Printed Circuit Board Deconstruction Techniques

Joe Grand

Grand Idea Studio, Inc.

joe@grandideastudio.com

Abstract

The primary purpose of printed circuit board (PCB) reverse engineering is to determine electronic system or subsystem functionality by analyzing how components are interconnected. We performed a series of experiments using both inexpensive home-based solutions and state-of-the-art technologies with a goal of removing exterior coatings and accessing individual PCB layers. This paper presents our results from the most effective techniques.

1 Introduction

Reverse engineering – the art of undesigning an existing system – is critical for determining functionality, forensic analysis/intelligence, or testing/verifying security schemes [1, 2]. The primary purpose of printed circuit board (PCB) reverse engineering is to understand how components are interconnected. One step in that process is to access and image each layer of the target circuit board. When all layers are placed together, a complete circuit layout can be identified. Armed with this information, one can clone the design (e.g., to create counterfeits or recreate a previous design whose documentation has been lost [3, 4, 5]), identify areas where new features/capabilities can be added (e.g., injecting malicious functionality into an existing, off-the-shelf product), locate specific connections (e.g., a serial port or on-chip debug interface that can aid in interaction with or manipulation of a system), or derive how a product works by creating a schematic diagram (a simplified, visual representation of the device’s electronic design).

This paper details the testing and analyses of PCB deconstruction techniques using both inexpensive home-based solutions with off-the-shelf materials and state-of-the-art technologies in an attempt to remove exterior coatings and expose the PCB layers. Some of the techniques discussed in this paper are employed by semiconductor manufacturers and PCB fabrication/assembly facilities for chip- and board-level failure analysis and testing [6, 7], though they are generally limited to small, specific areas.

In order for our research to mimic real-world scenarios as closely as possible, we used multiple PCBs with varying fabrication specifications, including simple 2-layer boards and complex, 10-layer boards from highly integrated, modern devices. Not every type was involved in every experiment, but having a wide range and large number allowed us to sufficiently test various techniques.

The rest of this paper is structured as follows: Section 2 provides a background on PCB fabrication and composition. Sections 3, 4, and 5 detail the techniques used in the three phases of PCB deconstruction: Solder mask removal, delayering, and imaging, respectively, and provide experiment procedures, results, and photos. Section 6 provides a list of the techniques and a characterization of each based on the time required, cost, access to equipment, ease of use, likelihood of success, and quality of result. We conclude with a summary of our work in Section 7.

This paper has been published in the Proceedings of the 8th USENIX Workshop on Offensive Technologies (WOOT’14), San Diego, CA, August 19, 2014.
2 PCB Composition

PCBs are created with layers of thin copper foil (conductive) laminated to insulating (non-conductive) layers. They form the physical carrier for and provide electrical pathways between electronic components. By accessing and imaging each individual copper layer of a PCB (Fig. 1), it is possible to reverse engineer the entire PCB layout.

Standard PCB fabrication technology allows for trace widths as low as 3mil and mechanically-drilled hole diameters of 8mil. State-of-the-art processes support trace and space widths less than 1mil, laser-drilled microvia diameters of 0.4mil, via-in-pad construction, and passive electronic components embedded into substrate. Copper thickness, defined as the weight of copper per square foot, typically ranges from 0.5oz (0.7mil) to 4oz (5.6mil). A PCB cross-section will often provide clues to its design and complexity (Fig. 2).

Once a PCB is fabricated, its surface is coated with solder mask (also known as solder resist). Comprised of epoxy, liquid photoimageable ink (LPI), or dry film photoimageable material, this non-conductive layer protects the PCB from dust and oxidation, and provides access to copper areas on the board that are desired to be exposed (such as component pads or test points). The most commonly used solder mask color is green, though many other colors are available. Darker colors make visual identification of traces difficult.

A thin surface finish, in the form of lead-based or lead-free solder, tin, silver, gold, or palladium, is then applied to the exposed copper to enhance solderability and/or for harder contact surfaces.

Finally, a component legend (also known as a silk-screen) is printed onto the board using epoxy or printable ink. This layer often contains the part designators, identification symbols, logos, and other manufacturing markings useful for PCB assembly/testing and field service operations.

A comprehensive guide to PCB fabrication and design processes can be found in [9].

3 Solder Mask Removal

The goal of this phase is to remove the solder mask from the PCB and expose the copper traces on the top and/or bottom layers with minimal damage. While it’s sometimes possible to identify the copper traces through existing solder mask, removing the solder mask will give a more clear view. The following processes assume no components are populated on the target PCB.
3.1 Sandpaper

Sandpaper is an effective and low cost method for solder mask removal. We obtained the best results by clamping the target PCB to a work table and using the sandpaper, held by hand, in even strokes at light pressure across the entire PCB surface (Fig. 3). Spare PCBs of the same height as the target were used as support material on both sides to help maintain planar motion and even sanding pressure. Care must be taken to ensure that the underlying copper layer isn’t damaged by excessive abrasion.

Different PCB surface finishes require different sandpaper grit sizes. For example, on a PCB with thick hot air solder leveling (HASL) finish, we first used 60 grit sandpaper to remove the thick solder from all of the exposed copper pads and then used 220 grit sandpaper to complete the solder mask removal. On the iPhone 4 Logic Board, which has immersion gold plating, thinner solder mask, and trace/space less than 3/3mil, we used a less abrasive 400 grit sandpaper (Fig. 4).

3.2 Fiberglass Scratch Brush

Fiberglass scratch brushes are handheld, pencil-shaped tools used for material cleaning and polishing. For our experiment, we used an Excelta Eurotool fiberglass scratch brush in even strokes at medium pressure (Fig. 5). The result was very clean with only light wear of the underlying copper. It is recommended to wear thick gloves when using this technique, as small fiberglass fragments break off the brush as it wears down and can easily embed into the skin.

3.3 Abrasive Blasting

Abrasive blasting is a method of forcibly propelling a stream of abrasive material against a target object. It is typically used to strip material from surfaces (e.g., from paint, calcium deposits, or fungus) or add texture/artificial wear to a product. The abrasive material (also known as media) comes in many forms to suit different materials and finishes, including garnet, glass beads, crushed walnut shells, and synthetic abrasives.

For our experiment, we used an industrial-caliber TP Tools Skat Blast 1536 Champion blast cabinet with an 80 pounds per square inch (PSI), 10-15 cubic feet per minute (CFM) output of 60 grit aluminum oxide (Fig. 6).

Micro-abrasive blasting cabinets also exist, which are designed to more accurately deliver abrasive to a small part or a small area of a larger part, but were not available for use during our research.
We obtained the best results when the nozzle was angled and held 6” to 8” away from the PCB. The copper and underlying substrate remained intact, though there was noticeable pitting due to the abrasive media (Fig. 7). A softer media, such as crushed walnut shells, may cause less surface wear.

Abrasive blasting is most suited for simple PCBs with large features (10/10mil trace/space or greater) and copper weight of 1oz (1.4mil) or more. Regardless of PCB construction, there is a risk of damaging underlying copper by overzealous use of the tool or remaining on one area of the PCB for too long.

3.4 Chemical

Chemical removal of solder mask is often used by PCB fabricators to remedy a manufacturing error or for failure analysis purposes. Ristoff C-8 and Magnastrip 500 are two chemicals specifically formulated for this purpose. They both require hazardous chemical handling and disposal procedures, and misuse can lead to fire, explosion, severe burns, and other health hazards. Neither chemical will attack the PCB substrate/laminate provided proper operating procedure is followed.

1. Heated the chemical to 120-140°F (up to 200°F for Magnastrip 500). We used a 1L glass beaker on a Barnstead Thermolyne Type 1900 Laboratory Hot Plate.

2. Placed the target PCB into the beaker and waited for solder mask stripping to occur (45-120 minutes for Ristoff C-8 and 15-60 minutes for Magnastrip 500). Actual processing time will vary due to chemical temperature, solder mask composition, and solder mask thickness. As the solder mask broke down, it flaked off the PCB into the solution.
3. Removed the PCB from the beaker and brushed lightly with a soft metal brush under running water. This helped to lift any remaining solder mask from the board.

The results for both chemicals were excellent, producing clean, exposed top/bottom copper layers with no abrasion or scratching (Fig. 9 and 10). However, silk-screen is more resistant to Magnastrip 500 than Ristoff C-8, and required a longer soak in order for the solder mask underneath the silk-screen to completely break down.

3.5 Laser

Laser skiving is traditionally used for selective, highly controlled material removal or rework (e.g., accessing and/or cutting a single trace on a PCB’s inner layer). Our experiments were performed using a LPKF Micro-Line 600D UV Laser System (Fig. 11), which is designed for accurate (+/-0.6mil), stress free cutting of flex circuits and coverlayer material (e.g., foil, film, or adhesive).

After a machine setup time of approximately 30 minutes, we ran single passes at medium power across small, specific areas of target PCBs. The laser was successful in removing solder mask from both boards, leaving copper fully intact (Fig. 12). The carbon residue/soot remaining on the exposed copper surfaces was removed with steel wool under running water.

Solder mask and substrate react more quickly to the UV laser than copper, so care must be taken to ensure that the laser power is properly adjusted to the minimum required for a given target PCB. Otherwise, subsequent copper layers could be exposed as inner layer substrates are inadvertently removed.

With the laser traveling at a maximum speed of 300mm/second (11.8”/second) and a beam diameter of approximately 20um (0.787mil), processing an entire PCB could take anywhere from a few minutes to a few hours depending on surface area and solder mask thickness.

4 Delayering

The goal of this phase is to access the inner copper layers of a multi-layer PCB by way of physical, destructive delayering. The following processes assume no components are populated on the target PCB.
Figure 13: Hand sanding to remove the PCB’s top copper layer (left) and the resulting inner layer 2 (right).

4.1 Sandpaper

Sandpaper is an effective and low cost method for removing layers of PCB material. However, the required pressure and repeated sanding motions can quickly cause operator fatigue in the arms and hands.

For our experiment, we mounted a target 4-layer PCB to our work table with double-sided tape. Then, we used 60 grit sandpaper held by a Norton Sheet Sander tool in hard, full strokes across the entire PCB area (Fig. 13). After approximately 20 minutes of effort, all substrate was successfully removed and inner layer 2 was exposed. The resulting layer exhibited minor scratching and noticeable wearing of copper along the edges due to uneven sanding.

4.2 Dremel Tool

The Dremel MultiPro is a common, off-the-shelf home improvement tool used in a variety of applications, including cutting, grinding, drilling, routing, polishing, and sanding. For our experiment, we used a Dremel 503 flapwheel (120 grit, 3/8” wide) attachment (Fig. 14). The flapwheel is difficult to align and must be kept flat in order to prevent an edge from digging into the PCB. A Dremel 225 flexible shaft will help to move the body of the Dremel tool away from the work surface and make it easier to keep the flapwheel flat against the PCB.

We were able to expose layer 3 of the target PCB in just under nine minutes using back and forth motions at medium pressure. It was difficult to achieve even abrasion across the entire PCB surface, which caused copper in some areas to be exposed earlier than others. This could be remedied with more practice using the tool.

4.3 CNC Milling

CNC milling machines are used for highly accurate, computer controlled removal or engraving of material. Many different types of CNC milling equipment exist, including PCB prototyping machines, which create custom PCBs by milling traces and pads on copper-clad stock.

For our experiment, we used a T-Tech QuickCircuit 5000 PCB Prototyping System (Fig. 15) with a Think & Tinker MN208-1250-019F 1/8” diameter carbide endmill specifically designed for working with non-ferrous materials. Control and manipulation of milling, drilling, and routing procedures are achieved using T-Tech’s IsoPro software running on a host computer, except for tool type, tool cutting depth (Z-axis), and solenoid force, which are manually set by the operator. The QuickCircuit 5000’s Z-axis can be adjusted in 10um (0.4mil) increments.

Figure 14: Using the Dremel tool to expose layer 3 through the substrate (left) and the resulting inner layer (right).

Figure 15: The T-Tech QuickCircuit 5000 PCB Prototyping System and host laptop running IsoPro 2.7.
Our goal was to access the inner layers of a small portion of the iPhone 4 Logic Board. First, a mechanical outline of the desired PCB area (0.92” x 0.58”) was created in IsoPro and configured to rubout all material inside of the area (Fig. 16). This step provided accurate, repeatable, and automatic positioning of the milling path, as opposed to manually controlling the machine. Then, we adjusted the Z-axis depth in approximately 1mil increments between runs of the milling machine (set to move at a rate of 8”/minute with a spindle speed of 24,000 RPM). When we could begin to see the next layer of copper beneath the substrate, we stopped milling and used a fiberglass scratch brush (detailed in Section 3.2) to remove the remaining substrate and expose the area.

We were successful in fully exposing inner layers 2 through 5 on a portion of the iPhone PCB in approximately two hours (Fig. 17). Some traces appear to be missing (likely due to rushed use of the scratch brush), but the overall result is promising given the complexity of the target PCB.

The method requires time and patience to slowly increase the Z-axis depth to avoid accidental damage of the target PCB’s inner layers. Though our experiment focused on a small portion of the PCB, the process could certainly be expanded to work on the entire board area with the same results.

### 4.4 Surface Grinding

Surface grinding is an abrasive machining process used for material grinding and surface finishing. A surface grinding machine consists of a rotating abrasive wheel (also known as a grinding wheel), work surface, and a reciprocating or rotary table controlled manually or by a computer.

Our experiment was performed on a Blohm PROFIMAT CNC Creep Feed Surface Grinder with a Radiac 1 3/8”-wide grinding wheel (Fig. 18). Despite its size, this machine is highly precise and allows depth control in 0.1mil increments. Once it is properly aligned to the target material and configured to the desired grinding parameters and surface finish (which takes approximately 30 minutes by a trained operator), it runs quickly and consistently.

A 6-layer target PCB was mounted to a 1” steel block, which was held in place by the machine’s magnetic chuck. The depth was adjusted in small increments (starting at 0.5mil and increasing to 2mil) in between runs of the surface grinder until we were able to see the next layer of copper beneath the substrate. Each
run of the machine took approximately 45 seconds. If the target PCB’s inter-layer spacing is known or can be determined with a cross-section measurement, less trial and error will be necessary and the process can be expedited. Occasionally, the grinding wheel was put through a dressing process to maintain the wheel’s desired roughness and shape. This process took approximately one minute.

Surface grinding was successful in revealing the inner layers of the PCB (Fig. 19). The resulting surface finish, 32 Root-Mean-Square (RMS), was so smooth that each copper layer was clearly visible through the remaining fiberglass substrate. This precluded the need to fully expose the copper layer in order to obtain a usable image.

The process will work well with PCBs of nearly any size, though custom mounting methods may need to be created for boards that do not contain mounting holes or to help flatten a board that is bowing/flexing. Ensure that the PCB is not removed from the machine part way through the process, as properly realigning the PCB is difficult and may affect subsequent grinding runs.

5 Imaging

The goal of this phase is to obtain individual image layers of a multi-layer PCB using non-destructive imaging techniques. Such techniques may be successful even against a fully assembled/populated PCB.

5.1 X-ray (2D)

X-ray inspection equipment is typically used during the PCB assembly process to verify component placement and proper solder quality, or after the assembly process for failure analysis to identify, locate, or troubleshoot defective features. X-ray waves are emitted from an X-ray tube on one side of the target object and captured by a detector on the opposite side.

For our experiment, we used a DAGE XD7500VR X-ray Inspection System (Fig. 20) with multiple target PCBs. For each PCB, a series of X-ray images were taken at a variety of angles and contrasts. Due to the nature of 2D X-ray imaging, the resulting images were composites of all PCB layers. This made it difficult to determine on which layer a particular trace was located (Fig. 21).
X-ray inspection can still be useful to some extent, as one can get a general sense of PCB construction/layout and, for simple boards, visually follow traces/connections by manipulating the X-ray's angle and field-of-view in real time. However, it would be a time consuming and tedious process to recreate full image layers using this method.

5.2 Computerized Tomography (3D X-ray)

Computerized Tomography (CT) is an X-ray imaging method where a series of 2D X-ray images are post-processed to create cross-sectional slices of the target object. CT is frequently employed for complex inspection and failure analysis of PCBs, electronic component packaging, and solder ball quality.

For our experiment, we used a Nordson DAGE XD7600NT Ruby X-ray Inspection System (similar in exterior appearance to Fig. 20). This particular system had Nordson DAGE's X-Plane software package installed, which provided the CT functionality.

The first step in the process was to capture a series of 2D X-ray images (between 60 and 720, depending on the desired resolution of the resulting cross-sectional slices) by rotating the X-ray 360° in a single axis around the target object. In our case, 360 images were taken around a 4-layer Emic 2 Text-to-Speech Module PCB at a 50° inclination angle. The entire scan took 36 minutes, corresponding to one image every 6 seconds. Next, mathematical post-processing of the images resulted in 240 2D slices that could be viewed in any plane (X, Y, or Z). The post-processing phase took only 3 minutes. These slices were then imported into VGStudio, an off-the-shelf software tool used for 3D model manipulation, which provided a graphical environment to more easily analyze the images and to add various effects to show depth or highlight specific areas (Fig. 22).

The results were impressive, as we could move through the slices along the Z plane (from top to bottom through the PCB) and easily identify each of the target PCB's layers (Fig. 23). Note that the success of CT may vary depending on PCB construction features, such as layer stack-up, material composition, copper weight, and component placement.

A minor limitation of CT is the size of the X-ray system's field-of-view. The more area that is visible within the field-of-view, the less resolution/detail will exist on the acquired images. As such, one will need to find the balance between sufficient board visibility and image quality, which in most cases won’t comprise the entire PCB area. In order to process a full PCB, multiple "segments" would need to be created and stitched together.

Figure 22: Screenshot from VGStudio 2.1 showing X, Y, and Z cross-sectional views of a PCB.

Figure 23: CT images of the Emic 2 PCB. The field-of-view was limited to the bottom center area of the board. The four layers (left to right) were confirmed to match the known layouts of Fig. 1.

9


6 Characterization Matrix

Depending on goals and available resources, some techniques may be more suitable than others. Table 1 provides a list of PCB deconstruction techniques along with a characterization of each based on the time required, cost, access to equipment, ease of use, likelihood of success, and quality of result. These criteria can be used to aid in the selection of the most appropriate method for a particular situation.

7 Conclusion

This paper detailed our PCB deconstruction experiments, including solder mask removal, delayering, and imaging, and provided a number of practical, effective techniques that could be used to access individual layers of a target circuit board.

It is hoped that our work will serve as a comprehensive guide to PCB deconstruction techniques, help those involved in electronic product development understand which PCB fabrication techniques make PCB reverse engineering more difficult, and help further the general knowledge and skill sets of the cyber security community and those involved in failure analysis, reverse engineering, and/or hardware hacking.

<table>
<thead>
<tr>
<th>Technique</th>
<th>Time Required</th>
<th>Cost</th>
<th>Access to Equipment</th>
<th>Ease of Use</th>
<th>Likelihood of Success</th>
<th>Quality of Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solder Mask Removal</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sandpaper</td>
<td>&lt; 1 hour</td>
<td>$</td>
<td>Easy</td>
<td>Easy</td>
<td>Fair</td>
<td>Good</td>
</tr>
<tr>
<td>Fiberglass scratch brush</td>
<td>&lt; 1 hour</td>
<td>$</td>
<td>Easy</td>
<td>Easy</td>
<td>Excellent</td>
<td>Excellent</td>
</tr>
<tr>
<td>Abrasive sand blasting</td>
<td>&lt; 1 hour</td>
<td>$$</td>
<td>Moderate</td>
<td>Medium</td>
<td>Fair</td>
<td>Good</td>
</tr>
<tr>
<td>Ristoff C-8</td>
<td>3-4 hours</td>
<td>$$</td>
<td>Difficult</td>
<td>Hard</td>
<td>Excellent</td>
<td>Excellent</td>
</tr>
<tr>
<td>Magnastrip 500</td>
<td>3-4 hours</td>
<td>$</td>
<td>Difficult</td>
<td>Hard</td>
<td>Excellent</td>
<td>Excellent</td>
</tr>
<tr>
<td>Laser</td>
<td>2-3 hours</td>
<td>$$$</td>
<td>Moderate</td>
<td>Hard</td>
<td>Varies</td>
<td>Excellent</td>
</tr>
</tbody>
</table>

Delayering

<table>
<thead>
<tr>
<th>Technique</th>
<th>Time Required</th>
<th>Cost</th>
<th>Access to Equipment</th>
<th>Ease of Use</th>
<th>Likelihood of Success</th>
<th>Quality of Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sandpaper</td>
<td>2-3 hours</td>
<td>$</td>
<td>Easy</td>
<td>Easy</td>
<td>Fair</td>
<td>Excellent</td>
</tr>
<tr>
<td>Dremel tool</td>
<td>&lt; 1 hour</td>
<td>$</td>
<td>Easy</td>
<td>Medium</td>
<td>Poor</td>
<td>Varies</td>
</tr>
<tr>
<td>CNC milling</td>
<td>3-4 hours</td>
<td>$$</td>
<td>Moderate</td>
<td>Hard</td>
<td>Excellent</td>
<td>Excellent</td>
</tr>
<tr>
<td>Surface grinding</td>
<td>3-4 hours</td>
<td>$$$</td>
<td>Moderate</td>
<td>Hard</td>
<td>Excellent</td>
<td>Excellent</td>
</tr>
</tbody>
</table>

Imaging

<table>
<thead>
<tr>
<th>Technique</th>
<th>Time Required</th>
<th>Cost</th>
<th>Access to Equipment</th>
<th>Ease of Use</th>
<th>Likelihood of Success</th>
<th>Quality of Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>X-ray (2D)</td>
<td>Many</td>
<td>$$$</td>
<td>Moderate</td>
<td>Medium</td>
<td>Poor</td>
<td>Varies</td>
</tr>
<tr>
<td>Computerized Tomography</td>
<td>1-2 hours</td>
<td>$$$</td>
<td>Moderate</td>
<td>Medium</td>
<td>Fair</td>
<td>Excellent</td>
</tr>
</tbody>
</table>

Table 1: Characterization matrix of PCB deconstruction techniques.
Acknowledgements

This work was funded by the Defense Advanced Research Projects Agency (DARPA) Cyber Fast Track program. The views and opinions expressed in this paper are those of the author and do not reflect the official policy or position of the Department of Defense or the United States Government.

We would like to thank BIT Systems for managing the project, the USENIX WOOT ‘14 anonymous reviewers for providing comments on this paper, and Keely, Benjamin, and Miles for their balance and support.

References


