Section 1: **Forensics Collection**

Length: **15 minutes**

Ivy Thomas

June 12, 2015

Bypass Touch ID with a Forged Fingerprint

Section 1. Forensics Collection

Objective: Using a high resolution scanner, collect fingerprints from targets described. Save and submit the best digital sample taken for each. Enroll the finger(s) used into Touch ID on iPhone 5s and iPhone 6.

Targets:

Latent fingerprint on the surface of the iPhone

Ink pad / card stock fingerprint

Clean finger-pad pressed to scanner glass

Procedure:

1. In Mac OS X, connect the HP ScanJet G4050 via USB and install drivers provided (HP_Scanjet_v1.3.0.dmg).

2. Power on the scanner and allow it to warm up, taking a test scan of the empty scanner bed to inspect for dust and anomalies before use. Avoid touching the glass except when described for the exercise.

3. While the scanner is warming up, analyze prints made and left on the surface of your iPhone, or your computer screen. How does the fingerprint deposit change when hands are washed, fingers brushed against nose? Pressed hard, or tapped lightly.

4. Two ink pads and 2 types of paper have been provided. Take fingerprints with a combination of each. Inspect closely for clarity and make an assessment of which materials will provide for the best scan.

5. Once the latent fingerprint and the inked fingerprint are ready, take high resolution (4800dpi) scans of each, cropping out excess canvas.

6. Next, take a scan of a clean finger-pad pressed to scanner glass.

7. Save to a thumb drive the best raw scan from each source collected and pass it to the Digital Retouching Team.

Section 2: **Digital Retouching**

Length: **20 minutes**

Ivy Thomas

June 12, 2015

Bypass Touch ID with a Forged Fingerprint

Section 2. Digital Retouching

Objective: Process provided raw scans of fingerprints into high-contrast black and white proofs. Export to PDF.

Targets:

3 raw scans provided by Forensics collection team (choose 1 for export)

1 raw scan of fingerprint provided by instructor

Note: Invert B&W, Flip Horizontally, Preserve Image Size — All Musts.

Procedure:

8. Advanced: Color Profiles — RICOH SP 112, B&W Laser

9. Import scans into GIMP (provided), Photoshop, or photo editing program of choice.

10. Rotate and crop as needed. Flip image horizontally.

11. Note the image size in inches. Though the pixel resolution will be reduced to 300 pixels per inch later in the exercise, the image size must not be modified.

12. Adjust the levels, exposure, and threshold to increase contrast to black and white. Reduce noise and retouch lines where needed.

13. After image is retouched satisfactorily, save a copy in PNG format before proceeding to reduce resolution for print template.

14. Resample the resolution of the file to 600 pixels per inch, ensure the image size is not modified.

15. Copy all layers to clipboard

16. Resize canvas to 8.5 x 11 inches, using a white (#000000) border

17. Paste contents of clipboard to create an array of 3x4, or twelve masks (Figure A) to create a contact sheet.

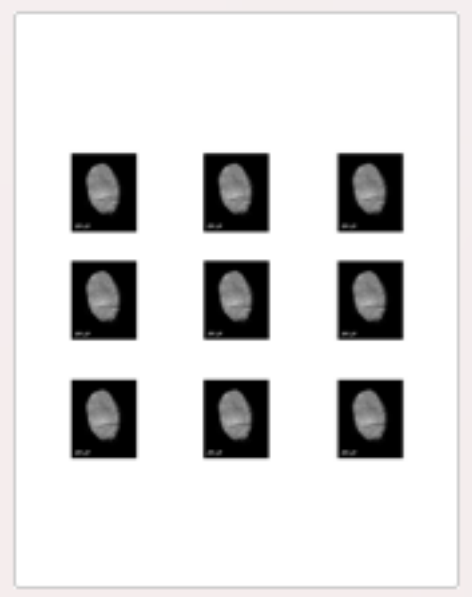
18. Save as a copy as PNG

19. Export to PDF, ensuring the PDF workflow does not modify any saved settings.

20. Repeat process for Fingerprint #2

21. Save both PDFs to the thumb drive provided, and pass to the Print Lab team.

(Figure A) Contact Sheet



Section 3: **Laser Print Lab**

Length: **10 minutes**

Ivy Thomas

June 12, 2015

Bypass Touch ID with a Forged Fingerprint

Section 3. Laser Print Lab

Objective: Print dummy fingerprint templates used for “toner transfer” to copper clad board (PCB). Print Techs will work closely with Toner Transfer Team to improve toner transfer process by manipulating factors such as thermal heat transfer, ink thickness, and paper stock.

Tech Notes: The “toner transfer” process transfers ink from paper surface and binds to the copper PCB. Regulating ink thickness and laser heat conduction to paper will be required to address flaws as they arise. The Lab Tech Team and Toner Transfer Team will work closely together to analyze and improve their results in order to produce a perfect toner transfer methodology.

Procedure:

22. Spin up a Windows 7 VM in VMware
23. Install VMware Tools
24. Install Ricoh SP 112 Print Driver
25. Install Adobe Reader
26. Import the PDFs to a shared folder accessible to the VM
27. Connect the printer to Windows VM
28. Print contact sheet, ensuring print output is to scale of 100%

Note: If toner transfer results in thick paper sediment transferring with the ink, the process must be tricked to lower the temperature of the paper when printing and heat pressing.

Section 4: **Toner Transfer**

Length: **25 minutes**

Ivy Thomas

June 12, 2015

Bypass Touch ID with a Forged Fingerprint

Section 4. Toner Transfer

Read all instructions before commencing exercise.

Objective: Produce a flawless toner transfer of the printed ink mask to copper clad board (PCB) using a heat transfer method. This method used is commonly used for etching printed circuit boards, however it works perfectly for etching fingerprints as well!

Safety: Nitrile Gloves must be worn at all times. Take extreme care to only use tools provided to handle hot objects such as tortilla press and copper boards

Procedure:

1. Preheat tortilla press for at least 25 minutes
2. Polish PCB to a high shine with jeweler's sandpaper, carefully handling PCB by edges to avoid contamination
3. Trim a fingerprint template to size and place it ink side down on the copper plated side of the PCB so the ink and copper are facing
4. Carefully place the paper and PCB on lower hot plate with the paper is facing up
5. Place several layers of folded parchment paper on top of the transfer.
6. Using the foam heat pad to grip the handle, close the tortilla press and hold steadily for 90 seconds.

1. Avoid jarring movements, or changing pressure of the handle as this may smear the ink.

7. Using precision tweezers, remove the PCB and place it in the bath of warm water for 5-10 minutes until paper can be gently rubbed away with fingertips
8. Once the PCB is masked to your liking, use a sharpie to mark the board in such a manner it can be recognized and differentiated later
9. If the transfer is imperfect, wipe the board with a cotton pad soaked in acetone to clean away all ink and residue. Repeat process, making changes where needed.
10. As a team, wave your arms wildly and shout: “TT Team Reporting In!!” Now, proceed to step 1 after covering any questions with a facilitator. (Sanity check…)

Troubleshooting:

A. The ink will not bond to the copper:
   i. Clean the board of all contaminants
B. Heavy paper residue sticking to ink
   i. The printer paper is getting too hot
C. the printed ridges are blurring into the valleys
   i. too much ink or proof is too dark:
      1. Use less ink
      2. Adjust levels

Section 5: **Wet Lab**

Length: **minutes**

Ivy Thomas

June 12, 2015

Bypass Touch ID with a Forged Fingerprint

Section 5. Wet Lab

Read all instructions before commencing exercise.

Objective: Using Ferric Chloride, manage chemical etching service of all PCB boards. Inspect incoming and outgoing plates for quality assurance.

Warning: Ferric Chloride eats metal. Imagine what it will do your body parts. No horseplay whatsoever allowed.

Safety: Nitrile Gloves must be worn at all times. Take extreme care to use only tools provided for submersion and removal of boards to and from Ferric Chloride bath. Ensure container lids are tightly sealed during agitation of liquids.

Procedure:

1. *Read all instructions before proceeding*
2. Pour 2 inches of water into trays provided
3. Pour approximately 1 cup of Ferric Chloride (FC) into reditainer provided
4. Using tongs, place PCB into FC bath
5. Replace lid, ensure it's completely sealed
6. Agitate reditainer rapidly for up to 20 minutes or when PCB is etched
7. Using tongs, remove PCB and place into H2O Bath #1, agitating for 20 seconds
8. Using tongs, remove PCB and place into H2O Bath #2, agitating briefly

9. Using tongs, remove PCB to paper towel and pat dry
10. Inspect closely, if etching is incomplete, return to FC bath, and repeat process until done
11. If etching is complete, wipe the board with a cotton pad soaked in acetone to remove all ink and residue
12. Pass the etched PCB to an instructor for inspection and further instruction on pairing with the
13. As a team, wave your arms wildly and shout: “WET LAB reporting for duty!!”

Now, proceed to step 1 after covering any questions with a facilitator.

Tip: Streamline your process by placing multiple boards in the bath per batch

Section 6: Wood Glue Dummy

Length: **30 minutes**

Ivy Thomas

June 12, 2015

Bypass Touch ID with a Forged Fingerprint

Section 5. Wood Glue Dummy

Read all instructions before commencing exercise.

Objective: Produce a conductive replica of the target fingerprint capable of authenticating against enrolled fingerprint and unlocking the iOS device. Additional objectives include successfully enrolling the replica into TouchID such that the un-enrolled finger is also capable of authenticating to Touch ID.

Tech Notes: In spite of all the ground work laid up to this step, a working dummy is very difficult produce. The dried dummy is no thicker than a credit card, any thicker will not register with Touch ID. No more than a micro-liter or two of glycerin must be mixed into the wood glue to help provide elasticity and prevent deformation when the dried dummy is later extracted from the mold. Just a thin layer of still wet graphite lube must be used to coat the surface of the mould split seconds before the mixture is applied with a fingertip.

It will take several attempts to become accustomed to the materials. Hence, wax paper is provided for practice.

Procedure:

1. Pour a quarter sized drop of wood glue onto the plastic tray provided
2. Pour a pin sized drop of glycerin onto a separate part of the tray

3. Ensure that the graphite lube is within reach
4. Dip your index finger lightly into the glycerin, then mix thoroughly into the wood glue, avoiding bubbles and clumping
5. Spray a layer of graphite lube over the mould, and immediately apply wood glue, spreading evenly over the surface with your finger
6. Allow the dummy to dry, using a blow dryer to expedite process
7. Once dummy is completely dry, use a nylon probe tool to carefully lift it from the board.
8. The dummy should look and feel just like skin, if the mixture is correct. Note that if the dummy splits, or feels oily to the touch, there's too much glycerin. If it looks like very dry skin, and lacks elasticity, more glycerin is needed.
9. Place the dummy over the surface of the Touch ID and press to authenticate.