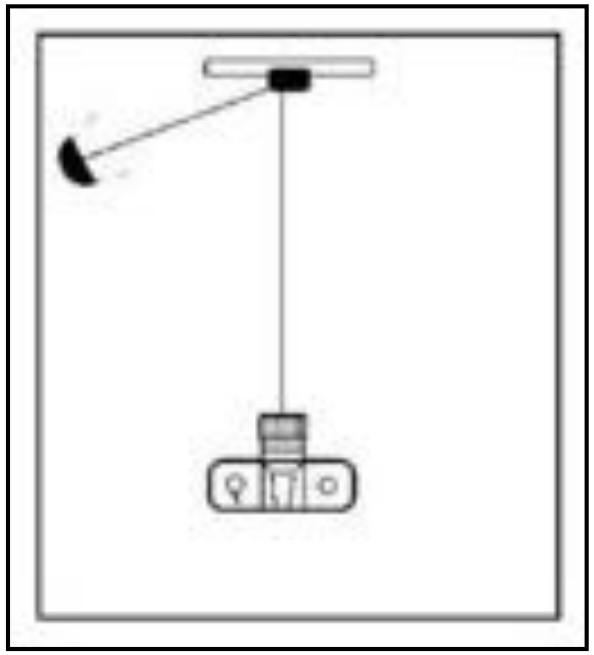
If I can get the fingerprint, then I can bypass Touch ID

All Things Security

The Nuance of Illusion

But latent fingerprints on the iPhone are invisible. Now what?

- Oblique lighting uses a light source positioned at a low angle
- Shows detail by creating shadows on the surface



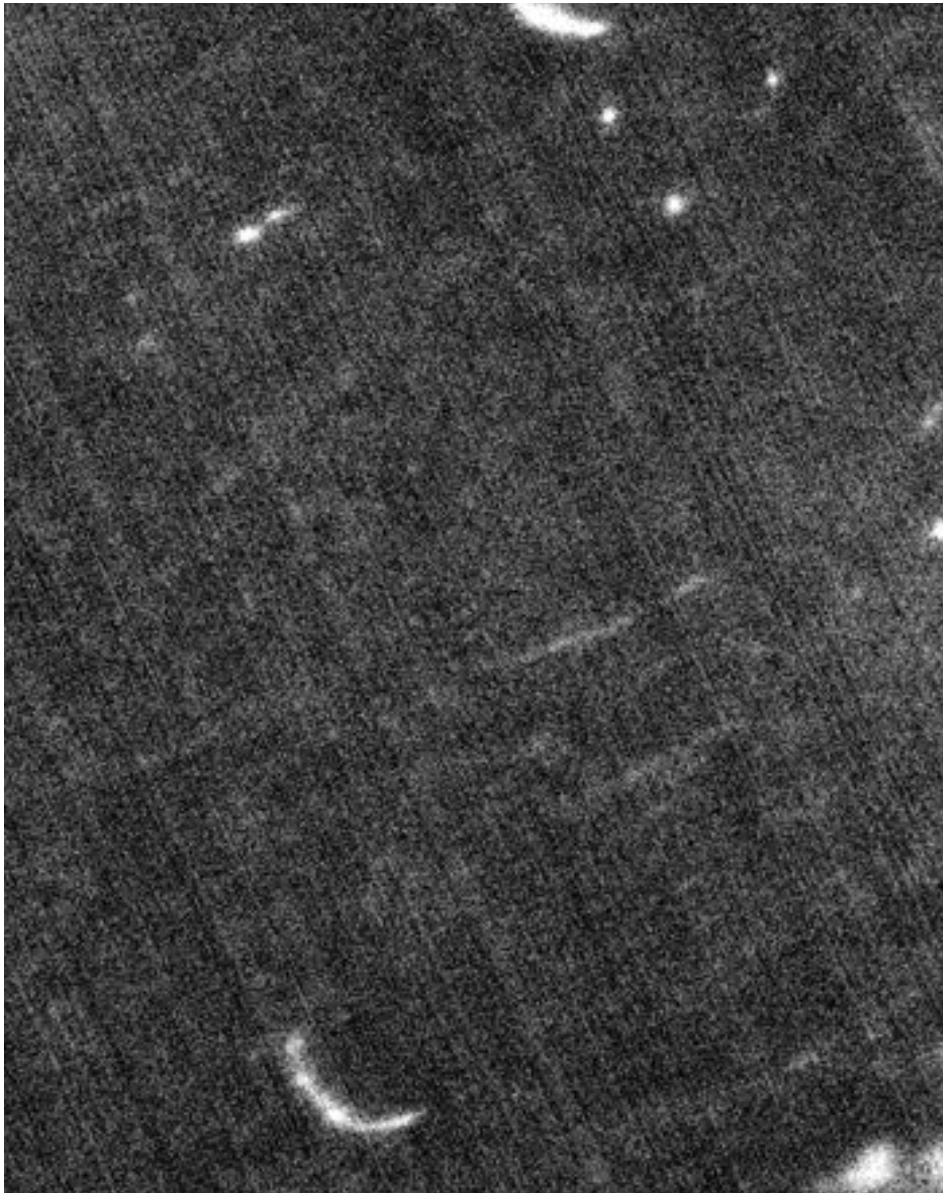
Between subtle shading and the absence of light…

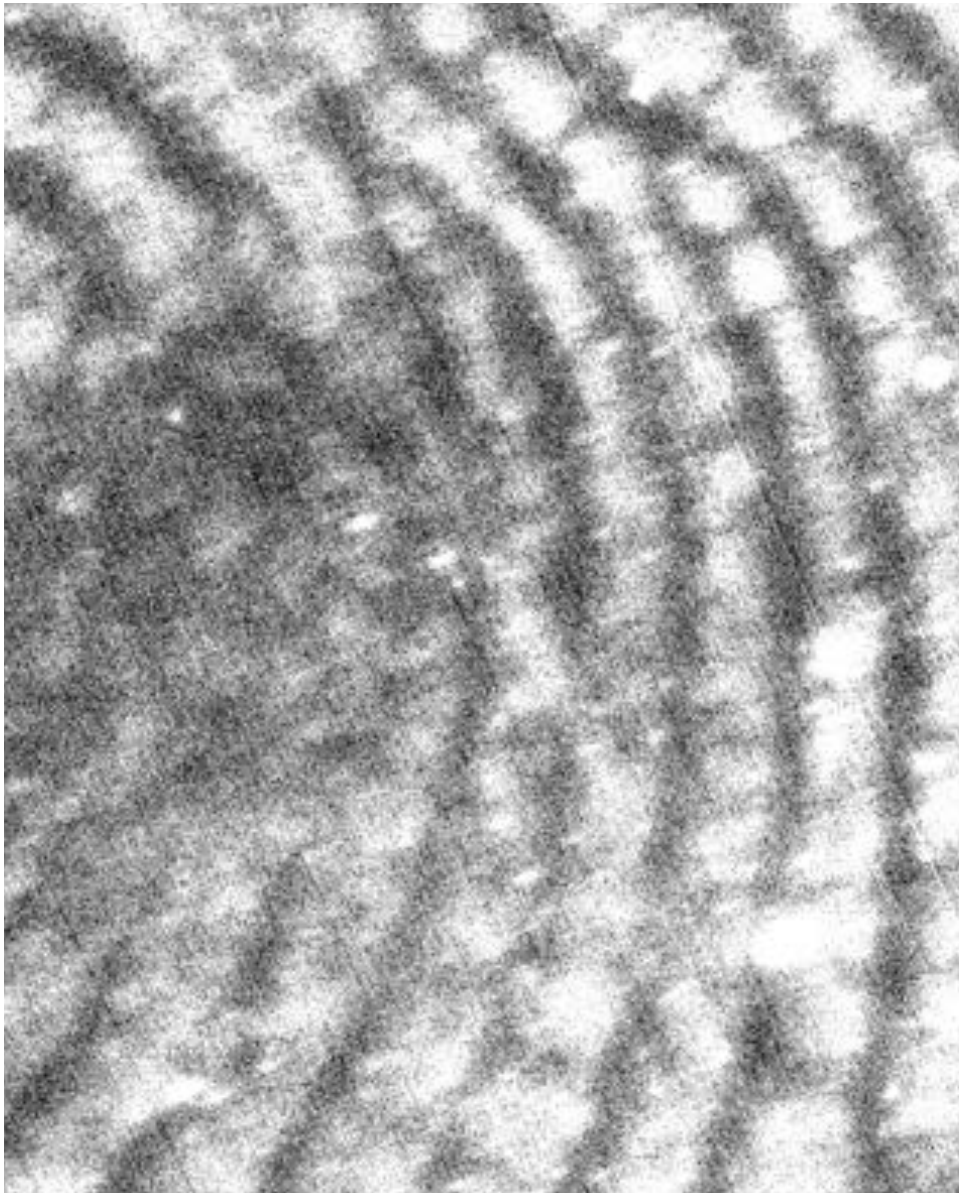
Digital Retouching

Between subtle shading and the absence of light…

All Things Security

Digital Retouching



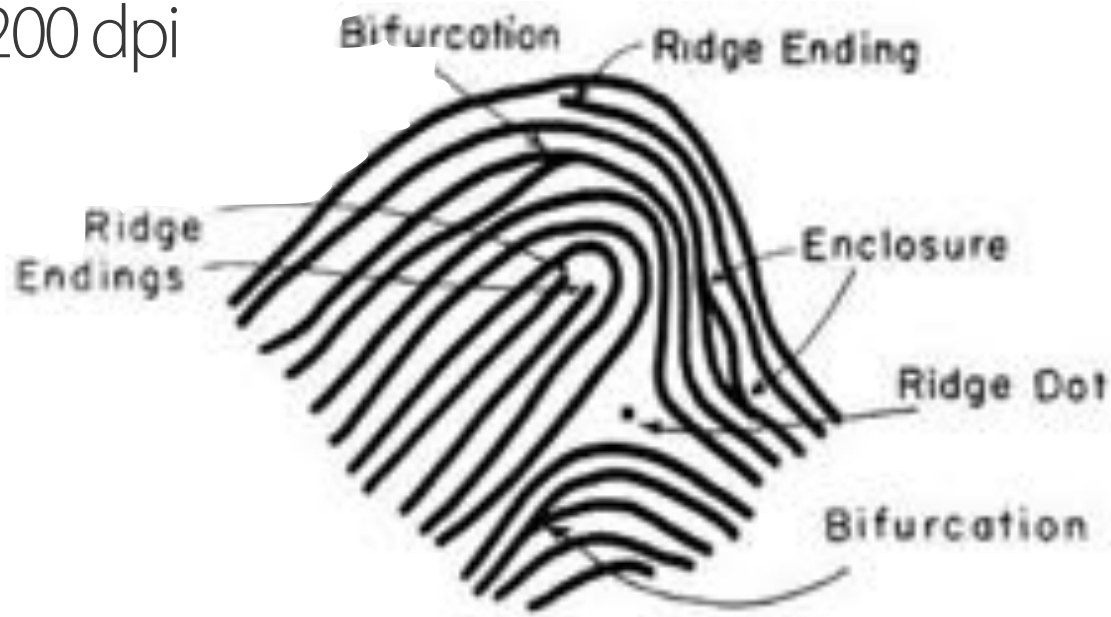


Between subtle shading and the absence of light…

All Things Security

Key Take-aways

- Ridges are white, furrows are black
- Don't destroy the minutiae
- Invert, then Mirror (Flip Horizontally)
- Scan 4800 dpi , Export 1200 dpi



Between subtle shading and the absence of light…

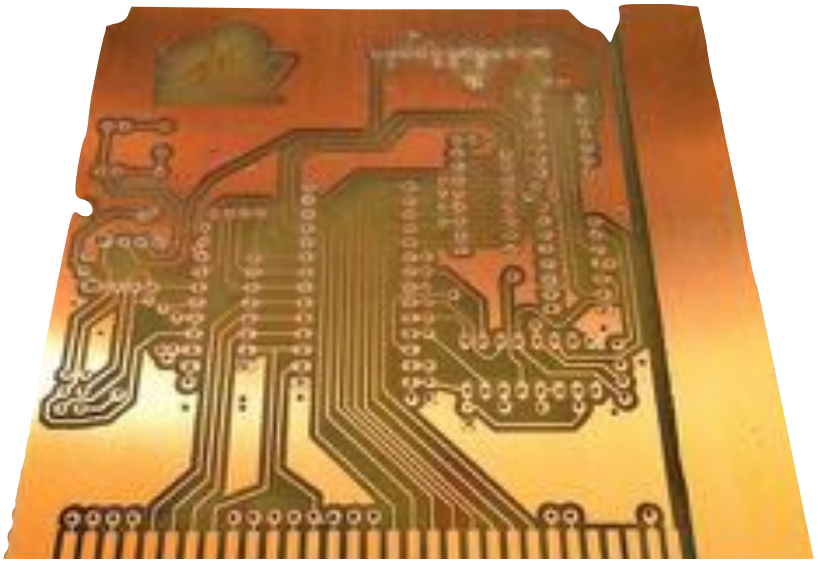
Building the 3D Mould

Challenge: Build a mould capable of producing a 3D replica of the finger pad complete with ridges identical in depth and pattern to the source fingerprint

Response: Dermal fingerprint ridges are 20-50 microns deep. The copper layer of a printed circuit board (PCB) is 34 microns thick, and can be custom etched using a chemical process.

Printed Circuit Boards (PCB)

- Used by DIY computer enthusiasts to prototype unique circuit board designs
- Also great for forgery!



3 Stages:

★ Ink Mask

★ Toner Transfer Method

★ Chemical Etching

The Ink Mask

- A laser printed template of the PCB design
- Printed onto "HP Brochure" or glossy paper
- Must be made with a Laser Printer

Toner Transfer

In PCB etching methodology, "toner transfer" is defined as the process of transferring laser toner to copper using thermal conduction

Chemical Etching

- The method by which unmasked copper on the board is corroded and shaped using a chemical bath composed of ferric chloride or other corrosive agents

- PCB is submerged for up to 20 minutes or until all excess copper is gone

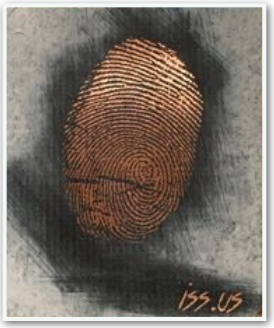
Zombie Children and Processes that Fail.

Challenge

- Ink won't stick to copper board

Response

- Ensure board is heating evenly and to the high temperature required for toner transfer



What we have here is a failure to exfoliate.

All Things Security

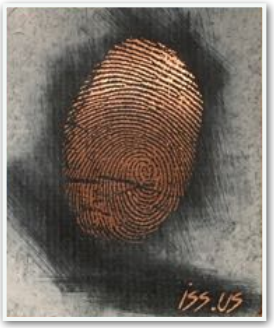
Zombie Children and Processes that Fail.

Challenge

- Ink won't stick evenly to copper board

Response

- Wear nitrile gloves at all times
- Ensure board is free of contaminants
- Buff w/ 2000 grain jeweler's sandpaper



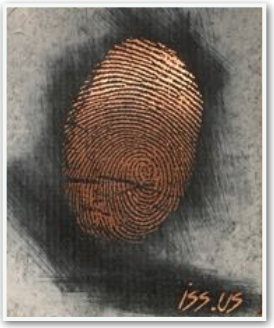
What we have here is a failure to exfoliate.

Before and After

actual color

What we have here is a failure to exfoliate.

All Things Security



Zombie Children and Processes that Fail.

Challenge

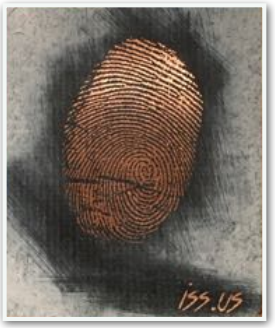
- Heavy paper residue sticking to ink

Response

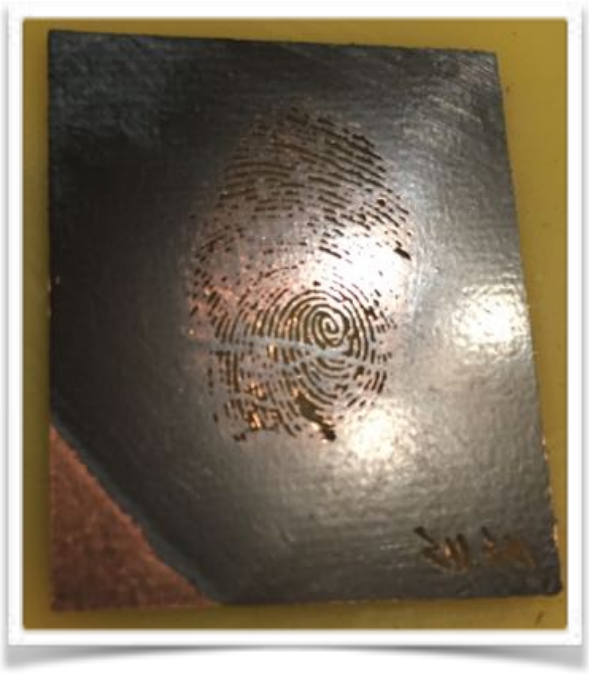
- paper is getting too hot and re-absorbing ink into it's core
- Limit to 90 seconds in the heat press

What we have here is a failure to exfoliate.

All Things Security



Zombie Children and Processes that Fail.



Challenge

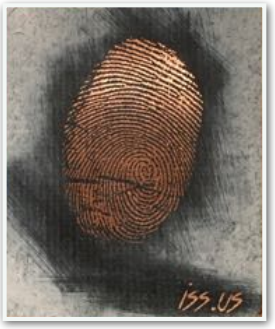
- Ink is too thick, ridge data disappearing due to bleeding ink

Response

- reduce toner output in printer dialogue

What we have here is a failure to exfoliate.

All Things Security



Mould Prototype

The Forged Fingerprint

Specifications

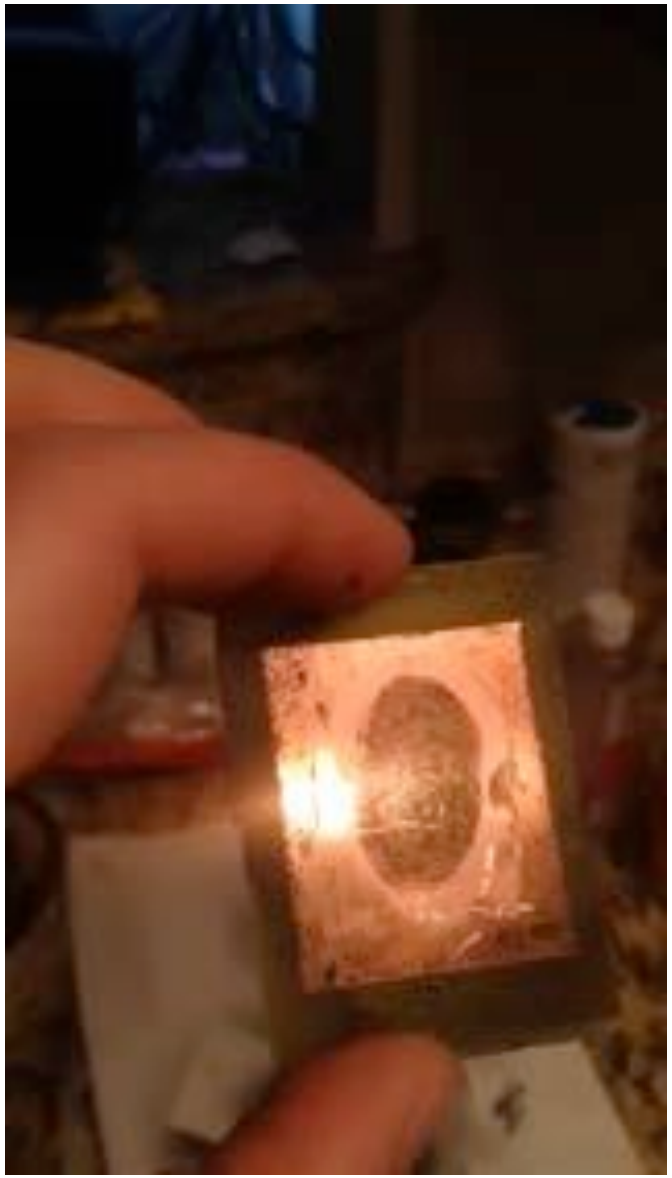
- No thicker than a credit card
- Readable surface larger than home button
- Must read as a "live finger"

Materials

- Wood Glue
- Glycerine
- Graphite Lube

Demo

The Forged Fingerprint



Touch ID

All Things Security

Lab

Did you bypass Touch ID with a Forged Fingerprint at PSU Mac Conference 2015?

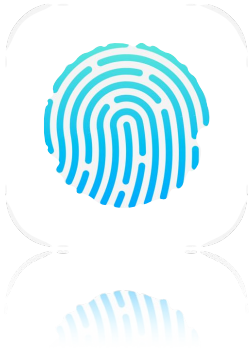
Please Tweet, and get the word out!

I just #HackedTouchID w/ a #ForgedFingerprint at #psumac HT @ivydigital (insert photo)

100 participants = 100 Bypasses - Can we do it?

All things Security

Biometrics & The Future



*"Hi, my name is ********."*

iOS Device Sensors

GPS Sensor

Audio Sensor

Infrared Sensor

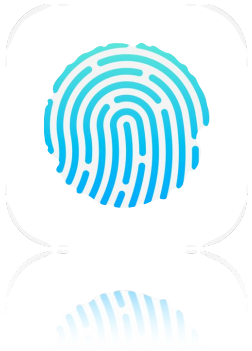
Accelerometer

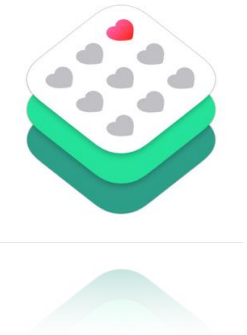
Capacitive Sensor

Magnetometer

Gyroscope

Camera Sensor





Biometric Technologies

TouchID

★ Fingerprint identity sensor built into home button
★ Provides on demand authentication for iPhone and ApplePay
★ Secure Enclave Processor for biometric data store

ResearchKit

★ Provides platform for big biometric data
★ Promotes deep mining for biometric identifiers
★ Opens a new surface for biometric authentication

"My voice is my passport."

All Things Security

DARPA

Active Authentication Program

- ★ Context-aware active authentication using smartphone accelerometer measurements
- ★ Provides "ways your computer or cell phone would know you are you"
- ★ Utilization of onboard sensors such as accelerometer, magnetometer, gyroscope
- ★ Provides identification of humans or their activities based on body movement patterns

All things

Biometric Technologies

TouchID

ResearchKit

"Verify Me."

All Things Security